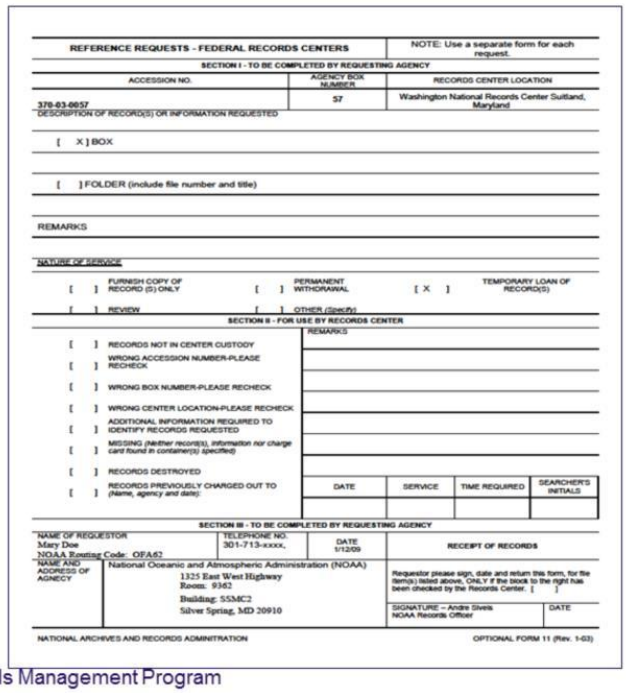
RETRIEVING RECORD FROM THE FRCs

- Provide the following information to process requests efficiently:
  - Full transfer number
  - Box number
  - Folder name or number, if applicable
  - Type of request
  - Name, agency, & phone number of requestor
  - Date & time needed if for pickup or review
  - Mailing address if mailed, UPS, or FedEx

SAMPLE OF-11 FORM



REFERENCE REQUESTS - FEDERAL RECORDS CENTERS — NOTE: Use a separate form for each request.

SECTION I - TO BE COMPLETED BY REQUESTING AGENCY

ACCESSION NO.	AGENCY BOX NUMBER	RECORDS CENTER LOCATION
370-03-0057	57	Washington National Records Center Suitland, Maryland

DESCRIPTION OF RECORD(S) OR INFORMATION REQUESTED

[X] BOX

[ ] FOLDER (include file number and title)

REMARKS

NATURE OF REMARK

[ ] FURNISH COPY OF RECORD (S) ONLY [ ] PERMANENT WITHDRAWAL [X] TEMPORARY LOAN OF RECORD(S)

[ ] REVIEW [ ] OTHER (Specify)

SECTION II - FOR USE BY RECORDS CENTER

REMARKS

[ ] RECORDS NOT IN CENTER CUSTODY
[ ] WRONG ACCESSION NUMBER-PLEASE RECHECK
[ ] WRONG BOX NUMBER-PLEASE RECHECK
[ ] WRONG CENTER LOCATION-PLEASE RECHECK
[ ] ADDITIONAL INFORMATION REQUIRED TO IDENTIFY RECORDS REQUESTED
[ ] MISSING *(Neither record(s), information nor charge card found in container(s) specified)*
[ ] RECORDS DESTROYED
[ ] RECORDS PREVIOUSLY CHARGED OUT TO *(Name, agency and date)*:

DATE	SERVICE	TIME REQUIRED	SEARCHER'S INITIALS

SECTION III - TO BE COMPLETED BY REQUESTING AGENCY

NAME OF REQUESTOR: Mary Doe
NOAA Routing Code: OFA62
TELEPHONE NO.: 301-713-xxxx,
DATE: 1/12/09
RECEIPT OF RECORDS

NAME AND ADDRESS OF AGENCY: National Oceanic and Atmospheric Administration (NOAA)
1325 East West Highway
Room: 9362
Building: 55MC2
Silver Spring, MD 20910

Requestor please sign, date and return this form, for file item(s) listed above, ONLY if the block to the right has been checked by the Records Center. [ ] [ ]

SIGNATURE – Andre Sivels, NOAA Records Officer — DATE

NATIONAL ARCHIVES AND RECORDS ADMINITRATION — OPTIONAL FORM 11 (Rev. 1-93)

REFERENCE SERVICES

- Properly completed requests are available for pickup, review or mailing with 24 hours (one business day) excluding weekends and holidays.
- Rush requests(filled in less than one business day) call 301-778-1520
- Additional charges apply to rush requests

Reference Service Cost

Service Type	Description	Unit of Measure	FY 11 Rate
Transfer Records	Processing	Per Transfer	$42.00
Transfer Box	Transfer of each box	Per transfer	$3.50
Disposition	Destroying Records	Per box	$5.75
Refile-Box	Cost of refiling whole box	Per box	$4.50
Refile- files	Cost of refilng individual files	Per file	$4.75
Interfiles	Filing record after transfer has occurred	Per file	$4.25
Photocopy	copies made	Per pages	$0.65
Reference -box	Requesting a box	Per box	$4.20
Reference -File	Requesting a file folder	per file folder	$4.75
Permanent Withdrawal	Sending box permanently to the agency	Per box	$4.30
Storage- per box	Cost of each box per month	Monthly	$0.21

Federal Records Centers

FRCs provide records storage services to Federal agencies.

FRC LOCATIONS

RECORDS SERVICING AREAS	FRC FACILITY	CONTACT NUMBER
Washington Metro Area	WNRC Suitland, MD	301-372-2925, ext 104
AL, FL, GA, KY, MS NC, SC, and TN	Atlanta, GA (Ellenwood, GA)	404-736-2820
CT ,ME, MA, NH, RI and VT	Boston, MA (Waltham, MA)	781-663-0130
IL, MN, WI, And Federal courts in IL, IN, MI, MN, OH, and WI	Chicago, IL	773) 948-9029
Ohio	Dayton, OH	937) 425-0606
CO(Rocky Mt. Region)	Denver, CO	(303) 407-5700
TX	Fort Worth, TX	817-551-2022
NJ, NY PR, the U.S. VI	Lee 's Summit, MO	816-268-8100
IA, KS, MO and NE	Lenexa, KS	913-563-7600
Ohio	Miamisburg, OH	(937) 425-0601
PA, DE, WV, MD and VA	Philadelphia, PA	215-305-2000
Massachusetts	Pittsfield MA	413-236-3600
AZ, Southern CA and Clark County, Nevada.	Riverside, CA(Perris CA)	(951) 956-2000
Northern and Central CA, NV (except Clark County), HI, American Samoa and the Trust Territory of the Pacific Islands,	San Francisco(San Bruno, CA	(650) 238-3500
ID, OR and WA	Seattle, WA	206-336-5145
Nationwide- Personnel Records	St. Louis, MO	314-801-0800

NOAA Records Management Contacts

Agency Records Officer — Andre Sivels 301-713-3540, ext 213

Records Liaisons Coordinators

• Charles McLeod	Offices of the Under Secretary, Assistant Secretary, Deputy Under Secretary, and Chief of Staff , 202-482-3436
• Gina Jackson	Office of General Counsel , 202-482-4080
• Nicky McClurkin	Office of Communications, 202-482-9184
• Lydia Kenlaw	Office of the Chief Administrative Officer, 301-713-0836 x 184
• Rose Fleming	Office of the Chief Financial Officer, 202-482-0917
• Jeremy Andrucyk	Office of the Acquisition and Grants, 301-713-2037
• Sarah Brabson	Office of the Chief Information Officer, 301-713-628-5751
• Tim Bagley	Legislative Affairs, 202-482-4666
• Nancy Jackson	Office of Marine and Aviation Operations (OMAO), 301-713-7616
• Maria Buie	Office of Workforce Management, 301-713-6305
• Tejuana Hickerson	Office of Program Analysis and Evaluation, 301-713-1622 x 191
• Donna Idlet	Office of Education, 202-482-1046
• Russell C. Jones	National Ocean Service, 301-713-3074 x 177
• Mike Justen	National Marine Fisheries Service, 301-713-1364 x 147
• David Murray	National Weather Service, 301-713-1698 x 119
• Brian J. Brown	National Environmental Satellite, Data, and Information Services, 301-713-9230
• Nicholas Leivers	Oceanic and Atmospheric Research, 301-713-1134
• Tejuana Hickerson	Program Planning and Integration , 301-713-1622 x 191
• Erin McNamara	Office of the Federal Coordinator for Meteorology, 301-427-2002 x 13

Tracking Records at FRCs (cont'd.)

NOTICE OF ACCESSION LOCATION CHANGE

THE RECORDS DESCRIBED IN THIS NOTICE HAVE BEEN RELOCATED WITHIN THE CENTER. PLEASE NOTE THIS CHANGE ON YOUR SF-135, AS THIS NEW LOCATION MUST BE FURNISHED WITH ANY REQUEST FOR RECORDS FROM THIS ACCESSION.

REMARKS

DATE OF NOTICE	NEW LOCATION
RECORDS DESCRIPTION	
ACCESSION NUMBER	SUBGROUP
DISPOSAL AUTHORITY	VOLUME (Cu. ft.)
SERIES DESCRIPTION	

OF FEDERAL RECORDS CENTER

NA FORM 13016 (1-93)

RECORDS TRANSMITTAL AND RECEIPT — Complete and send original and two copies of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse. PAGE 1 OF PAGES

1. TO (Complete the address for the records center serving your area as shown in 36 CFR 1228.150): Federal Records Center
Bldg 48, DFC
Denver, CO 80225

2. AGENCY TRANSFER AUTHORIZATION — TRANSFERRING AGENCY OFFICIAL (Signature and title): JANE JONES (Director) — DATE

3. AGENCY CONTACT — TRANSFERRING AGENCY LIAISON OFFICIAL (Name, office and telephone No.): John Smith, Property, 555-356-6789

4. RECORDS CENTER RECEIPT — RECORDS RECEIVED BY (Signature and title) — DATE

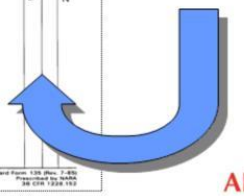
5. FROM (Enter the name and complete mailing address of the office retiring the records. The signed receipt of this form will be sent to this address):
Bureau of Public Recreation
Eastern Regional Office
12345 Exercise Road
Reston, VA 01113

Fold Line

6. **RECORDS DATA**

ACCESSION NUMBER: RG	FY	NUMBER	VOLUME (Cu. Ft.)	AGENCY BOX NUMBERS	SERIES DESCRIPTION (With inclusive dates of records)	RETENTION PERIOD	DISPOSAL AUTHORITY (Schedule and item number)	DISPOSAL DATE	COMPLETED BY RECORDS CENTER: LOCATION	DISP AUTH TYPE	DISP CODE
700	99	0023	6	1-6	ADVISORY COMMISSION FILES Closed FY 1999	R	N1-700-98-1 Item 202	P/2024	206758	B	A N

NSN 7540-00-634-4093 — 135-107 — Standard Form 135 (Rev. 7-93) Prescribed by NARA 36 CFR 1228.152



ARCIS Archives and Records Centers Information System

NARA's Federal Records Centers

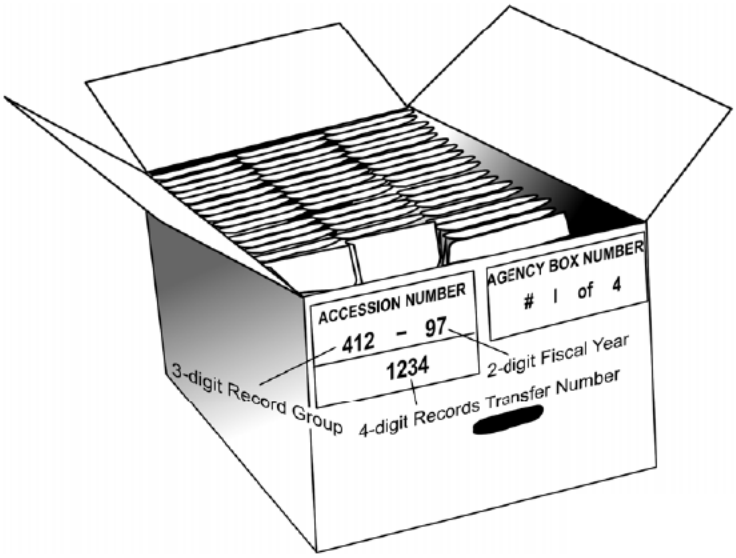
- NARA is authorized by law to establish, maintain, and operate records centers for Federal agencies.
- The Department of Commerce pays for the storage of all DOC records, including NOAA's.
- Information about NARA's FRCs is available through NARA's FRC web site: www.archives.gov/frc

Additional Information Contact

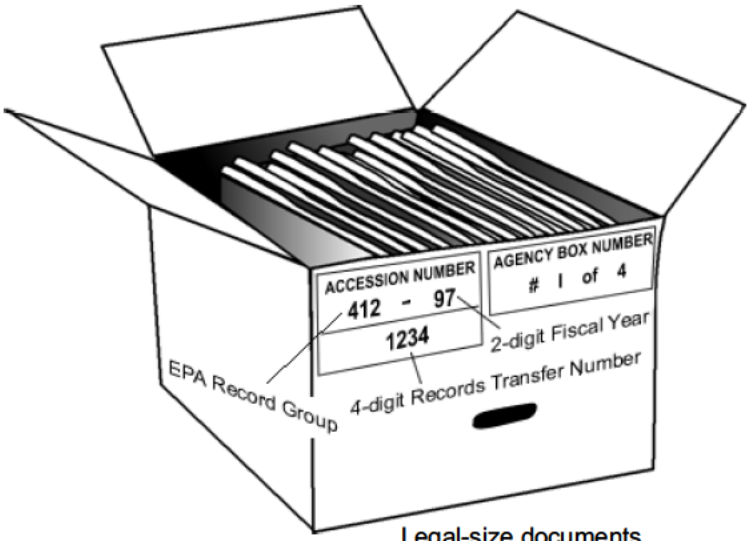
- Andre Sivels, Agency Records Officer 301-713-3540, ext 213
- Your Records Liaison Officer
- http://www.archives.gov/frc/forms/sf-135-intro.html

QUESTIONS

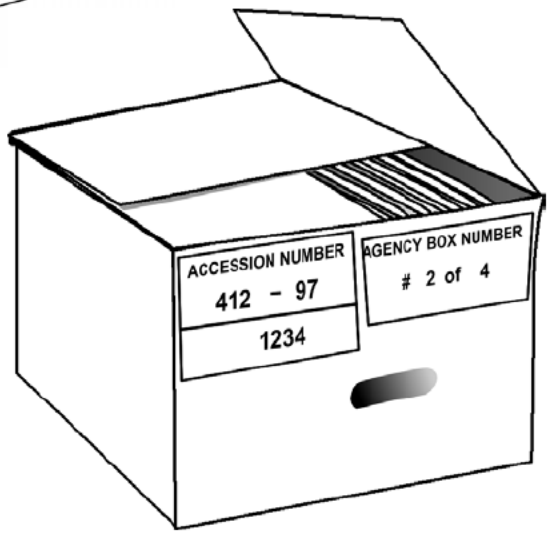
Records Retirement Box



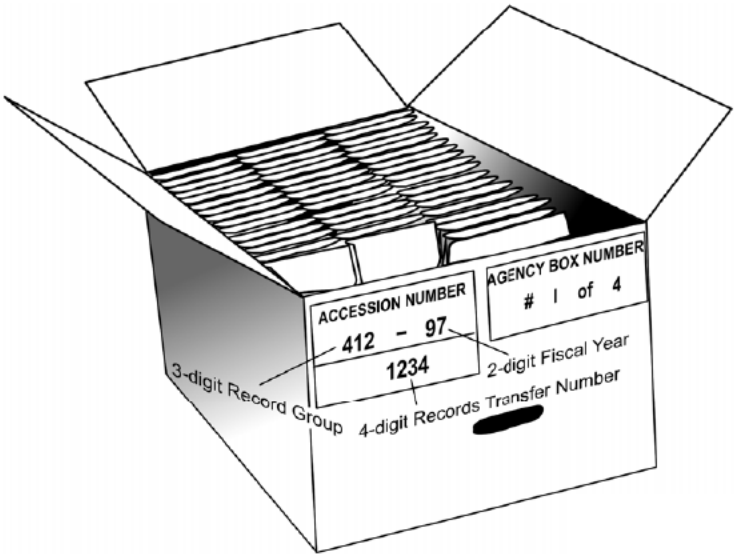
Letter-Size Documents



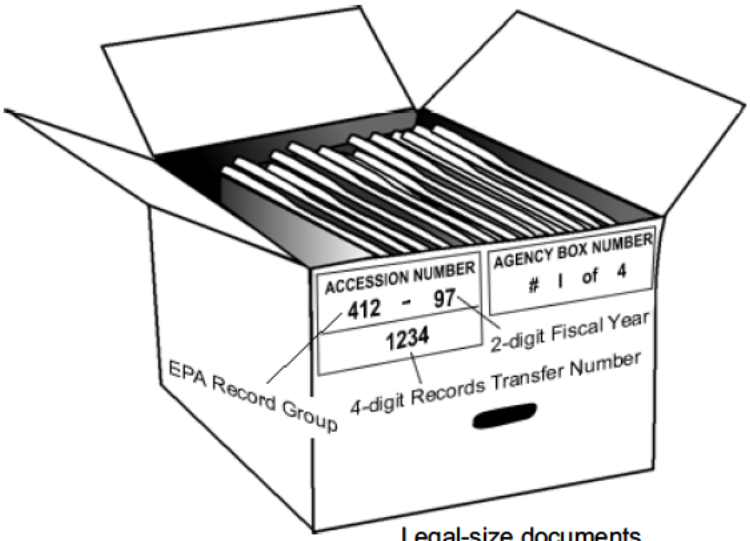
Legal-size documents



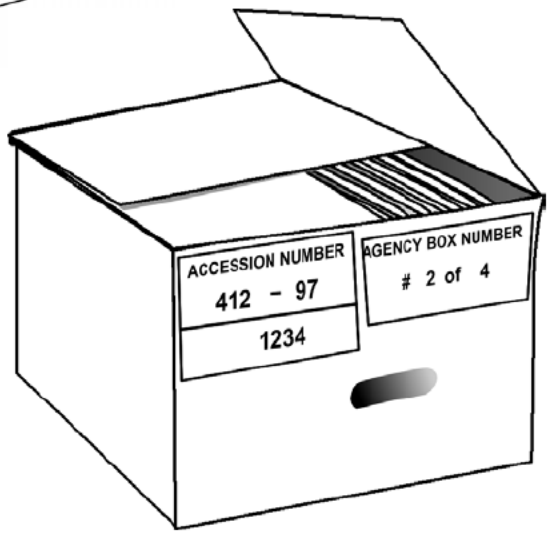
Records Retirement Box



Letter-Size Documents



Legal-size documents



Agricultural Research Service
U.S. Department of Agriculture

Accession 310-98-0004

Flies Closed November 1995

Box 1

AM 100.1	Compliance of ARS with the Animal Welfare Act
AM 100.2	Organization Changes
AM 100.3	Position Management
AM 105.2	Delegations of Authority
AM 110.6	ARS International Programs
AM 130.3	Human Metabolic Unit
AM 130.5	Research Assessment Committee: Pesticide Impact Assessment
AM 150.1	Dissemination of Public Information by ARS
AM 150.6	Manuscript Clearance Procedures for Publishing in Non-USDA Media
AM 150.7	Outside (Non-USDA) Publishing
AM 175.2	USDA Alphabetical and Organizational Lists

Box 2

AM 240.6	Pollution Abatement at ARS Facilities
AM 252.4	For Official Use Only Material
AM 510.5	Program Reports in ARS
AM 520.2	Approval of Proposed Projects
AM 545	Sponsored Research
AM 905	Releasing Plant Germ Plasm
AM 910	National Agricultural Pesticide Impact Assessment Program

Page 1 of 1

Figure 3-2. Sample Box and Folder List for Permanent Records

RECORDS TRANSMITTAL AND RECEIPT

Complete and send original and one copy of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse.

PAGE **1** OF 1 PAGES

1 TO *(Complete the address for the records center serving your area as shown in 36 CFR 1228.150.)*

Federal Records Center
Washington National Records Center (WNRC)
4205 Suitland Road,
Suitland, MD 20746-8001

5 FROM *(Enter the name and complete mailing address of the office retiring the records. The signed receipt of this form will be sent to this address.)*

Andre Sivels, Records Officer
National Oceanic and Atmospheric Administration
1315 East West Highway
SSMC3 Room 10632
Silver Spring, MD 20910

2	AGENCY TRANSFER AUTHOR-IZATION	TRANSFERRING AGENCY OFFICIAL *(signature and title)* Andre Sivels 301-713-3540 x213 NOAA Records Officer Andre .Sivels @noaa.gov	DATE 1/8/09
3	AGENCY CONTACT	TRANSFERRING AGENCY LIAISON OFFICIAL (*Name, office and telephone No)* Mary Doe – SSMC2 – RM xxxx 301-713-xxxx, etc xxx	
4	RECORDS CENTER RECEIPT	RECORDS RECEIVED BY (*Signature and Title)*	DATE

Fold Line

6 **RECORDS DATA**

ACCESSION NUMBER			VOLUME *(cu. ft.)*	AGENCY BOX NUMBERS	SERIES DESCRIPTION *(with inclusive dates of records)*	RESTRIC-TION	DISPOSAL AUTHORITY *(schedule and item number)*	DISPOSAL DATE	COMPLETED BY RECORDS CENTER			
RG	FY	NUMBER							LOCATION	SHELF PLAN	CONT TYPE	AUTO DISP
(a)	*(b)*	*(c)*	*(d)*	*(e)*	*(f)*	*(g)*	*(h)*	*(i)*	*(j)*	*(k)*	*(l)*	*(m)*
370	11	001	8	1 8	Travel Files (FY 09)	NA	403 15	1/2016				

REFERENCE REQUESTS - FEDERAL RECORDS CENTERS

NOTE: Use a separate form for each request.

SECTION I - TO BE COMPLETED BY REQUESTING AGENCY

ACCESSION NO.	AGENCY BOX NUMBER	RECORDS CENTER LOCATION
370-03-0057	**57**	Washington National Records Center Suitland, Maryland

DESCRIPTION OF RECORD(S) OR INFORMATION REQUESTED

[X] BOX

[ ] FOLDER (include file number and title)

REMARKS

NATURE OF SERVICE

[ ] FURNISH COPY OF RECORD (S) ONLY [ ] PERMANENT WITHDRAWAL [X] TEMPORARY LOAN OF RECORD(S)

[ ] REVIEW [ ] OTHER *(Specify)*

SECTION II - FOR USE BY RECORDS CENTER

[ ] RECORDS NOT IN CENTER CUSTODY

[ ] WRONG ACCESSION NUMBER PLEASE RECHECK

[ ] WRONG BOX NUMBER PLEASE RECHECK

[ ] WRONG CENTER LOCATION PLEASE RECHECK

[ ] ADDITIONAL INFORMATION REQUIRED TO IDENTIFY RECORDS REQUESTED

[ ] MISSING *(Neither record(s), information nor charge card found in container(s) specified)*

[ ] RECORDS DESTROYED

[ ] RECORDS PREVIOUSLY CHARGED OUT TO *(Name, agency and date):*

REMARKS

DATE	SERVICE	TIME REQUIRED	SEARCHER'S INITIALS

SECTION III - TO BE COMPLETED BY REQUESTING AGENCY

NAME OF REQUESTOR	TELEPHONE NO.	DATE	**RECEIPT OF RECORDS**
Mary Doe NOAA Routing Code: OFA62	301-713-xxxx,	1/12/09	

NAME AND ADDRESS OF AGNECY

National Oceanic and Atmospheric Administration (NOAA)
1325 East West Highway
Room: 9362
Building: SSMC2
Silver Spring, MD 20910

Requestor please sign, date and return this form, for file item(s) listed above, ONLY if the block to the right has been checked by the Records Center. [ ]

SIGNATURE Andre Sivels
NOAA Records Officer

DATE

RECORDS TRANSMITTAL AND RECEIPT

Complete and send original and two copies of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse.

PAGE 1 OF PAGES

1. TO *(Complete the address for the records center serving your area as shown in 36 CFR 1228.150.)*

Federal Records Center

5. FROM *(Enter the name and complete mailing address of the office retiring the records. The signed receipt of this form will be sent to this address)*

Mark Graff, FIOA Officer
NOAA-OCIO
9th Floor
1315 East-West Highway
Silver Spring, MD 20910

2. AGENCY TRANSFER AUTHORIZATION	TRANSFERRING AGENCY OFFICIAL *(Signature and title)* Andre Sivels, RO	DATE 02/14/2018
3. AGENCY CONTACT	TRANSFERRING AGENCY LIAISON OFFICIAL *(Name, office and telephone No.)* Sarah Brabson, RLO	
4. RECORDS CENTER RECEIPT	RECORDS RECEIVED BY *(Signature and title)*	DATE

Fold Line ◄

6. **RECORDS DATA**

ACCESSION NUMBER RG (a)	FY (b)	NUMBER (c)	VOLUME *(cu. ft.)* (d)	AGENCY BOX NUMBERS (e)	SERIES DESCRIPTION *(With inclusive dates of records)* (f)	RESTRICTION (g)	DISPOSAL AUTHORITY *(Schedule and item number)* (h)	DISPOSAL DATE (i)	COMPLETED BY RECORDS CENTER LOCATION (j)	SHELF PLAN (k)	CONT. TYPE (l)	AUTO. DISP. (m)
370	18	xxxx	30	1-30	Access and Disclosure Request Files (10/1/2013-9/30/2016		DAA-GRS-2016-0002-0001	10/1/22				

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, February 16, 2018 10:24 AM
To:	Mark Graff NOAA Federal
Subject:	Two NWS PTAs for signature
Attachments:	NOAA8102 PTA 02152018.pdf; NOAA8106 PTA November 2017(1).pdf

Mark, attached are NOAA8102 and NOAA8106 PTAs. I had recently contacted NWS when I realized the PTA had been "circulating for signatures" since November. That's why it's in the old template, but it won't be going to DOC as no PII.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, February 16, 2018 1:35 PM
To:	Toland, Michael; PrivacyAct; Gitelman, Steve (Contractor)
Cc:	Mark Graff NOAA Federal
Subject:	NOAA 21 SORN in new template
Attachments:	NOAA 21 SORN in new template.docx

Mike et al The only change is the addition of the newest breach routine use. This program does not use volunteers.

Thanks, Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Douglas Perry - NOAA Federal

From:	Douglas Perry NOAA Federal
Sent:	Friday, February 16, 2018 2:32 PM
To:	Jean Apedo NOAA Federal
Cc:	Ann Madden NOAA Federal; Sarah Brabson NOAA Federal; Mark Graff
Subject:	Re: Completed: Signed by ISSO: NOAA0900 2018 PIA and PTA
Attachments:	NOAA0900 PTA 2018 approved.pdf; NOAA0900 052317 for new signatures_2018 certification.pdf

Jean,
See signed attachments.

On Thu, Feb 8, 2018 at 8:59 AM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:

> Good morning Doug,
>
> Attached are NIOAA0900 PTA and PIA for your review.
>
> Thank you.
>
> **From:** Ann Madden NOAA Federal [mailto:ann.madden@noaa.gov]
> **Sent:** Thursday, February 08, 2018 8:34 AM
> **To:** Jean Apedo NOAA Federal
> **Cc:** Sarah Brabson
> **Subject:** Fwd: Completed: Signed by ISSO: NOAA0900 2018 PIA and PTA
>
> Jean
>
> Can you please review and sign? I can get them to Doug next.
>
> Thanks
>
> Ann
>
> Forwarded message
> From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
> Date: Wed, Feb 7, 2018 at 10:50 AM
> Subject: Fwd: Completed: Signed by ISSO: NOAA0900 2018 PIA and PTA
> To: Ann Rivers <Ann.Madden@noaa.gov>

Doug

~~~~~~

Douglas A. Perry

Deputy Chief Information Officer
National Oceanic and Atmospheric Administration

Office: (301) 713-9600

www.noaa.gov
~~~~~~

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, February 16, 2018 2:42 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA0900 re signed PIA and new PTA for certilfication
Attachments:	NOAA0900 PTA 2018 approved.pdf; NOAA0900 052317 for new signatures_2018 certification.pdf

Mark, please sign thx. I haven't signed the certification yet, pending SK's update on controls.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, February 21, 2018 8:04 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Two NWS PTAs for signature
Attachments:	NOAA8106 PTA November 2017(1) mhg.pdf; NOAA8102 PTA 02152018 mhg.pdf

Got it here you go. Are all the other PTAs and PIAs going to be in the new format, then, or are there a few stragglers that will still be in the old format?

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Fri, Feb 16, 2018 at 10:24 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, attached are NOAA8102 and NOAA8106 PTAs. I had recently contacted NWS when I realized the PTA had been "circulating for signatures" since November. That's why it's in the old template, but it won't be going to DOC as no PII.
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Version Number: 01-2017

U.S. Department of Commerce
NOAA/NWS

Privacy Threshold Analysis
for the
Automated Surface Observing System

U.S. Department of Commerce Privacy Threshold Analysis

Automated Surface Observing System

Unique Project Identifier: 006-48-01-12-01-3123-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The Automated Surface Observing System (ASOS) Operation and Maintenance (O&M) program directly supports NOAA's Strategic Goals to: 1- Serve Society's Needs for Weather and Water; and 2 - Support the Nation's Commerce with Information for Safe, Efficient, and Environmentally Sound Transportation. ASOS directly supports improvements to NWS GPRA measures as the primary system providing real-time surface observations for the initialization and validation of NWS forecast and warning products. The GPRA measure is: Weather and Water Goal/Local Forecast and Warning Program ASOS availability. The Automated Surface Observing Systems (ASOS) program is a joint effort of NOAA's National Weather Service (NWS), the Federal Aviation Administration (FAA), and the Department of Defense (DOD). There are 571 FAA-sponsored, 313 NWS-sponsored and 110 DOD-sponsored ASOSs, mainly located at airports in the National Airspace System (NAS) and at airports operated under the DOD. ASOS is the nation's primary surface weather observing network. ASOS supports NWS forecasting and warning activities, FAA's aviation operations, and the needs of the meteorological, hydrological, and climatologically research communities. The ASOS program is in the O&M phase with a product improvement program that focuses on sensor improvements. There is no replacement for ASOS planned within NOAA. ASOS sustainment activities, including technology refresh of the ASOS IT infrastructure is planned and required to satisfy IT security requirements, FAA Next Generation 4-D Weather Cube requirements, and user needs for higher resolution data.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

X No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

X No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

X No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

X No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

X No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the Automated Surface Observing System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

X I certify the criteria implied by the questions above **do not apply** to the Automated Surface Observing System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Mason Oliver

Signature of ISSO or SO: OLIVER.MASON.MICHAEL ALAN.1458085117 Digitally signed by OLIVER.MASON.MICHAEL ALAN.1458085117 Date: 2018.02.15 11:16:40 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.02.15 10:30:24 -10'00' Date: _____

Name of Authorizing Official (AO): Joseph Pica

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2018.02.16 09:53:41 05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892 Date 2018 02 21 07 59 01 05'00' Date: _____

Version Number: 01-2015

U.S. Department of Commerce
NOAA/NWS

Privacy Threshold Analysis
for the
Upper Air Observing System
(UAOS) NOAA8106

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NWS, Office of Observations
Upper Air Observing System (UAOS)

Unique Project Identifier: NOAA8106

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
Upper Air Observing Systems (UAOS) is a major application. UAOS supports the NWS mission for providing weather, hydrologic, climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, and for the protection of life and property and the enhancement of the national economy. The NWS data and products form a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. The national information database and infrastructure are not located within the UAOS system boundary.

UAOS provides NWS with environmental sounding measurements from balloon-borne radiosondes, small units containing temperature, humidity, and pressure sensors, as well as Global Positioning System (GPS) receivers, measurements which are transmitted back to a system on the ground for further processing into sounding observation products. The movement of the radiosonde is tracked to infer the wind direction and speed profiles throughout different levels of the atmosphere using differential GPS. The radiosondes are launched twice daily at 92 NWS managed locations across the United States and its territories.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

X No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552 (b) (4)). This information is exempt from automatic release under the (b) (4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies

____ Other business entities

X No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

X No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

____ I certify the criteria implied by one or more of the questions above **apply** to UAOS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

X I certify the criteria implied by the questions above **do not apply** to UAOS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Timika Bobb

Signature of ISSO or SO: BOBB.TIMIKA.L.1288251459 Digitally signed by BOBB.TIMIKA.L.1288251459 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=CONTRACTOR, cn=BOBB.TIMIKA.L.1288251459 Date: 2017.11.21 14:29:39 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.01.18 10:14:02 -05'00' Date: _____

Name of Authorizing Official (AO): Joseph Pica

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2018.02.16 10:00:09 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.21 08:02:46 -05'00' Date: _____

Toland, Michael (Federal)

From:	Toland, Michael (Federal)
Sent:	Tuesday, February 20, 2018 2:37 PM
To:	Arnold, Josephine (Federal); Brabson, Sarah (Federal); Cash, Angenette; Curry, Vernon E; Daniel, Tiffany; Fletcher, Catherine; Graff, Mark (Federal); Green, Wade; Hitt, Lucas; Jaramillo, Edwina Martha; Klemmer, Richard; Kong, Stephen (Federal); Lynch, Heather; Owens II, John; Pardun, John; Piel, Jennifer; Pilot, Adrienne; Reinhart, Liz; Staunton, Dondi; Townsend, Janice; Bachman, Robin J; Berg, Robin; Brockett, Del; Callahan, Brian; Crenshaw, Byron; Glenn, K. Robert; Kang, Shine; Mix, Ida; Moses, Sandranette (Federal); Moulder, Pamela (Federal); Pham, Toan; Rose, Carol; Schiller, Susannah B.; Schmidt, Carolyn M.; Swisher, Robert (Federal)
Cc:	Gitelman, Steve (Contractor)
Subject:	Data Call: Comments to SORN Commerce/DEPT 18: due March 13, 2018
Attachments:	DEPT 18 _revised draft 17 11 15_OPOG Comments.docx

Dear Bureau Privacy Act and Chief Privacy Officers:

DUE DATE: on or before March 13, 2018.

As we have been discussing during past Privacy Council meetings, OPOG is in the process of working with you and other program offices on updating not only your system of records notices (SORNs), but Department-wide SORNs, as well. We are starting with COMMERCE/DEPT-18, "Employees Personnel Files Not Covered by Notices of Other Agencies." Please review the attached draft SORN and update it as needed for your specific missions. Sections that we ask you to pay attention to include:

- System Location;
- System Manager(s);
- Purpose(s) of the System;
- Categories of Individuals Covered by the System;
- Categories of Records in the System; and
- Notification Procedures.

Please also feel free to include other comments or edits, as needed. We have turned on MS Word's Track Changes Feature so that we can track your comments and suggested edits.

Please contact Steve Gitelman, 202-482-8294 or sgitelman@doc.gov should you have any questions or need additional information.

Regards,

Mike

Michael J. Toland, Ph.D.
Deputy Chief FOIA Officer,
Departmental FOIA Public Liaison Officer,

Departmental Privacy Act Officer, and
Deputy Director FOIA/Privacy Act Operations
U.S. Department of Commerce
Office of Privacy and Open Government
Office: (202) 482-3842
Email: mtoland@doc.gov

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, February 21, 2018 9:18 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA0900 re signed PIA and new PTA for certilfication
Attachments:	NOAA0900 052317 for new signatures_2018 certification mhg.pdf; NOAA0900 PTA 2018 approved mhg.pdf

Both look good signed contingent on certification and SAR review. However, this appears to be the old template. I thought Kathy/Catrina indicated she wouldn't be accepting any more 2015 templates, even for re certifications, during the last CRB.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Fri, Feb 16, 2018 at 2:41 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, please sign thx. I haven't signed the certification yet, pending SK's update on controls.
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA0900
NOAA Emergency Notification System (NOAA ENS)

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NOAA ENS (0900)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

National Oceanic and Atmospheric Administration (NOAA) is committed to emergency preparedness, including communicating with NOAA staff prior to, during, and after an all-hazards or emergency events. NOAA's Emergency Notification System (ENS) is a commercial cloud-based application by which designated NOAA persons can quickly broadcast emergency alerts to NOAA staff via phone, text, and email. It provides NOAA staff with consistent event specific information and direction, and ability to account for staff in the aftermath thereof. The information in the system is obtained from the NOAA Staff Directory (NSD) and consists of: name, work phone number, work cell phone number, work email address, and work mailing address. In addition, NOAA staff may choose to enter their personal mobile phone number and personal email address into the NSD for upload to the NOAA ENS. There is no information sharing outside of NOAA other than if contact information is needed for a privacy incident response.

The cloud-based application is owned by Everbridge, Inc. The locations are Amazon Web Services West region: Burbank, California and Denver, Colorado.

The authority for the collection of this data is Federal Continuity Directive 1, Code of Federal Regulations, Title 41, Chapter 102 Federal Management Regulation (FMR), Part 102-74 (41 CFR §102-74.230 - 102-74.260), DOC's Departmental Organizational Order (DOO) 20-6, and guidance provided by DOC's Manual of Security Policies and Procedures, Chapter 7.

This is a moderate impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System		f. Commercial Sources		i. Alteration in Character	

Management Changes				of Data	
j. Other changes that create new privacy risks (specify):					

_X__ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): communicating with NOAA staff prior to, during, and after an all-hazards or emergency events.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NOAA ENS is a cloud-based, software-as-a-service, vendor-hosted mass notification system that provides tools for reaching pre-defined contacts during an emergency situation. The purpose of the Emergency Notification System is to simplify management of emergency communication processes and procedures quickly and easily to communicate with all employees, Associates and visitors. This system is designed to help respond in a fast and decisive way during emergency situations. The multi-modal communications system, including phone, text, email, pagers, and more, allows NOAA to rapidly and efficiently reach our staff wherever they are. This ensures the life safety and security of all staff (including contractors) during emergencies.

The data collected contains personally identifiable information (PII) obtained from the NOAA Staff Directory (employees and contractors) and/or disclosed by the end-user for contacting in the case of emergency situations.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of a privacy breach

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA0201, which contains the NOAA staff directory. *There is no direct connection: the data is loaded onto a server, and downloaded by ENS.*

	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.homelandsecurity.noaa.gov/ (bottom left of page). There is also a link to it on ENS's page after logging in, but that is not accessible except to ENS users. You can request the log-in screen from this page: https://manager.everbridge.net/saml/login/NOAA but you will not be able to log in, of course. I have sent a screenshot of the page in the cover email.	
X	Yes, notice is provided by other means.	Specify how: Notice is provided to client users when they provide optional information to the NOAA Lightweight Directory Access Protocol (staff directory). There is a warning notice on the page on which information is submitted.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Work related PII is automatically uploaded to the system from the staff directory; however, personal PII, e.g. personal cell phone number, is optional.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Users are presented with the options on the staff directory (LDAP) screen where data is optionally entered. The only uses for the information in the staff directory are for contacting staff routinely, or once the info is in ENS, for contacting staff by ENS in emergencies.
	No, individuals do not have an	Specify why not:

	opportunity to consent to particular uses of their PII/BII.	

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users are presented with the options on the staff directory (LDAP) screen where data is optionally entered. This update reminder is displayed upon system entry for any purpose.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: System user account access is tracked.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 6/17/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access is restricted, requiring authorized users, those with a "need to know", to log in. Account access is tracked. Information from the NOAA Staff Directory is uploaded to a server and downloaded by ENS, rather than having a direct connection.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: Yes, this system is covered by an existing system of records notice. Provide the system name and number: DEPT-18: Employees' personnel files not covered by notices of other agencies. That is, the information in this system is a subset of that information.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: There is an approved record control schedule. "Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use." from http://www.corporateservices.noaa.gov/audit/records management/schedules/index.html , Chapter 200-12.
	No, there is not an approved record control schedule.

	Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified.
X	Quantity of PII	Provide explanation: PII is limited to contact information.
X	Data Field Sensitivity	Provide explanation: There is no sensitive PII collected.
X	Context of Use	Provide explanation: ENS is used for emergency contact/notification purpose only.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Restricted access to LDAP server (authentication log in) and ENS use.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: SK Bhachech Office: Everbridge Phone: +1.781.373.9866 Email: sk.bhachech@everbridge.com I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DocuSigned by: [signature] 8191C42CF98D4D7... Date signed: 2/7/2018	**Information Technology Security Officer** Name: Jean Apedo Office: NOAA OCIO/ITSEC Phone: 301.628.5730 Email: jean.apedo@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: APEDO.JEAN.1188076064 Digitally signed by APEDO.JEAN.1188076064 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn APEDO.JEAN.1188076064 Date: 2018.02.08 08:56:42 -05'00' Date signed:
Authorizing Official Name: Douglas Perry Office: NOAA OCIO Phone: 301.713.9600 Email: zachary.goldstein@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.02.16 14:29:07 05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.21 09:16:42 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Emergency Notification System

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Emergency Notification System

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) *Whether it is a general support system, major application, or other type of system:* NOAA's Emergency Notification System (ENS) is a commercial cloud-based application by which designated NOAA persons can quickly broadcast emergency alerts to NOAA staff via phone, text, and email. It provides NOAA staff with consistent event specific information and direction, and ability to account for staff in the aftermath thereof. The information in the system is obtained from the NOAA Staff Directory (NSD) and consists of: name, work phone number, work cell phone number, work email address, and work mailing address. In addition, NOAA staff may choose to enter their personal mobile phone number and personal email address into the NSD for upload to the NOAA ENS. There is no information sharing outside of NOAA other than if contact information is needed for a privacy incident response.

b) *System location:* Silver Spring MD.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects) This is a standalone system, to which bulk uploads are made from the NOAA Staff Directory.

d) The purpose that the system is designed to serve: This is a system by which NOAA persons can quickly broadcast emergency alerts to NOAA staff via phone, text, and email. It provides NOAA staff with consistent event specific information and direction, and ability to account for staff in the aftermath thereof.

e) *The way the system operates to achieve the purpose:* Using the staff directory information, the ENS sends out emergency broadcasts to staff work contact information.

f) A general description of the type of information collected, maintained, use, or disseminated by the system: Name, work phone number, work cell phone number, work email address, and work mailing address.

g) Identify individuals who have access to information on the system: Access is restricted, requiring authorized users, those with a "need to know", to log in. These include system staff and contractors.

h) How information in the system is retrieved by the user: Information from the NOAA Staff Directory is uploaded to a server and downloaded by ENS, where it is accessed by authorized personnel in order to deliver notifications.

i) How information is transmitted to and from the system: Information is uploaded from the Staff Directory and alerts are sent out to NOAA staff and contractors by the system.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

___X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X___ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X___ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

____X_ I certify the criteria implied by one or more of the questions above **apply** to the NOAA0900 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): ISSO: SK Bhachech

Signature of ISSO or SO: DocuSigned by: 8191C42EF98D4D7... Date: 2/7/2018

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: APEDO.JEAN.1188076064 Digitally signed by APEDO.JEAN.1188076064 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn APEDO.JEAN.1188076064 Date: 2018.02.08 08:58:22 05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.02.16 14:31:02 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.21 09:15:30 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, February 21, 2018 10:45 AM
To:	Mark Graff NOAA Federal
Subject:	Fwd: NOAA0900 Certification Documents
Attachments:	NOAA0900 Annual Review Certification Form_for MHG signature mhg.pdf; NOAA0900 052317 PIA for new signatures_2018 certification mhg.pdf; NOAA0900 PTA 2018 approved mhg.pdf

Forgot to cc you.

Forwarded message
From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Wed, Feb 21, 2018 at 10:44 AM
Subject: NOAA0900 Certification Documents
To: CPO <CPO@doc.gov>, "Purvis, Catrina" <CPurvis@doc.gov>, "Martin, Lisa" <LMartin1@doc.gov>, "Toland, Michael" <MToland@doc.gov>, "Ferguson, Dorrie" <dFerguson@doc.gov>

All I had told Kathy that this certification would not be available till this week as it took some time to obtain current POA&M updates from the contractor owned system. We are satisfied with what we received, and can now send the certification docs to you. Attached are the PTA, re signed and re ATO dated PIA (no other change) and certification.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA0900
NOAA Emergency Notification System (NOAA ENS)

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NOAA ENS (0900)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

National Oceanic and Atmospheric Administration (NOAA) is committed to emergency preparedness, including communicating with NOAA staff prior to, during, and after an all-hazards or emergency events. NOAA's Emergency Notification System (ENS) is a commercial cloud-based application by which designated NOAA persons can quickly broadcast emergency alerts to NOAA staff via phone, text, and email. It provides NOAA staff with consistent event specific information and direction, and ability to account for staff in the aftermath thereof. The information in the system is obtained from the NOAA Staff Directory (NSD) and consists of: name, work phone number, work cell phone number, work email address, and work mailing address. In addition, NOAA staff may choose to enter their personal mobile phone number and personal email address into the NSD for upload to the NOAA ENS. There is no information sharing outside of NOAA other than if contact information is needed for a privacy incident response.

The cloud-based application is owned by Everbridge, Inc. The locations are Amazon Web Services West region: Burbank, California and Denver, Colorado.

The authority for the collection of this data is Federal Continuity Directive 1, Code of Federal Regulations, Title 41, Chapter 102 Federal Management Regulation (FMR), Part 102-74 (41 CFR §102-74.230 - 102-74.260), DOC's Departmental Organizational Order (DOO) 20-6, and guidance provided by DOC's Manual of Security Policies and Procedures, Chapter 7.

This is a moderate impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System		f. Commercial Sources		i. Alteration in Character	

Management Changes				of Data	
j. Other changes that create new privacy risks (specify):					

_X__ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): communicating with NOAA staff prior to, during, and after an all-hazards or emergency events.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NOAA ENS is a cloud-based, software-as-a-service, vendor-hosted mass notification system that provides tools for reaching pre-defined contacts during an emergency situation. The purpose of the Emergency Notification System is to simplify management of emergency communication processes and procedures quickly and easily to communicate with all employees, Associates and visitors. This system is designed to help respond in a fast and decisive way during emergency situations. The multi-modal communications system, including phone, text, email, pagers, and more, allows NOAA to rapidly and efficiently reach our staff wherever they are. This ensures the life safety and security of all staff (including contractors) during emergencies.

The data collected contains personally identifiable information (PII) obtained from the NOAA Staff Directory (employees and contractors) and/or disclosed by the end-user for contacting in the case of emergency situations.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of a privacy breach

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA0201, which contains the NOAA staff directory. *There is no direct connection: the data is loaded onto a server, and downloaded by ENS.*

	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.homelandsecurity.noaa.gov/ (bottom left of page). There is also a link to it on ENS's page after logging in, but that is not accessible except to ENS users. You can request the log-in screen from this page: https://manager.everbridge.net/saml/login/NOAA but you will not be able to log in, of course. I have sent a screenshot of the page in the cover email.	
X	Yes, notice is provided by other means.	Specify how: Notice is provided to client users when they provide optional information to the NOAA Lightweight Directory Access Protocol (staff directory). There is a warning notice on the page on which information is submitted.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Work related PII is automatically uploaded to the system from the staff directory; however, personal PII, e.g. personal cell phone number, is optional.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Users are presented with the options on the staff directory (LDAP) screen where data is optionally entered. The only uses for the information in the staff directory are for contacting staff routinely, or once the info is in ENS, for contacting staff by ENS in emergencies.
	No, individuals do not have an	Specify why not:

	opportunity to consent to particular uses of their PII/BII.	

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users are presented with the options on the staff directory (LDAP) screen where data is optionally entered. This update reminder is displayed upon system entry for any purpose.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: System user account access is tracked.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 6/17/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access is restricted, requiring authorized users, those with a "need to know", to log in. Account access is tracked. Information from the NOAA Staff Directory is uploaded to a server and downloaded by ENS, rather than having a direct connection.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: Yes, this system is covered by an existing system of records notice. Provide the system name and number: DEPT-18: Employees' personnel files not covered by notices of other agencies. That is, the information in this system is a subset of that information.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: There is an approved record control schedule. "Destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use." from http://www.corporateservices.noaa.gov/audit/records management/schedules/index.html , Chapter 200-12.
	No, there is not an approved record control schedule.

	Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified.
X	Quantity of PII	Provide explanation: PII is limited to contact information.
X	Data Field Sensitivity	Provide explanation: There is no sensitive PII collected.
X	Context of Use	Provide explanation: ENS is used for emergency contact/notification purpose only.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Restricted access to LDAP server (authentication log in) and ENS use.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: SK Bhachech Office: Everbridge Phone: +1.781.373.9866 Email: sk.bhachech@everbridge.com I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DocuSigned by: [signature] 8191C42CF98D4D7... Date signed: 2/7/2018	**Information Technology Security Officer** Name: Jean Apedo Office: NOAA OCIO/ITSEC Phone: 301.628.5730 Email: jean.apedo@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: APEDO.JEAN.1188076064 Digitally signed by APEDO.JEAN.1188076064 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn APEDO.JEAN.1188076064 Date: 2018.02.08 08:56:42 -05'00' Date signed:
Authorizing Official Name: Douglas Perry Office: NOAA OCIO Phone: 301.713.9600 Email: zachary.goldstein@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.02.16 14:29:07 05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.21 09:16:42 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA:__NOAA0900, Emergency Notification System_____

FISMA Name/ID (if different):

_____

Name of IT System/ Program Owner: ___Scott Burnett_____

Name of Information System Security Officer:_SK Bhachech_____

Name of Authorizing Official(s): Douglas Perry_____

Date of Last PIA Compliance Review Board (CRB): _____6 15 17_____
(This date must be within three (3) years.)

Date of PIA Review:_____2 8 18_____

Name of Reviewer: Captain Anne Lynch_____

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____Anne K. Lynch CAPT/NOAA_____

Date of Privacy Act (PA) Review: _____2/21/2018_____

Name of Reviewer: _Sarah Brabson_____

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488

Digitally signed by BRABSON.SARAH.1365710488
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BRABSON.SARAH.1365710488
Date: 2018.02.21 08:10:20 -05'00'

Date of BCPO Review: 2/21/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer:

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.02.21 10:12:45 -05'00'

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Emergency Notification System

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Emergency Notification System

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) *Whether it is a general support system, major application, or other type of system:* NOAA's Emergency Notification System (ENS) is a commercial cloud-based application by which designated NOAA persons can quickly broadcast emergency alerts to NOAA staff via phone, text, and email. It provides NOAA staff with consistent event specific information and direction, and ability to account for staff in the aftermath thereof. The information in the system is obtained from the NOAA Staff Directory (NSD) and consists of: name, work phone number, work cell phone number, work email address, and work mailing address. In addition, NOAA staff may choose to enter their personal mobile phone number and personal email address into the NSD for upload to the NOAA ENS. There is no information sharing outside of NOAA other than if contact information is needed for a privacy incident response.

b) *System location:* Silver Spring MD.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects) This is a standalone system, to which bulk uploads are made from the NOAA Staff Directory.

d) The purpose that the system is designed to serve: This is a system by which NOAA persons can quickly broadcast emergency alerts to NOAA staff via phone, text, and email. It provides NOAA staff with consistent event specific information and direction, and ability to account for staff in the aftermath thereof.

e) *The way the system operates to achieve the purpose:* Using the staff directory information, the ENS sends out emergency broadcasts to staff work contact information.

f) A general description of the type of information collected, maintained, use, or disseminated by the system: Name, work phone number, work cell phone number, work email address, and work mailing address.

g) Identify individuals who have access to information on the system: Access is restricted, requiring authorized users, those with a "need to know", to log in. These include system staff and contractors.

h) How information in the system is retrieved by the user: Information from the NOAA Staff Directory is uploaded to a server and downloaded by ENS, where it is accessed by authorized personnel in order to deliver notifications.

i) How information is transmitted to and from the system: Information is uploaded from the Staff Directory and alerts are sent out to NOAA staff and contractors by the system.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

___X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X___ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X___ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

____X_ I certify the criteria implied by one or more of the questions above **apply** to the NOAA0900 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): ISSO: SK Bhachech

Signature of ISSO or SO: DocuSigned by: 8191C42EF98D4D7... Date: 2/7/2018

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: APEDO.JEAN.1188076064 Digitally signed by APEDO.JEAN.1188076064 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn APEDO.JEAN.1188076064 Date: 2018.02.08 08:58:22 05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.02.16 14:31:02 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.21 09:15:30 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, February 22, 2018 4:29 PM
To:	Mark Graff NOAA Federal
Subject:	Here's the PTA . . .
Attachments:	NOAA8107 FY18 PTA.pdf

On Thu, Feb 22, 2018 at 4:28 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> thanks, Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, February 22, 2018 4:44 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Here's the PTA . . .
Attachments:	NOAA8107 FY18 PTA mhg.pdf

AWIPS is good. Love the non PII FISMA Systems.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Thu, Feb 22, 2018 at 4:28 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> On Thu, Feb 22, 2018 at 4:28 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> thanks, Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751

Ce (b)(6)

2/14/2018

U.S. Department of Commerce
National Oceanic and Atmospheric Administration
National Weather Service

Privacy Threshold Analysis
for the
Advanced Weather Interactive Processing System (AWIPS)
NOAA8107

U.S. Department of Commerce Privacy Threshold Analysis

Advanced Weather Interactive Processing System (AWIPS)

Unique Project Identifier: NOAA8107

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

AWIPS is an integrated suite of automated data-processing equipment that supports complex analysis, interactive processing, display of meteorological, hydrological, satellite, and radar data, and provides rapid dissemination of warnings and forecasts in a highly reliable manner. This system is used principally at NWS Weather Forecast Offices (WFO), River Forecast Centers (RFC), and National Centers for Environmental Prediction (NCEP) centers to support weather and hydrologic forecast and warning operations. AWIPS systems are located at over 170 of these sites across the United States and its territories.

AWIPS is considered a major application and a mission system within the National Weather Service. The system obtains data from NESDIS satellite feeds and National Center model data over established Weather Service networks, as well as locally acquired data at each field site (such as from weather balloons) and broadcasts this data via satellite to forecasters at field sites. Forecasters use AWIPS software on workstations at the field sites to analyze this data and generate weather forecasts and warnings that will be disseminated to the public (over other systems).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__X__ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

___X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the

submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X___ DOC employees
__X__ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

__X__ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the NOAA8107 AWIPS system and as a consequence of this applicability, I will perform and document a PIA for this IT system.

___X__ I certify the criteria implied by the questions above **do not apply** to the NOAA8107 AWIPS system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Julie Raugh

Signature of ISSO or SO: RAUGH.JULIE.LILES.1463520140 Digitally signed by RAUGH.JULIE.LILES.1463520140 Date: 2018.02.22 08:36:40 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): Andrew Browne / Paula Reis

Signature of ITSO: REIS.PAULA.1281289523 Digitally signed by REIS.PAULA.1281289523 Date: 2018.02.22 14:55:24 05'00' Date: _____

Name of Authorizing Official (AO): David Michaud

Signature of AO: MICHAUD.DAVID.L.1365815212 Digitally signed by MICHAUD.DAVID.L.1365815212 Date: 2018.02.22 09:05:55 05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892 DN: c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892 Date: 2018 02 22 16:43:30 05'00' Date: _____

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Friday, February 23, 2018 9:43 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Do you have a signed 2018 PTA for NOAA6301?
Attachments:	NOAA6301_PTA_2018 v2 mhg.pdf

Here you go this is the one I just signed last month, but yes it is still in the old template.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Fri, Feb 23, 2018 at 9:41 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> I have on the management tool that it was signed, bur cannot find a signed copy in my files or in an email to DOC plus it's in the old template.
>
> I am workng on yet another request to Catrina to sign the certification related PIA . . Kathy originally asked on the 9th and then I asked on Monday, since Kathy is on leave. The ISSO needs it for a FISMA audit.
>
> I thought I'd resend the docs, then realized I don't have a PTA signed by you. If you don't have one either, I'll forward to you. Then I can put it on the new template . .
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

Unique Project Identifier: 006-00-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The NOAA6301 National Centers for Coastal Ocean Science (NCCOS) Research Support System provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. NCCOS's mission is to provide coastal managers with scientific information and tools needed to balance society's environmental, social, and economic goals.

NCCOS is passionate about supporting NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:

·To deliver high quality science in a timely and consistent manner using productive and strong partnerships.

·To develop and maintain relevant research, long term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.

·To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.

·To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

The NOAA6301 system:

· provides support to the program areas which are responsible for conducting research in the areas of marine bio-toxins; eco-toxicology; forensics; biotechnology; marine mammal stranding and necropsies; risk analysis; DNA sequencing; and marine related viruses and pathogens;

· provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus - NCCOS Head Quarters (HQ), Center for

Sponsored Coastal Ocean Research (CSCOR), and Center for Coastal Monitoring and Assessment (CCMA); Beaufort, NC - Center for Coastal Fisheries and Habitat Research (CCFHR); Charleston, SC Center for Coastal Environmental Health and Biomolecular Research (CCEHBR) and Hollings Marine Laboratory (HML); and Oxford, MD Cooperative Oxford Laboratory (COL); Beaufort, NC (CCFHR); Charleston, SC (CCEHBRC and CHHR/HML); and Oxford, MD (CCEHBRO);

· provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, LAN and WAN, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services; and

· Provides continued service to the local area network (LAN) and the wide area network (WAN) connections for non-SSMC locations.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X__ This is an existing information system in which changes do not create new privacy risks.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
__X_ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X_ DOC employees
__X_ Contractors working on behalf of DOC
__X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X_ I certify the criteria implied by one or more of the questions above **apply** to the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

____ I certify the criteria implied by the questions above **do not apply** to the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Rohit Munjal

Signature of ISSO: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381 Date: 2018.01.05 09:43:16 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.17 14:18:00 05'00' Date: _____

Name of Authorizing Official (AO): Steven Thur

Signature of AO: Digitally signed by THUR.STEVEN.M.1365841299 Date: 2018.01.19 07:49:11 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.23 10:18:48 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, February 23, 2018 10:13 AM
To:	Purvis, Catrina; CPO
Cc:	Gioffre, Kathy (Federal); Mark Graff NOAA Federal
Subject:	Re: Requesting signature on NOAA6301 PIA submitted with certification
Attachments:	NOAA6301 PTA 2018 mhg.pdf; NOAA6301_PIA_2018 v3 mhg.pdf; NOAA6301_PIA_Annual_Review_Certification_2018 mhg v2.pdf

Hi, Catrina, if you have a few minutes, could you at least review and sign the NOAA6301 PIA associated with the certification? Here are the docs again. No changes to the PIA except the ATO date.

thx Sarah

On Tue, Feb 20, 2018 at 8:27 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Hi, Catrina, Kathy said she sent you the subject item for signature on February 9. I'm contacting you directly since she is now on leave. This specific signature request is based on NOAA6301's having been selected by NOAA OCIO for a compliance review by the NOAA FISMA Team, prior to the ATO renewal. Rohit Munjal, the ISSO would need the signed PIA as soon as possible for upload into CSAM.
>
> As you may recall, all of NOS's ATO dates are toward the end of March, so if Kathy has sent you any other NOS certifications for review and signature, could you please sign those also and send to me? The others are NOAA6101, NOAA6205 and NOAA6501.
>
> Thanks, Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2017

U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the
National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

Unique Project Identifier: 006-00-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The NOAA6301 National Centers for Coastal Ocean Science (NCCOS) Research Support System provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. NCCOS's mission is to provide coastal managers with scientific information and tools needed to balance society's environmental, social, and economic goals.

NCCOS is passionate about supporting NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:
·To deliver high quality science in a timely and consistent manner using productive and strong partnerships.
·To develop and maintain relevant research, long term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.
·To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.
·To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

The NOAA6301 system:
· provides support to the program areas which are responsible for conducting research in the areas of marine bio-toxins; eco-toxicology; forensics; biotechnology; marine mammal stranding and necropsies; risk analysis; DNA sequencing; and marine related viruses and pathogens;
· provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus - NCCOS Head Quarters (HQ), Center for Sponsored Coastal Ocean Research (CSCOR), and Center for Coastal Monitoring and

Assessment (CCMA); Beaufort, NC - Center for Coastal Fisheries and Habitat Research (CCFHR); Charleston, SC Center for Coastal Environmental Health and Biomolecular Research (CCEHBR) and Hollings Marine Laboratory (HML); and Oxford, MD Cooperative Oxford Laboratory (COL); Beaufort, NC (CCFHR); Charleston, SC (CCEHBRC and CHHR/HML); and Oxford, MD (CCEHBRO);
provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, LAN and WAN, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services; and
· provides continued service to the local area network (LAN) and the wide area network (WAN) connections for non-SSMC locations.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

___X_ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
__X__ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

___X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X_ I certify the criteria implied by one or more of the questions above **apply** to the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

____ I certify the criteria implied by the questions above **do not apply** to the National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Rohit Munjal

Signature of ISSO: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381 Date: 2018.01.05 09:43:16 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): John D. Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.17 14:18:00 05'00' Date: _____

Name of Authorizing Official (AO): Steven Thur

Signature of AO: Digitally signed by THUR.STEVEN.M.1365841299 Date: 2018.01.19 07:49:11 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.23 10:18:48 -05'00' Date: _____

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Centers for Coastal Ocean Science (NCCOS) Research Support System (NOAA6301)

Unique Project Identifier: 006-00-02-00-01-0511-00

Introduction: System Description

The NOAA6301 NCCOS Research Support System provides the network infrastructure, hardware and software necessary to enable the mission of NCCOS, the organization. NCCOS's mission is to provide coastal managers with scientific information and tools needed to balance society's environmental, social, and economic goals.

NCCOS is passionate about supporting NOAA's environmental and economic missions by providing valuable scientific information to its constituents. NCCOS's fundamental principles are:

·To deliver high quality science in a timely and consistent manner using productive and strong partnerships.

·To develop and maintain relevant research, long term data collection and analyses, and forecasting capabilities in support of its customers, stakeholders, and partners.

·To build capacity in the private, local, state, and tribal sectors by transferring technology and providing technical assistance and knowledge to its customers and partners.

·To conduct the anticipatory science necessary to manage potential impacts of multiple stressors on coastal ecosystems.

The NOAA6301 system:

· provides support to the program areas which are responsible for conducting research in the areas of marine bio-toxins; eco-toxicology; forensics; biotechnology; marine mammal stranding and necropsies; risk analysis; DNA sequencing; and marine related viruses and pathogens;

· provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus - NCCOS Head Quarters (HQ), Center for Sponsored Coastal Ocean Research (CSCOR), and Center for Coastal Monitoring and Assessment (CCMA); Beaufort, NC - Center for Coastal Fisheries and Habitat Research (CCFHR); Charleston, SC Center for Coastal Environmental Health and Biomolecular Research (CCEHBR) and Hollings Marine Laboratory (HML); and Oxford, MD Cooperative Oxford Laboratory (COL);

· provides all resources related to data management, electronic file, COTS, printing, computer and software, field data acquisition, backup and restoration, LAN, helpdesk, specialty applications for GIS and statistical analysis, moderate programming, Web design and Web product delivery, video conferencing, and other media support services; and

· Provides continued service to the local area network (LAN) connections for non-SSMC locations.

In addition to the general purposes office automation support (file/printer sharing, application

hosting, collaboration, etc.) provided by NOAA6301, the system provides help desk services and supports a number of web sites and internal minor applications, one of which stores PII for the purpose of conducting the external grant review process as defined within the NOAA Grants Online System, (FISMA system ID, NOAA1101, PIA signed 7/6/2017). Grant applications are downloaded from Grants Online on a case by case basis, for review. They are stored by opportunity or grant number.

As detailed in the information sharing section below, NCCOS gathers and stores PII related to employees and contractors for Human Resource-related issues such as the hiring process as well as workforce planning, COOP Operations, and documentation. The NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts.

Information Sharing

NOAA6301 NCCOS Research Support System General Support System (GSS) collects and collects and stores limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by staff, partners, volunteers, and government and non-government collaborators) to facilitate internal and external communications to facilitate business and collaborative functions. This is not a central collection, but rather separated by function or individual project or person.

NOAA6301 is a general support system for NCCOS and stores information about individuals during the application and hiring of (electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase), including standard HR information (such as Travel authorization and vouchers, passports and international travel forms (completed by the employee through the travel portal), information for security badging process (contact information only the employee completed the badge application on paper forms, which are taken to the NOAA Office of Security), and performance appraisal ranking).

NCCOS' employee data is collected, stored and maintained for internal COOP, Human Resources, and workforce planning purposes (federal employee/contractor).

NCCOS collects BII during the pre and post activities associated with the acquisition and management of contracts. The storage is in the form of PDF forms or MS Word documents. There is no major application or database used to collect or store BII or employee PII information. NCCOS does not have a separate HR division since NCCOS utilizes the NOAA Workforce Management Office.

With exception of the CSCOR Review Application, all information is stored on supervisors' and acquisition managers' restricted access file storage available only to the specific employee(s). Access is restricted to those on a need to know basis, by permissions settings and/or passwords. The data is access controlled when on a supervisor's desktop machine or file share; if stored on a supervisor's laptop, the data is encrypted since all mobile devices have full encryption. The CSCOR Review Application although managed by NCCOS, is hosted by an NOAA6001 NOS Enterprise Services server and is restricted by username and password.

CSCOR Review Application Information in identifying form is made available by NOAA Grants Online (FISMA system ID, NOAA1101, PIA signed 7/6/2017) to NCCOS to accomplish Independent Individual Merit Reviews supporting the NOAA Grants Online system and process.

Information about the NOAA Grants Program may be found at: http://www.corporateservices.noaa.gov/~grantsonline/index.html. This is a non-public system. Information extracted from NOAA Grants Online to support the Independent Individual Merit Reviews is temporarily stored to facilitate the review process lifecycle. This information can include any general personal information and work related information. Although it is not the intent to extract PII information from the NOAA Grants Online system, it is possible the information could contain the Employer Identification Number (EIN). The EIN is a non-mandatory field which may be populated on the grants information made available by federal forms not managed by NCCOS. The NCCOS information system does not collect this identifying information directly.

A citation of the legal authority to collect PII and/or BII

The general legislation supporting the system is 5 U.S.C.301, one of the statutes concerning government organization and employees.

Additional authorities from DEPT-2, Accounts Receivable: H.R. 4613 (97th): Debt Collection Act of 1982, a bill to increase the efficiency of Government-wide efforts to collect debts owed the United States and to provide additional procedures for the collection of debts owed the United States and 5 U.S.C. 5701-09; 31 U.S.C. 951-953, 4 CFR 102.4, FPMR 101-7; Treasury Fiscal Requirements Manual.

Additional authorities from GSA/GOVT-9, System for Award Management: Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204, and 40 U.S.C. 121(c), Regulations by Administrator. For the Entity Management functional area of Systems Award Management, the authorities for collecting the information and maintaining the system are the Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c). For the exclusions portion of the Performance Information functional area, the authorities for collecting the information and maintaining the system are FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989).

The Federal Information Processing Standard (FIPS) 199 security impact category for NOAA6301 is moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	

b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X__ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID	X**	f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport	x	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: ** Same data element checked for Grants Online, as in the NOAA1101 PIA.					

General Personal Data (GPD)					
a. Name	x	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	x	o. Medical Information	
d. Gender		j. Telephone Number	x	p. Military Service	
e. Age		k. Email Address	x	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	d. Telephone Number	x	g. Salary	x
b. Job Title	x	e. Email Address	x	h. Work History	x
c. Work Address	x	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): NCCOS does not capture photographs for badging since it is performed and stored by the NOAA badging office of security.					

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	
b. IP Address	x	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Pre and Post Acquisition. This BII information would be obtained and utilized during the pre acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate. This information is protected under 41 USC 253, the FOIA Exemption 3 statute for contract proposals and collections associated with them.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	
Telephone		Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify) NOAA Grants Online http://www.corporateservices.noaa.gov/~grantsonline/index.html.					

Non-government Sources					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): NCCOS does not acquire PII from other non-government sources other than associated through formal partnership agreements and for the purpose of facilities safety, security, and COOP. Other non-government sources would be only for BII associated with Pre/Post Acquisition Sensitive Information obtained through delivered bids on NCCOS Acquisitions.					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

x	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

x	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	x
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Collected BII would be associated with determine qualification/eligibility for open acquisitions. PII would be collected for administrative actions, for HR and Workforce management. PII/BII: NOAA Grants Online - Grant Merit Reviews			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

In general, the laws that created the various NOS programs, specifically NCCOS, include provisions for the program to accomplish a mission. The mission may involve partnerships and educating the public. The collection and storage of information is part of accomplishing the legislated mission of the NCCOS, the NOS, and NOAA (members of the public and federal employees).

NOAA6301 stores PII on an ad hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking. This information is stored temporarily during the hiring phase, as well as standard HR information such as travel authorization and vouchers, passports and international travel forms, information for the security badging process (name, work email address and work telephone number, and performance appraisal ranking.

NCCOS stores limited PII and potentially an EIN (BII), for grant review only, on an ad hoc basis about individuals or entities that are providing information in support of a grant application submitted through NOAA Grants Online which is retained for the review process lifecycle only.

BII Pre and Post Acquisition. This BII information would be obtained and utilized during the pre-acquisition obtained through deliverable BIDS package and contain specific company information. BII information would be maintained on specific secure network folders during the execution of awarded contract and other information from companies not receiving awards would be deleted, when appropriate.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	x		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA6301connects to the NOS Line Office information system NOAA6001 and other NOAA information systems for VPN, Security and Network Operations. NCCOS established security permissions based on NOS Active Directory Network account (enforced 2FA when possible), restrictions in firewall ACL and security permissions on specific network folders where documentation is stored.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	x
Contractors	x		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
x	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://coastalscience.noaa.gov/contact/privacy. A PAS for Grants Online has been finalized and has been posted at: https://grantsonline.rdc.noaa.gov/	
x	Yes, notice is provided by other means.	Specify how: (Specific to PII) Verbally by administrative appointed staff or supervisor OR this address is referenced: https://coastalscience.noaa.gov/contact/privacy. This is an NOS standard privacy policy and not specific to NCCOS. BII is provided for the purpose of acquisition consideration only through government managed acquisition processes and forms only. NCCOS does not generate or maintain additional forms or processes to support acquisition activities. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.

	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

x	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: PII: No information collected is mandatory. Individuals are verbally told by administrative appointed staff or supervisor that they can decline or individuals are directed to review the privacy policy at this address: https://coastalscience.noaa.gov/contact/privacy, where it is stated all information collected is voluntary. This is an NOS standard privacy policy and not specific to NCCOS. BII provided for acquisition consideration is not mandatory. However, declining to provide the information necessary to evaluate them for an acquisition could result in non-award. PII provided within NOAA Grants Online, utilized within the CSCOR Review Application, is managed through the NOAA Grants Online application only. Completion of the Grants Online application would be needed for award consideration.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Applicants for positions are providing their personal information on a voluntary basis through their resumes. There is only one use for this information. The employment application contains the Privacy Act notice. Applicants have the opportunity to consent to only particular uses of their PII, in writing, to the HR representative or their supervisor, but it may affect the overall processing of their employment. For ongoing employee business, such as travel, there is only one specific use for each PII collection. BII is submitted for a specific purpose which consent is implied with the submittal of the package. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

x	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: (Specific to PII) NCCOS employees can contact HR staff or the federal employee personnel page to update their information, as they are informed as part of new employee

		orientation. BII is provided for the purpose of acquisition consideration through government managed acquisition processes and forms only. NCCOS dos not generate or maintain additional forms or processes to support acquisition activities. BII provided within NOAA Grants Online utilized within the CSCOR Review Application is managed through the NOAA Grants Online application only. Regarding contracts and grants that are in process or awarded, the applicants or awardees would send updates to the stated NOAA contact.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
x	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
x	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
x	Access to the PII/BII is restricted to authorized personnel only.
x	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: With exception to the CSCOR Review Application, access to storage folders are restricted by ACL and since PII/BII is not centralized in a database it cannot be easily monitored for access. The CSCOR Review Application has a database which is monitored, tracked and recorded.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 3/23/2017. Next one is no later than 3/22/2018. ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
x	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
x	Other (specify): All appropriate contractors and contract clauses include non-disclosure, but not all federal employees sign a confidentiality agreement or non-disclosure agreement.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

All information is stored within the accredited boundaries of NOAA6301 in network data shares controlled by established permission based on the organizational, project, or employee access rights. Any access to specific restricted files or folders must be requested through an access change request which is reviewed and documented by the NOAA6301 Information System Security Officer for authorization and mission 'need-to-know' requirement prior to implementation. Least privilege is implemented through file share permissions to ensure privacy and open only to those demonstrating a "need to know."

Any PII information which is transmitted electronically must follow the federal government and NOAA standard procedure of secure packaging such as utilization of Department of Commerce (DOC) Accellion for encryption in transit.

NCCOS implements security controls listed in NIST Special Publication 800-53 R4 required for a moderate system. In compliance with NIST Special Publication 800-53 rev 4, NCCOS has a security program, with performance measures and goals, in order to complete continuous monitoring activities, which include annual security control reviews, quarterly vulnerability scanning, monthly review of security access control list, weekly review of audit logs, handling of access change requests and change control board activities. The risk assessment includes the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII data along with the countermeasures.

The controls supporting the use of Microsoft Azure FedRamp approved system as a customer are in place in NOAA6301. There are currently Web applications, with no PII, hosted on Microsoft Azure. As noted in Section 12.2, we are transitioning CSCOR to Azure prior to December 2018. The same sharing controls that are in place currently for CSCOR will apply when it is moved to Azure.

Every year the IT system undergoes a thorough continuous monitoring for the assessment and authorization (A&A) process that is performed by an independent. The A&A process ensures that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) and NOAA guidelines for continued operation.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/DEPT-18 - Employees Personnel Files Not Covered By Notices of Other Agencies; DEPT-2, Accounts Receivable; GSA/GOVT-9, System for Award Management.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created:

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: Chapters 1601 and 1607 of NOAA's Records Schedules, http://www.corporateservices.noaa.gov/audit/records_management/schedules/, provide supplemental record retention guidance for the NCCOS Research Support System. Chapter 1601 pertains to general administration for the National Ocean Service and Chapter 1607 pertains to specific records managed by the NCCOS Research Support System. Specifically, 1601-02 Grants Working Files (N1- 370-02-5), 1601-04 Electronic Copies (N1-370-02-5), 1601-05 NOS Annual Operating Plan (AOP) Information Tracking Systems (N1-370-04-4), 1609-06 in the NOAA Disposition Handbook and 1607-04 Program Funding Database. The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. In accordance with GRS 20, item 3, the data is presently being retained indefinitely. For NCCOS administrative PII data, the records would be covered under the following NARA general records schedules: GRS 2 – payroll and pay administrative records GRS 20 – electronic records GRS 23 – records common to most offices within agencies NCCOS' contact information (contractor and partner) is collected to provide a means for the Office of Coast Survey to communicate and respond to needs and requests. This data would be retained as long as the individual continued to request contact and information. It is technologically possible to delete information at the request of the individual. There is no scheduled records retention for this information.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
x	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	x	Overwriting	x
Degaussing	x	Deleting	x
Other (specify): Compliant sanitization methods.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Evaluated how easily PII could be used to identify a specific individual. Based on contact information, individuals can be identified.
X	Quantity of PII	Provide explanation: Considered how many individuals can be identified from the PII. The PII is only temporarily stored for a limited amount of individuals, therefore reducing the breach impact.
X	Data Field Sensitivity	Provide explanation: Data fields are limited and only used when absolutely required. SSN is not one of these data fields. EIN is a field which can be populated within NOAA Grants Online, however, is not required and is not utilized. This field will not be extracted from NOAA Grants Online in the future revision of the CSCOR Review Application.
X	Context of Use	Provide explanation: Evaluated the context of use—the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The use of the PII is restricted to specific individuals, stored for a limited amount of time and is not utilized in more than one way reducing the impact.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The PII is only temporarily stored in a protected location for a limited amount of individuals, therefore reducing the breach impact.
X	Other:	Provide explanation: The loss of a single individual's PII would have an impact on that individual through possible identify theft and NCCOS as a government identity BUT it would not have an impact on the NCCOS mission or have a serious impact on reputation.

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
x	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

x	Yes, the conduct of this PIA results in required technology changes. Explanation: NOAA6301 is utilizing Azure SQL in the Microsoft Azure PaaS environment to store web application data. Although there is currently no PII/BII associated with the web/apps and transitioning to the new environment is not expected prior to December 2018, controls are already in place to encrypt at rest data through the Azure SQL TDE capability: https://msdn.microsoft.com/en-us/library/dn948096.aspx. All SQL databases will have this feature turned on at inception and it will remain on. This storage is currently planned only for CSCOR and will further secure the CSCOR Review Application Database.
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Rohit Munjal Office: NOS/NCCOS Phone: 240-533-0289 Email: Rohit.Munjal@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381 Date: 2018.01.05 09:46:15 -05'00' Date signed:	**Information Technology Security Officer** Name: John D. Parker Office: NOS Phone: 240-533-0832 Email:John.D.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.13658359 14 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.01.17 14:46:55 -05'00' Date signed:
Authorizing Official Name: Steven Thur Office: NOS/NCCOS Phone: 240-533-0146 Email: Steven.Thur@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Digitally signed by THUR.STEVEN.M.1365841299 Date: 2018.01.19 07:50:30 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.23 10:12:39 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NCCOS Research Support System

FISMA Name/ID (if different): NOAA6301

Name of IT System/ Program Owner: National Centers for Coastal Ocean Science

Name of Information System Security Officer: Rohit Munjal

Name of Authorizing Official(s): Steven Thur / Cheryl Marlin

Date of Last PIA Compliance Review Board (CRB): 3/16/2017

(This date must be within three (3) years.)

Date of PIA Review: 1/8/2018

Name of Reviewer: Rohit Munjal

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: MUNJAL.ROHIT.1500946381 Digitally signed by MUNJAL.ROHIT.1500946381 Date: 2018.01.08 12:19:26 05'00'

Date of Privacy Act (PA) Review: 1/23/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Digitally signed by BRABSON.SARAH.1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON.SARAH.1365710488 Date 2018 02 01 08 52 48 05'00'

Date of BCPO Review: 1/23/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 01 23 10 17 27 05'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, February 23, 2018 2:31 PM
To:	Mark Graff NOAA Federal
Subject:	Fwd: PTA and PIA
Attachments:	NOAA8885_PIA_FY18_signed.pdf; NOAA8885_PTA_FY18_signed.pdf; NOAA8885_PIA_Annual_Review_Certification_FY18_for MHG signature.pdf; NOAA8885 POA&M.docx

Mark, here are the NOAA8885 PIA, PTA and certification for your signature. I signed the certification also. Also attached are the details on the one open POA&M, scheduled for completion by August 2018. The latest SAR is in the PIA folder. There were several unsatisfied audit and accountability controls, that's about it.

(b)(5)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

FISMA Name/ID (if different): _____

Name of IT System/ Program Owner: Sean Wink

Name of Information System Security Officer: Chris Hornbrook

Name of Authorizing Official(s): Grant Cooper, Ph.D.

Date of Last PIA Compliance Review Board (CRB): June 30, 2017

(This date must be within three (3) years.)

Date of PIA Review: February 20, 2018

Name of Reviewer: Sean Wink

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: WINK.SEAN.P.1365853270 Digitally signed by WINK.SEAN.P.1365853270 Date: 2018.02.22 13:35:29 -07'00'

Date of Privacy Act (PA) Review: 2/23/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 02 23 13 41 56 05'00'

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: _____

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Friday, February 23, 2018 4:12 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: PTA and PIA
Attachments:	NOAA8885_PIA_Annual_Review_Certification_FY18_for MHG signature mhg.pdf; NOAA8885_PIA_FY18_signed mhg.pdf; NOAA8885_PTA_FY18_signed mhg.pdf

Looks good

The only concern I had wa (b)(5) [redacted] I'm guessing OPOG will ask the same thing, so we may want to clarify.

Assuming they are not additional PII elements to the FISMA system, attached are the signed versions of the PTA/PIA/Certification.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) [redacted] (C)

On Fri, Feb 23, 2018 at 2:31 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, here are the NOAA8885 PIA, PTA and certification for your signature. I signed the certification also. Also attached are the details on the one open POA&M, scheduled for completion by August 2018. The latest SAR is in the PIA folder. There were several unsatisfied audit and accountability controls, that's about it.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

FISMA Name/ID (if different): _____

Name of IT System/ Program Owner: Sean Wink

Name of Information System Security Officer: Chris Hornbrook

Name of Authorizing Official(s): Grant Cooper, Ph.D.

Date of Last PIA Compliance Review Board (CRB): June 30, 2017

(This date must be within three (3) years.)

Date of PIA Review: February 20, 2018

Name of Reviewer: Sean Wink

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: WINK.SEAN.P.1365853270 Digitally signed by WINK.SEAN.P.1365853270 Date: 2018.02.22 13:35:29 -07'00'

Date of Privacy Act (PA) Review: 2/23/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 02 23 13 41 56 05'00'

Date of BCPO Review: 2.23.18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 02 23 16 06 00 05'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

The NOAA8885 System is designed and used to collect, process, and disseminate supplemental weather data that supports warning and forecast products for the protection of life, property, and the enhancement of the national economy. NOAA8885 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA8885 also provides administrative functions as well as scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

Although there are a variety of hardware and operating systems, several of the activities are interconnected. NOAA8885 provides direct and indirect mission support for the NWS as a Government agency. The mission support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web-based server systems. The system also supports a variety of users, functions, and applications.

The NWS Western Region Headquarters Workforce Database, located in Salt Lake City, Utah, consists of basic identifying information about employees and contractors. The database is maintained as a supplement to other employee records and is used by Western Region Headquarters Administration staff to aid in tracking job vacancies, developing statistical reports, and performing other related administrative tasks. There are also local databases at the WFO/RFC that maintain information on volunteers who provide weather reports to NWS staff.

Information Sharing: Employee/contractor information is not shared with any third parties or unauthorized personnel. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is only available to members of the NWS Western Region. Specific information about individual personnel is only available to authorized NWS Western Region Headquarters Administration Staff. Volunteer database information is accessible to forecast staff so they can contact volunteers for severe weather information.

The statutory authorities covering the collection of this data are 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce]. In addition: 44 U.S.C. 3101; 5 U.S.C. 4101 et seq., 5 U.SC. 1302, 3302, E.O. 10577, 3 CFR 1954-1958 Comp. p. 218, E.O. 12107, 3 CFR 1978 Comp. p264; and Federal Personnel Manual and related directives for NOAA and the Department of Commerce.

This is a FIPS 199 moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

___X___ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): Spotter ID , radio call sign if applicable (volunteers)					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): For volunteers: County, elevation, latitude/longitude, what hours can be contacted for severe weather reports, possession of a rain gauge, anemometer, thermometer, snow stick, or weather station , twitter account/facebook account information, last time attended spotter class.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
Other work-related data (specify): GS level series, position, division/organization name, regional office location, optional text field with current/relevant personnel issues.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Information on volunteers that is utilized to determine suitability for the program and to provide reports pertaining to local weather conditions.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in

reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NWS Western Region Headquarters Workforce Database maintains information concerning federal employees and contractors in the Western Region workforce. This information is managed by the NWS Western Region Headquarters Administration Personnel.
The information maintained includes:

- Name
- Position
- GS Level/Series
- Division/Organization Name
- Regional Office Location
- Optional text field with current/relevant personnel issues.

This information is maintained to aid in tracking job vacancies, maintenance of organization structures, and other administrative related activities. The information is used by Western Region Headquarters Administration staff to supplement managing employee records, providing statistical data, etc. The information is not shared with any third parties or unauthorized personnel. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is only available to members of the NWS Western Region. Specific information about individual personnel is only available to authorized NWS Western Region Headquarters Administration Staff.

There are also local databases at the local WFO/RFC that maintain information on volunteers who provide weather reports to staff. The WFO/RFC database information is collected to contact volunteers when severe weather information is needed. The database holds the following information on these volunteers:

- First and last name
- Mailing address
- County
- Phone (home/cell)
- Spotter ID
- Elevation
- Email address
- What hours they can be contacted for severe weather reports
- Do they have a rain gauge, anemometer, thermometer, snow stick, or weather station
- Radio Call sign
- Twitter account
- Facebook account
- Last time attended spotter class
- Latitude / Longitude

Information in this database is provided on a voluntary basis; volunteers sign up and provide the information during spotter talks the NWS provides in preparation for the severe weather season. Volunteers have the opportunity to decline providing their information, if they do not want to participate in the future. This database information is accessible to forecast staff so they can contact volunteers for severe weather information.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the

PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors			
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The updated Volunteer Privacy Act statement, and privacy policy, can be found at: http://www.nws.noaa.gov/om/coop/index.htm.	
X	Yes, notice is provided by other means.	Specify how: For the volunteer database, information is provided on a voluntary basis and users are notified by a

		statement on the volunteer and emergency planning forms. For the workforce database, individuals are notified at the time of employment that the collection of this information is mandatory as a condition of employment.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the volunteer database, the information is provided on a purely volunteer basis and users are not required to provide information. For the workforce database, individuals (federal employees) may decline, in writing to their supervisor, not to have their information added to the database with the understanding that it may affect their employment.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For the volunteer data, the information is provided on a purely volunteer basis and users provide the information to participate in the program which constitutes consent to use the information for the stated purpose. The NOAA Web site privacy policy states "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." For the workforce data, employees and contractors are required to provide the information as a condition of employment, but may consent to only particular uses, in writing, to their supervisors, with the understanding that it may affect their employment.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the volunteer data, users may request their data from, and send updates, if needed, to their local station manager. For the workforce data, information is routinely updated as an employee's role or position changes. Employees cannot review the information, but may request their information, and ask that it be updated, through their supervisor. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Management Division (AMD) Chief.

	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Standard system audit logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/30/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
N/A	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access to data is controlled by the use of account permissions, firewall access lists, and two-factor authentication. Active Directory group memberships and assigned permissions are employed to manage control of the access to folders, files and shares. Access is based on a "need to have" basis and the least privilege principle. Only authorized individuals have access to information.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: NOAA–11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1300 National Weather Service Records Disposition Schedule NOAA Records Control Schedule Chapter 300
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Although name, general location, and phone number can be used to identify individuals, this information is available via other sources. There would be low impact to the individual if information was released.
X	Quantity of PII	Provide explanation: A moderate amount of PII is collected (name, phone, number, location); however, the data is not in a sensitive context.
X	Data Field Sensitivity	Provide explanation: Data fields contain items such as name, GS Level, and phone, however there is not a sensitive context related to the data (e.g. not health information).
X	Context of Use	Provide explanation: Based on the use of the information outlined in section 5.1, the impact would be low if information was accessed.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access is limited to internal authorized federal employees. Access restrictions are in place as outlined in section 8 as well as the NOAA8885 System Security Plan (SSP).
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Addition of volunteer data elements to PAS and NOAA-11 SORN.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes.

	Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

System Owner Name: Sean Wink Office: NOAA NWS Western Region Phone: 385-419-3131 Email: sean.wink@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: WINK.SEAN.P.1365853270 Digitally signed by WINK.SEAN.P.1365853270 Date: 2018.02.22 08:37:59 -07'00'	**Information Technology Security Officer** Name: Andrew Browne Office: NOAA NWS Office of the CIO Phone: 301-427-9033 Email: andrew.browne@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.02.22 15:24:03 -05'00'
Authorizing Official Name: Grant Cooper, Ph.D. Office: NOAA NWS Western Region Phone: 801-524-5122 Email: grant.cooper@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPER.GRANT.ALEXANDER.IV.1047689399 Digitally signed by COOPER.GRANT.ALEXANDER.IV.1047689399 Date: 2018.02.22 08:50:50 -07'00'	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.23 16:07:13 -05'00'

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for
National Weather Service (NWS) Western Region General Support System (NOAA8885)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA8885 National Weather Service (NWS) Western Region General Support System (NOAA8885)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The National Weather Service (NWS) provides weather, hydrologic, climate forecasts, and warnings for the United States, its territories, adjacent waters, and ocean areas. The NOAA8885 System is designed and used to collect, process, and disseminate supplemental weather data that supports warning and forecast products for the protection of life, property, and the enhancement of the national economy. NOAA8885 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA8885 also provides administrative functions as well as scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

Functional areas of NOAA8885 can be classified into six major areas.

- Observations Meteorological/Hydrological Sensing systems.
- Operations/Production Operations/Production of Watches, Warnings, & Forecasts.
- Dissemination Systems used for the dissemination of NWS information.
- Administration Office Automation, Word Processing, Email, etc.
- Security Systems supporting the security posture of the Enterprise
- Network Networking/Transport Infrastructure

Although there are a variety of hardware and operating systems, several of the activities are interconnected. NOAA8885 provides direct and indirect mission support for the NWS as a Government agency. The mission support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web- based server systems. The system also supports a variety of users, functions, and applications.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

__√__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__√__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is]

privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__√__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__√__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__√__ DOC employees
__√__ Contractors working on behalf of DOC
__√__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__√__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__√__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__√__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA8885 system and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA8885 system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Sean Wink

Signature of SO: WINK.SEAN.P.1365853270 Digitally signed by WINK.SEAN.P.1365853270 Date: 2018.02.22 09:33:40 07'00' Date: _____

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.02.22 15:25:19 -05'00' Date: _____

Name of Authorizing Official (AO): Grant Cooper, Ph.D.

Signature of AO: COOPER.GRANT.ALEXANDER.IV.1047689399 Digitally signed by COOPER.GRANT.ALEXANDER.IV.1047689399 Date: 2018.02.22 09:35:23 -07'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892 DN: c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892 Date: 2018 02 23 16:03:38 05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, February 23, 2018 4:58 PM
To:	Mark Graff NOAA Federal
Cc:	Eric Barton NOAA Federal
Subject:	Re: ACCSP and SERO (NOAA4300) System Interconnect Agreement
Attachments:	NOAA 19 PA SORN_new template_categories added_111417.docx

(b)(5) [redacted].

http://www.accsp.org/

On Fri, Feb 23, 2018 at 4:28 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

Hi Eric,

There would be a couple questions on this that probably need to be fleshed out before this went into place

- (b)(5) [redacted]
- [redacted]
- [redacted]?

With this info, I can probably run this by the Department (OPOG), who would need to make sure they concur as to the "Computer Matching" portion, since they ultimately would be the ones to administer/approve any new computer matching programs under the CMPPA.

Thanks Eric,

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) [redacted] (C)

On Fri, Feb 23, 2018 at 4:13 PM, Eric Barton NOAA Federal <eric.barton@noaa.gov> wrote:

Good Afternoon,

I was hoping to discuss an issue that involves the sharing of PII with ACCSP with one or both of you when time permits. (b)(5) [redacted], just to show due diligence, but I would also like your input on this to make it as thorough as possible.

Thank you, and have a great weekend!

Eric Barton
ISSO, Southeast Regional Office
National Marine Fisheries Service
727 551 5746

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6) [redacted]

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, February 26, 2018 10:05 AM
To:	Mark Graff NOAA Federal
Subject:	NOAA4000 PTA for your signature
Attachments:	4000 AR02 PTA 20180201 Signed RV.pdf

The PIA incorporating Clearview is in process, also.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, February 26, 2018 10:35 AM
To:	Gioffre, Kathy (Federal); CPO; Ferguson, Dorrie
Cc:	Mark Graff NOAA Federal; Chris Hornbrook NOAA Federal; Sean Wink NOAA Federal
Subject:	NOAA8885 certification documentation for OPOG review
Attachments:	NOAA8885_PIA_Annual_Review_Certification_FY18_for MHG signature mhg.pdf; NOAA8885_PIA_FY18 for recertification.pdf; NOAA8885_PTA_FY18_signed mhg.pdf

Attached are the re signed PIA with updated ATO date, a new PTA, and the certification.

Next ATO date is 80 30 18.

Thanks, Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

FISMA Name/ID (if different): _____

Name of IT System/ Program Owner: Sean Wink

Name of Information System Security Officer: Chris Hornbrook

Name of Authorizing Official(s): Grant Cooper, Ph.D.

Date of Last PIA Compliance Review Board (CRB): June 30, 2017

(This date must be within three (3) years.)

Date of PIA Review: February 20, 2018

Name of Reviewer: Sean Wink

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: WINK.SEAN.P.1365853270 Digitally signed by WINK.SEAN.P.1365853270 Date: 2018.02.22 13:35:29 -07'00'

Date of Privacy Act (PA) Review: 2/23/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 02 23 13 41 56 05'00'

Date of BCPO Review: 2.23.18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 02 23 16 06 00 05'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

The NOAA8885 System is designed and used to collect, process, and disseminate supplemental weather data that supports warning and forecast products for the protection of life, property, and the enhancement of the national economy. NOAA8885 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA8885 also provides administrative functions as well as scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

Although there are a variety of hardware and operating systems, several of the activities are interconnected. NOAA8885 provides direct and indirect mission support for the NWS as a Government agency. The mission support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web-based server systems. The system also supports a variety of users, functions, and applications.

The NWS Western Region Headquarters Workforce Database, located in Salt Lake City, Utah, consists of basic identifying information about employees and contractors. The database is maintained as a supplement to other employee records and is used by Western Region Headquarters Administration staff to aid in tracking job vacancies, developing statistical reports, and performing other related administrative tasks. There are also local databases at the WFO/RFC that maintain information on volunteers who provide weather reports to NWS staff.

Information Sharing: Employee/contractor information is not shared with any third parties or unauthorized personnel. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is only available to members of the NWS Western Region. Specific information about individual personnel is only available to authorized NWS Western Region Headquarters Administration Staff. Volunteer database information is accessible to forecast staff so they can contact volunteers for severe weather information.

The statutory authorities covering the collection of this data are 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce]. In addition: 44 U.S.C. 3101; 5 U.S.C. 4101 et seq., 5 U.SC. 1302, 3302, E.O. 10577, 3 CFR 1954-1958 Comp. p. 218, E.O. 12107, 3 CFR 1978 Comp. p264; and Federal Personnel Manual and related directives for NOAA and the Department of Commerce.

This is a FIPS 199 moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

___X___ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): Spotter ID , radio call sign if applicable (volunteers)					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): For volunteers: County, elevation, latitude/longitude, what hours can be contacted for severe weather reports, possession of a rain gauge, anemometer, thermometer, snow stick, or weather station , twitter account/facebook account information, last time attended spotter class.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
Other work-related data (specify): GS level series, position, division/organization name, regional office location, optional text field with current/relevant personnel issues.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Information on volunteers that is utilized to determine suitability for the program and to provide reports pertaining to local weather conditions.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in

reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NWS Western Region Headquarters Workforce Database maintains information concerning federal employees and contractors in the Western Region workforce. This information is managed by the NWS Western Region Headquarters Administration Personnel.
The information maintained includes:

- Name
- Position
- GS Level/Series
- Division/Organization Name
- Regional Office Location
- Optional text field with current/relevant personnel issues.

This information is maintained to aid in tracking job vacancies, maintenance of organization structures, and other administrative related activities. The information is used by Western Region Headquarters Administration staff to supplement managing employee records, providing statistical data, etc. The information is not shared with any third parties or unauthorized personnel. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is only available to members of the NWS Western Region. Specific information about individual personnel is only available to authorized NWS Western Region Headquarters Administration Staff.

There are also local databases at the local WFO/RFC that maintain information on volunteers who provide weather reports to staff. The WFO/RFC database information is collected to contact volunteers when severe weather information is needed. The database holds the following information on these volunteers:

- First and last name
- Mailing address
- County
- Phone (home/cell)
- Spotter ID
- Elevation
- Email address
- What hours they can be contacted for severe weather reports
- Do they have a rain gauge, anemometer, thermometer, snow stick, or weather station
- Radio Call sign
- Twitter account
- Facebook account
- Last time attended spotter class
- Latitude / Longitude

Information in this database is provided on a voluntary basis; volunteers sign up and provide the information during spotter talks the NWS provides in preparation for the severe weather season. Volunteers have the opportunity to decline providing their information, if they do not want to participate in the future. This database information is accessible to forecast staff so they can contact volunteers for severe weather information.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the

PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors			
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The updated Volunteer Privacy Act statement, and privacy policy, can be found at: http://www.nws.noaa.gov/om/coop/index.htm.	
X	Yes, notice is provided by other means.	Specify how: For the volunteer database, information is provided on a voluntary basis and users are notified by a

		statement on the volunteer and emergency planning forms. For the workforce database, individuals are notified at the time of employment that the collection of this information is mandatory as a condition of employment.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the volunteer database, the information is provided on a purely volunteer basis and users are not required to provide information. For the workforce database, individuals (federal employees) may decline, in writing to their supervisor, not to have their information added to the database with the understanding that it may affect their employment.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For the volunteer data, the information is provided on a purely volunteer basis and users provide the information to participate in the program which constitutes consent to use the information for the stated purpose. The NOAA Web site privacy policy states "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." For the workforce data, employees and contractors are required to provide the information as a condition of employment, but may consent to only particular uses, in writing, to their supervisors, with the understanding that it may affect their employment.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the volunteer data, users may request their data from, and send updates, if needed, to their local station manager. For the workforce data, information is routinely updated as an employee's role or position changes. Employees cannot review the information, but may request their information, and ask that it be updated, through their supervisor. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Management Division (AMD) Chief.

	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Standard system audit logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/21/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
N/A	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access to data is controlled by the use of account permissions, firewall access lists, and two-factor authentication. Active Directory group memberships and assigned permissions are employed to manage control of the access to folders, files and shares. Access is based on a "need to have" basis and the least privilege principle. Only authorized individuals have access to information.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: NOAA–11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1300 National Weather Service Records Disposition Schedule NOAA Records Control Schedule Chapter 300
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Although name, general location, and phone number can be used to identify individuals, this information is available via other sources. There would be low impact to the individual if information was released.
X	Quantity of PII	Provide explanation: A moderate amount of PII is collected (name, phone, number, location); however, the data is not in a sensitive context.
X	Data Field Sensitivity	Provide explanation: Data fields contain items such as name, GS Level, and phone, however there is not a sensitive context related to the data (e.g. not health information).
X	Context of Use	Provide explanation: Based on the use of the information outlined in section 5.1, the impact would be low if information was accessed.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access is limited to internal authorized federal employees. Access restrictions are in place as outlined in section 8 as well as the NOAA8885 System Security Plan (SSP).
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:

	Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

System Owner Name: Sean Wink Office: NOAA NWS Western Region Phone: 385-419-3131 Email: sean.wink@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: WINK.SEAN.P.1365853270 Digitally signed by WINK.SEAN.P.1365853270 Date: 2018.02.22 08:37:59 -07'00'	**Information Technology Security Officer** Name: Andrew Browne Office: NOAA NWS Office of the CIO Phone: 301-427-9033 Email: andrew.browne@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.02.22 15:24:03 -05'00'
Authorizing Official Name: Grant Cooper, Ph.D. Office: NOAA NWS Western Region Phone: 801-524-5122 Email: grant.cooper@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPER.GRANT.ALEXANDER.IV.1047689399 Digitally signed by COOPER.GRANT.ALEXANDER.IV.1047689399 Date: 2018.02.22 08:50:50 -07'00'	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892 Date 2018 02 23 16 07 13 05'00'

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for
National Weather Service (NWS) Western Region General Support System (NOAA8885)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA8885 National Weather Service (NWS) Western Region General Support System (NOAA8885)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The National Weather Service (NWS) provides weather, hydrologic, climate forecasts, and warnings for the United States, its territories, adjacent waters, and ocean areas. The NOAA8885 System is designed and used to collect, process, and disseminate supplemental weather data that supports warning and forecast products for the protection of life, property, and the enhancement of the national economy. NOAA8885 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA8885 also provides administrative functions as well as scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

Functional areas of NOAA8885 can be classified into six major areas.

- Observations Meteorological/Hydrological Sensing systems.
- Operations/Production Operations/Production of Watches, Warnings, & Forecasts.
- Dissemination Systems used for the dissemination of NWS information.
- Administration Office Automation, Word Processing, Email, etc.
- Security Systems supporting the security posture of the Enterprise
- Network Networking/Transport Infrastructure

Although there are a variety of hardware and operating systems, several of the activities are interconnected. NOAA8885 provides direct and indirect mission support for the NWS as a Government agency. The mission support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web- based server systems. The system also supports a variety of users, functions, and applications.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

__√__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__√__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is]

privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__√__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__√__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__√__ DOC employees
__√__ Contractors working on behalf of DOC
__√__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__√__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__√__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__√__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA8885 system and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA8885 system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Sean Wink

Signature of SO: WINK.SEAN.P.1365853270 Digitally signed by WINK.SEAN.P.1365853270 Date: 2018.02.22 09:33:40 07'00' Date: _____

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.02.22 15:25:19 -05'00' Date: _____

Name of Authorizing Official (AO): Grant Cooper, Ph.D.

Signature of AO: COOPER.GRANT.ALEXANDER.IV.1047689399 Digitally signed by COOPER.GRANT.ALEXANDER.IV.1047689399 Date: 2018.02.22 09:35:23 -07'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892 DN: c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892 Date: 2018 02 23 16:03:38 05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, February 26, 2018 11:30 AM
To:	Mark Graff NOAA Federal
Subject:	NOAA4930 PTA for signature
Attachments:	4930_PTA_20180201 (1).pdf

Mark, this is not a Clearwell system. thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, February 26, 2018 11:36 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA4930 PTA for signature
Attachments:	4000 AR02 PTA 20180201 Signed RV mhg.pdf; 4930_PTA_20180201 (1) mhg.pdf

Looks good here are both the 4000 and 4930 PTA.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Mon, Feb 26, 2018 at 11:29 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, this is not a Clearwell system. thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Version Number: 01-2017

U.S. Department of Commerce
National Marine Fisheries Service
(NMFS)

Privacy Threshold Analysis
for the
NOAA4000 - Fisheries WAN and Enterprise Services

U.S. Department of Commerce Privacy Threshold Analysis

NOAA4000 - Fisheries WAN and Enterprise Services

Unique Project Identifier: 006-03-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The NMFS Headquarters information system (NOAA4000) is divided up into the following major components or areas of responsibility: IT Infrastructure and IT Services. IT Infrastructure is comprised of the hardware and software used within the environment to support the NMFS mission. The IT Services component on the other hand are those technology services provided to the NMFS organization that are supported by the IT infrastructure. The final component of the NOAA4000 system are the physical locations where the end-users and IT infrastructure reside.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) General Support System
b) Silver Spring, MD (SSMC3)
c) Interconnects with several systems
    i) US Coast Guard
    ii) Pacific States Marine Fisheries Commission
    iii) US Custom and Border Protection
    iv) Information Technology Center (ITC - NOAA1101)
    v) Other NOAA NMFS Systems (Permits, S&T, GARFO, NEFSC, SER, SEFSC, NWR, NWFSC, AKR, AKFSC, SWR, PIR, SWFSC, PIFSC)
d) The primary purpose of NMFS WAN connectivity:
    • Connectivity to Fisheries sites throughout the United States.
    • Access to electronic messaging to allow employees to send messages to Fisheries employees and external colleagues

• Internet access

e) IT Services

HQ based services

Local Area Network (LAN)
VoIP

Enterprise services

Wide Area Network (WAN)
Service Desk
Application Hosting
Security Services
Enterprise Active Directory

f) Name, DoB, Email, Place of Birth, Social Security, Taxpayer ID, Driver's License, Employer, ID, Passport, Financial Transaction, Employee ID, Occupation, Job Title, Salary, Work History, Voice, Recordings/Signature, Audit data, Case files, Seized property.

g) All users authorized to access the WAN using 2-factor authentication. Public Web - any user.

h) Via WAN connection and web interface.

i) Via WAN connection and web interface.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Use of FOIA request application.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes.
Information collected to fulfill FOIA request may contain BII or PII.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA4000 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Signature of ISSO or SO: BRIDGETT.CYNTHIA.MCCANN.1460827074 Digitally signed by BRIDGETT.CYNTHIA.MCCANN.1460827074 Date: 2018.02.08 07:03:11 -05'00'

Name of Information Technology Security Officer (ITSO):

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2018.02.06 16:42:33 -05'00'

Name of Authorizing Official (AO):

Signature of AO: VARGHESE.KOYICKAL.ROY.1400785496 Digitally signed by VARGHESE.KOYICKAL.ROY.1400785496 Date: 2018.02.14 16:30:01 -05'00'

Name of Bureau Chief Privacy Officer (BCPO):

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892 DN: c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892 Date: 2018 02 26 10:18:46 05 00'

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA4930 - Southwest Fisheries Science Center (SWFSC) Network

U.S. Department of Commerce

Privacy Threshold Analysis

NOAA4930 - Southwest Fisheries Science Center (SWFSC) Network

Unique Project Identifier: 006-03-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: NOAA4930 is a General Support System supporting users consisting of scientific, administrative, and support staff distributed among the California cities of La Jolla, Monterey, and Santa Cruz. There are a variety hardware platforms and operating systems interconnected on this network system. The systems are designed and configured to support the staff in meeting the agency mission.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) The NOAA4930 system is a General Support System supporting approximately 375 users consisting of scientific, administrative, and support staff.
b) The NOAA4930 system is comprised of the NOAA/NMFS Southwest Fisheries Science Center facilities located in the cities of La Jolla, Santa Cruz and Monterey in the state of California.
c) The NOAA4930 system is interconnected with the NMFS WAN (NOAA4000).
d) The NOAA4930 system is designed and configured to support the staff in meeting the agency mission in fisheries research, the management of local human resources and facilities.
e) The operational system functions that are provided include:
    - Network File Storage, Sharing, and Printing
    - Internet Access
    - NMFS Wide Area Network Connectivity
    - Administrative Support Systems
    - Scientific Database Access
    - Scientific Statistical Data Analysis
    - Geographic Information Systems
    - Web Based Information Dissemination

- Telecommunications

f) The categories of data inputted, stored and processed include administrative, scientific, statistical, economic, research and development, and technical.
g) NOAA4930 information is accessed by NOAA4930 authorized employees, contractors, students and volunteers.
h) NOAA4930 information is retrieved via government furnished IT equipment after verifying authentication and authorization levels.
i) NOAA4930 transmission is protected using defense in depth architecture. Particularly sensitive information is encrypted while in transmission.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

__X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

_X__ Companies
____ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X__ DOC employees
_X__ Contractors working on behalf of DOC
_X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA4930 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA4930 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Richard Cosgrove

Signature of ISSO or SO: COSGROVE.RICHARD.E.III.1365890672 Digitally signed by COSGROVE.RICHARD.E.III.1365890672 Date: 2018.02.01 10:14:59 08'00' Date: 02/01/2018

Name of Information Technology Security Officer (ITSO): Catherine Amores

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2018.02.26 09:53:50 05'00' Date: _____

Name of Authorizing Official (AO): Kristen Koch

Signature of AO: KOCH.KRISTEN.CLARE.1365892284 Digitally signed by KOCH.KRISTEN.CLARE.1365892284 Date: 2018.02.02 10:53:51 -08'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.26 11:35:30 -05'00' Date: _____

John D. Parker - NOAA Federal

From:	John D. Parker NOAA Federal
Sent:	Monday, February 26, 2018 12:15 PM
To:	James Cooperman NOAA Affiliate
Cc:	Jonathan Gordon NOAA Federal; _NOS IT Security Program; Sarah Brabson NOAA Federal; Mark Graff
Subject:	Re: PIA/PTA
Attachments:	NOAA6602 PIA_V2 02 2018.docx; NOAA6602 PTA_V2 02 2018.docx

Hi Jim,

I have no additional changes. I have included Sarah and Mark on this email with the files attached.

John

--

John D. Parker, CISSP, CISA <John.D.Parker@noaa.gov>
NOS IT Security Officer
DOC/NOAA/NOS IMO
240-533-0832 (office)
(b)(6) (mobile)
Email NOS IT security inquires: NOS.ITSP@noaa.gov

On 2/23/2018 9:41 AM, James Cooperman NOAA Affiliate wrote:

> John
>
> Attached are the PIA and PTA for your review. With your approval I will finalize the documents and send out for signatures.
>
> Jim Cooperman
>
> James Cooperman CTR
> Information System Security Office
> Office of National Marine Sanctuaries
> Desk 240-533-0680
> Cell (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 1, 2018 3:49 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA5032 PTA for signature
Attachments:	NOAA5032_PTA_Feb2018_for OSPO coAO signature vig.pdf

Mark, this one is a candidate for certification, and I briefed the ISSO accordingly.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, March 1, 2018 4:01 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA5032 PTA for signature
Attachments:	NOAA5032_PTA_Feb2018_for OSPO coAO signature vig mhg.pdf

Looks good attached.

If you want to just let me know when the SAR or POA&Ms are ready for review.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Thu, Mar 1, 2018 at 3:48 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, this one is a candidate for certification, and I briefed the ISSO accordingly.
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

U.S. Department of Commerce (DOC)
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)

Privacy Threshold Analysis (PTA)
For the
Wallops Command and Data Acquisition Station Administrative Local Area Network (NOAA5032)

Version: 1.0
February 12, 2018

U.S. Department of Commerce Privacy Threshold Analysis

Office of Satellite and Product and Operations (OSPO)

Unique Project Identifier: NOAA5032

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
(a) The Wallops Command and Data Acquisition Station (WCDAS) Administrative LAN (NOAA5032) is a General Support, office automation system that (b) is located within the WCDAS computer facility in Wallops Island, VA. (c) NOAA5032 relies on the NOAA NOC (NOAA 0200) for e-mail, and VPN access to NSOF (NOAA5044) for Internet connectivity. (d) The WCDAS Administrative LAN supports the NESDIS mission by providing IT resources to WCDAS personnel. Specifically, it is used to support electronic mail, purchasing, logistics, facility management, inventory, human resource, contract administration, general management functions and office automation functions (e) The WCDAS Administration LAN enables communication among OSPO and various NOAA groups to conduct administrative functions which include daily, weekly, monthly, and annual reports. The WCDAS Administration LAN is used to support electronic mail (GMAIL) through the use of Google, purchasing, logistics, facility management, inventory, human resource, contracts administration, general management functions, and office automation functions. (f) Types of data transiting thru or residing on the WCDAS Administration LAN include administrative email messages, data concerning time and attendance reports, status reports, travel orders, Federal grants, environmental monitoring, budget and capital planning, contingency planning, facilities management, workplace policy, human resources, goods acquisition, and IT infrastructure management. Data transiting or resident on the WCDAS Administrative LAN are typically in the form of e-mail messages, Excel spreadsheets, word processing documents, CAD drawings and simple databases resident on individual workstations. (g) The Users community of the WCDAS Administration LAN include management, technical, operations and administrative staff located at the Wallops Command and Data Acquisition Station. (h) Workstations located in the users' offices are used by the operational personnel, to log into their own user accounts on the WCDAS Domain where they can perform various administrative functions, and print to local and / or network printers. (i) A

dedicated DS-3 link provides the Wide Area Network (WAN) access from WCDAS Administration LAN to and from the Internet through the NOAA NOC.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

___ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X_ I certify the criteria implied by one or more of the questions above **apply** to the Wallops Command and Data Acquisition Station Administrative Local Area Network and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Wallops Command and Data Acquisition Station Administrative Local Area Network and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Owner (SO): Johnny R. Clark

Signature of SO: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK.JOHNNY.R.1365842791 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=CLARK.JOHNNY.R.1365842791 Date: 2018.02.14 09:32:40 05'00' Date: 2/14/2018

Name of Information Technology Security Officer (ITSO): Nancy A. DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.02.14 15:01:31 -05'00' Date: 02/14/2018

Name of Authorizing Official (AO): Vanessa L. Griffin

Signature of AO: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.01 14:40:34 05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark H. Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.01 16:00:06 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, March 2, 2018 9:02 AM
To:	James Schreiber NOAA Federal
Cc:	Mark Graff NOAA Federal; Isaac Sanvee NOAA Affiliate; Eric Most NOAA Federal; Mark Hall; jeffrey.vandam@noaa.gov; Bob Clark; _NESDIS HQ IT Security Team; OSPO.ITsecurity@noaa.gov; Nancy Defrancesco
Subject:	Re: NOAA5032_Re: PTA Expired on 2 15 2018
Attachments:	NOAA5032_PTA_Feb2018_for OSPO coAO signature vig mhg.pdf

Here's the signed PTA.

On Thu, Mar 1, 2018 at 3:58 PM, James Schreiber NOAA Federal <james.schreiber@noaa.gov> wrote:

> Thanks Sarah, the ISSOs are now working to update the PIA and complete the certification form and we will be sending back to you shortly.
>
> Regards, James
>
> On Thu, Mar 1, 2018 at 3:03 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Thanks, James. I'll send to Mark for signature and return to you.
> >
> > Since no new privacy risks, we can go ahead and do a certification to that effect, and send to DOC at least a couple of months before your ATO date. We will send them the signed PTA, the previous PIA with most recent ATO date put in Section 8.1, and Question 1.1 answered with "approved PIA and no new privacy risks".
> >
> > Here's the previous PIA in Word for you to make those changes and circulate for signatures.
> >
> > And here's the certification form which needs just one NESDIS signature (whoever best to state no new privacy risks), then I will sign as the Privacy Act Officer, and then Mark.
> >
> > If you have time to work on this now, we can go ahead and send to DOC and they will sign in plenty of time for your next ATO date.
> >
> > On Thu, Mar 1, 2018 at 2:50 PM, James Schreiber NOAA Federal <james.schreiber@noaa.gov> wrote:
> >
> > > Sarah and Mark, for your review and signature approval, please see attached PTA for WCDAS LAN NOAA5032.
> > >
> > > Thank you, James
> > >
> > > Sarah D. Brabson
> > > IT Infrastructure Investment Program Manager
> > > PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

James Schreiber, CISSP, PMP, CIPP/G, GCIH
4231 Suitland Road
NSOF Rm: 1405
Suitland, MD 20746
Ph: (301) 817 3891

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

U.S. Department of Commerce (DOC)
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)

Privacy Threshold Analysis (PTA)
For the
Wallops Command and Data Acquisition Station Administrative Local Area Network (NOAA5032)

Version: 1.0
February 12, 2018

U.S. Department of Commerce Privacy Threshold Analysis

Office of Satellite and Product and Operations (OSPO)

Unique Project Identifier: NOAA5032

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
(a) The Wallops Command and Data Acquisition Station (WCDAS) Administrative LAN (NOAA5032) is a General Support, office automation system that (b) is located within the WCDAS computer facility in Wallops Island, VA. (c) NOAA5032 relies on the NOAA NOC (NOAA 0200) for e-mail, and VPN access to NSOF (NOAA5044) for Internet connectivity. (d) The WCDAS Administrative LAN supports the NESDIS mission by providing IT resources to WCDAS personnel. Specifically, it is used to support electronic mail, purchasing, logistics, facility management, inventory, human resource, contract administration, general management functions and office automation functions (e) The WCDAS Administration LAN enables communication among OSPO and various NOAA groups to conduct administrative functions which include daily, weekly, monthly, and annual reports. The WCDAS Administration LAN is used to support electronic mail (GMAIL) through the use of Google, purchasing, logistics, facility management, inventory, human resource, contracts administration, general management functions, and office automation functions. (f) Types of data transiting thru or residing on the WCDAS Administration LAN include administrative email messages, data concerning time and attendance reports, status reports, travel orders, Federal grants, environmental monitoring, budget and capital planning, contingency planning, facilities management, workplace policy, human resources, goods acquisition, and IT infrastructure management. Data transiting or resident on the WCDAS Administrative LAN are typically in the form of e-mail messages, Excel spreadsheets, word processing documents, CAD drawings and simple databases resident on individual workstations. (g) The Users community of the WCDAS Administration LAN include management, technical, operations and administrative staff located at the Wallops Command and Data Acquisition Station. (h) Workstations located in the users' offices are used by the operational personnel, to log into their own user accounts on the WCDAS Domain where they can perform various administrative functions, and print to local and / or network printers. (i) A

dedicated DS-3 link provides the Wide Area Network (WAN) access from WCDAS Administration LAN to and from the Internet through the NOAA NOC.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

___ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X_ I certify the criteria implied by one or more of the questions above **apply** to the Wallops Command and Data Acquisition Station Administrative Local Area Network and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Wallops Command and Data Acquisition Station Administrative Local Area Network and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Owner (SO): Johnny R. Clark

Signature of SO: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK.JOHNNY.R.1365842791 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=CLARK.JOHNNY.R.1365842791 Date: 2018.02.14 09:32:40 05'00' Date: 2/14/2018

Name of Information Technology Security Officer (ITSO): Nancy A. DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.02.14 15:01:31 -05'00' Date: 02/14/2018

Name of Authorizing Official (AO): Vanessa L. Griffin

Signature of AO: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.01 14:40:34 05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark H. Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.01 16:00:06 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, March 2, 2018 2:59 PM
To:	Mark Graff NOAA Federal
Cc:	Sally Bibb
Subject:	Fwd: DRAFT Suggested edits to SORN 19
Attachments:	Privacy Act NOAA 19 PA SORN (2015 07 23) akr bibb_sb.docx

Mark Shared with you a couple of weeks ago, this is where we left off.

thx Sarah

Forwarded message
From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Mon, Feb 12, 2018 at 9:53 AM
Subject: Re: DRAFT Suggested edits to SORN 19
To: Sally Bibb NOAA Federal <sally.bibb@noaa.gov>
Cc: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Sally, I went over this again and thought that since in the other routine uses we do not go into nearly as much detail, I made an edit using track changes. I also didn't know that we make applications available to the public.

Please see attached.

On Fri, Feb 9, 2018 at 9:18 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Looks good. Since this is a NOAA wide routine use, I had already involved Mark Graff, our NOAA Privacy and FOIA Officer. But why not an Alaska person as well? We don't usually put this much detail into a routine use, but I started to do so with my first draft.
>
> On Fri, Feb 9, 2018 at 9:01 PM, Sally Bibb NOAA Federal <sally.bibb@noaa.gov> wrote:
>
> > Hi Sarah I took a stab at editing the routine use statement for the things that we release to the public on web sites or in response to ad hoc requests for information.
> >
> > (b)(5) [redacted]
> >
> > [redacted]. What do you think about that addition?

Mainly wanted your general review to see if the things I added to the routine use paragraph seemed appropriate.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, March 5, 2018 9:44 AM
To:	Thomas Grigsby NOAA Affiliate; Maxine Reid NOAA Affiliate; Jean Apedo NOAA Federal; Hadona Diep; Cameron Shelton NOAA Federal
Cc:	Mark Graff NOAA Federal
Subject:	Fwd: FW: FW: Final NOAA1200 PIA, pdf'd for signatures
Attachments:	NOAA1200 PIA 022818 for signatures_AO approval mhg.pdf; PTA Template 01 2017_instructions corrected.docx

NOAA1200 PIA signed by Mark. I will send this to DOC, asking for an expedited review. But in the meantime, I belatedly realized the PTA needs updating from April . . . for one thing, it says no new privacy risks and DOC requires a current PTA for the CRB, that agrees with the privacy risk/no privacy risk answer on the PIA.

Here's the current PTA template. Most of the outline from the PIA system description matches, just a couple of items are different, so you can mostly copy and paste.

I'll tell DOC that we'll have the new PTA before the CRB.

Sorry, should have noticed sooner the need for update . .

thx Sarah

Forwarded message
From: **Mark Graff - NOAA Federal** <mark.graff@noaa.gov>
Date: Mon, Mar 5, 2018 at 9:09 AM
Subject: Re: FW: FW: Final NOAA1200 PIA, pdf'd for signatures
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>

Got it signed and attached.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Mon, Mar 5, 2018 at 8:58 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Mark, please sign asap!!

thx Sarah

Forwarded message
From: **Douglas Perry - NOAA Federal** <douglas.a.perry@noaa.gov>
Date: Mon, Mar 5, 2018 at 8:18 AM
Subject: Re: FW: FW: Final NOAA1200 PIA, pdf'd for signatures
To: Jean Apedo NOAA Federal <jean.apedo@noaa.gov>
Cc: Ann Madden NOAA Federal <Ann.Madden@noaa.gov>, Sarah Brabson <Sarah.Brabson@noaa.gov>, Mark Graff <Mark.Graff@noaa.gov>, Thomas Grigsby NOAA Affiliate <thomas.grigsby@noaa.gov>

See attached signed PIA. I suggest that we schedule a briefing prior to request for signature in the future. NOAA1200 hosts many applications and is one of our more complicated PIAs.

On Thu, Mar 1, 2018 at 2:45 PM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:

Doug,

Please find attached the latest version of NOAA1200 PIA. We'll be looking for a better method to review these documents going forward.

Thank you.

From: Sarah Brabson - NOAA Federal [mailto:sarah.brabson@noaa.gov]
Sent: Thursday, March 01, 2018 2:24 PM
To: Jean Apedo - NOAA Federal
Subject: Fwd: FW: Final NOAA1200 PIA, pdf'd for signatures

Jean, one last time and send to Doug . . .thx

Forwarded message
From: **Cameron Shelton - NOAA Federal** <cameron.shelton@noaa.gov>
Date: Thu, Mar 1, 2018 at 2:00 PM
Subject: Re: FW: Final NOAA1200 PIA, pdf'd for signatures
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
Cc: Jean Apedo NOAA Federal <jean.apedo@noaa.gov>, Maxine Reid NOAA Affiliate <maxine.reid@noaa.gov>, Thomas Grigsby NOAA Affiliate <thomas.grigsby@noaa.gov>, Ann Madden NOAA Federal <Ann.Madden@noaa.gov>

On Thu, Mar 1, 2018 at 12:26 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

HI, Cameron, one last time, could you sign this PIA and send to Jean? thx

On Thu, Mar 1, 2018 at 8:42 AM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:

Good morning Cameron,

This is the final version approved by Doug. Please sign and forward to Doug and Ann. Kindly copy me and Sarah.

Thank you.

From: Douglas Perry - NOAA Federal [mailto:Douglas.A.Perry@noaa.gov]
Sent: Thursday, March 01, 2018 8:28 AM
To: Sarah Brabson - NOAA Federal
Cc: Ann Rivers; Jean Apedo - NOAA Federal; Maxine Reid - NOAA Affiliate; Thomas Grigsby - NOAA Affiliate
Subject: Re: FW: Final NOAA1200 PIA, pdf'd for signatures

Thanks for answering my questions and incorporating recommended changes. Please route this version for final signatures.

Best regards,

Doug

On Wed, Feb 28, 2018 at 3:46 PM Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Doug, here is the revised PIA, sorry for the earlier omission. thx Sarah
>
> On Wed, Feb 28, 2018 at 3:39 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> Doug Here's the unsigned PIA with the building entry card reader added in Section 3.1 attached. Just don't want to start with the new signatures again until you let us know you're okay with this version.
>
> thanks, Sarah
>
> On Wed, Feb 28, 2018 at 2:49 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Doug, do you still have issues? Do you want the letters removed from the paragraphs in the system description. We have added the building entry card reader.

Anxiously yours, Sarah

On Wed, Feb 28, 2018 at 2:24 PM, Douglas Perry NOAA Federal <douglas.a.perry@noaa.gov> wrote:

where is the template and questions?

On Wed, Feb 28, 2018 at 2:22 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

The a,b and c are from the new DOC template, as I stated. They are questions we are asked to address in the system description.

I will ask system folks about C Cure and relation to building entry card readers. If a simple check is needed, we'll add it.

On Wed, Feb 28, 2018 at 2:14 PM, Douglas Perry NOAA Federal <douglas.a.perry@noaa.gov> wrote:

Sarah,

Thanks for answering the earlier questions.

I still don't understand the significance of the letters (ie, "a,b and c").

If C-Cure is in the boundary of this system, why isn't the "Building entry readers" box checked in 3.1?

On Tue, Feb 27, 2018 at 4:24 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Hi, Doug I explained the letters in the system description.

AIS is now spelled out as Application Information System.

We removed a checkmark stating no new technologies in 2.5, where biometrics was checked.

C Cure is indeed in the system boundaries. It's listed in the Appendix after the signature page.

Also, regarding the choice of high confidentiality level, Mark reminded us from last year's DOC PIA review: The combination of credit card info, along with SSNs, and Financial account information, being leveraged for the GSS purposes of NOAA1200, was determined to meet the threshold--not because of the volume of PII, but rather that any breach, under the NIST 800-122 standard, would be catastrophic and lead to a complete compromise of the identity, financial, and security information of the individuals affected. In particular, the System sharing with OSY, CFO, and GC transverses virtually every Sensitive PII field captured in the PIA, and the compromise of that data meets the 800-122 standard (remember that, unlike the FIPS 199 "High" standard, the 800-122 standard is not limited by the number of individuals for whom the compromise would cause catastrophic loss).

If this information suffices, we will send you the PIA for signature, as soon as we have Cameron's and Jean's.

thx Sarah

On Tue, Feb 27, 2018 at 11:56 AM, Douglas Perry NOAA Federal <douglas.a.perry@noaa.gov> wrote:

> Jean,
>
> See comments below:

In the Introduction section, there are letters, such as "a,b and c" at the beginning of paragraphs... what is the purpose of these? The paragraph beginning "d,e and f" has an acronym "AIS" that isn't defined... what does this stand for?

Section 3.1 has "Building entry readers" unchecked ... is C-Cure within the system boundary?

Section 11.1 indicates that the potential impact is "High" ... how would disclosure of the information contained in NOAA1200 have a "severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals"? The "high" determination contradicts the following section (Section 11.2) which indicates that the confidentiality impact level is "moderate" in the "Data Field Sensitivity" section.

On Fri, Feb 16, 2018 at 10:03 AM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:

Good morning Doug,

Attached is NOAA1200 PIA for your approval. Please note that the ATO is due in about 4 weeks.

Thank you.

From: Sarah Brabson - NOAA Federal [mailto:sarah.brabson@noaa.gov]
Sent: Friday, February 16, 2018 9:55 AM
To: Jean Apedo - NOAA Federal
Cc: Mark Graff - NOAA Federal
Subject: Re: Final NOAA1200 PIA, pdf'd for signatures

Doug

~~~~~~

Douglas A. Perry

Deputy Chief Information Officer
National Oceanic and Atmospheric Administration

Office: (301) 713-9600

www.noaa.gov

~~~~~~

Douglas A. Perry

Deputy Chief Information Officer
National Oceanic and Atmospheric Administration

Office: (301) 713-9600

www.noaa.gov

The contents of this message are mine personally and do not necessarily reflect any position of NOAA.

U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Impact Assessment
for the
CORPORATE SERVICES (CorpSrv), NOAA1200

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NOAA1200, CorpSrv

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

a, b and c - NOAA1200 / CorpSrv, is a General Support System (GSS) consisting of multiple subsystems. NOAA1200 is hosted in the NOAA network infrastructure and not a standalone system.

The NOAA1200 core system consists of user desktop and laptop workstations, Microsoft Windows' file and print servers, a limited number of network infrastructure components that support NOAA's executive offices and corporate financial and administrative services Program Support Units located at sites within the United States.

1. Boulder, CO;
2. Fairmont, WV;
3. Germantown, MD;
4. Honolulu, HI;
5. Kansas City, MO;
6. Largo, MD; and
7. Newport, OR;
8. Norfolk, VA
9. Norfolk, VA;
10. Seattle, WA;
11. Silver Spring, MD;
12. Tampa, FL;
13. Washington, DC.

NOAA1200 supports a user base of approximately 3,000 users, and provides connectivity to the NOAA network for both local and remote access to the following basic administrative services: collaboration platforms includes Google Suite for government cloud, file servers, printing; file backup and restoration; and account management and storage.

d, e, and f - NOAA1200 workstations allows Application Information System (AIS) users (including Trusted Agents) to connect to other privacy systems of record. The process of submitting, retrieving and storing sensitive information varies with each of the various privacy systems users connecting via CorpSrv workstations. Residual data from other privacy systems may be stored, and/or processed on user workstations or file servers.

Trusted Agents and other users access privacy systems with CorpSrv workstations. Trusted Agents and other users may store Form CD591 (PIV request form) used for government issued identification cards on corpsrv systems for archival purposes. These records which are submitted and processed in other government privacy systems of record may include fingerprints and a photograph, driver's license and passport numbers. OF-306 Declaration for Federal Employment may be archived in CorpSrv when scanned for submission to a personal security office.

g. - NOAA1200 shares data with twelve hosted applications, including Acquisition and Grants Office, Office of Civil Rights, Workforce Management office, General Counsel and the Office

of the Chief Financial Officer, among others.

Unified Messaging Service (UMS) / Google Government Suite (G-STE)

Google Services is comprised of Google's multi-tenant public and hybrid Google Apps cloud instances and multi-tenant public cloud Google App Engine. These services are built atop the Google Common Infrastructure. Google Apps is a Software-as-a-Service (SaaS) cloud deployment model that allows customers the ability to communicate, store files and collaborate with Gmail, Hangouts, Talk, Calendar, Drive, Docs, Sheets, Slides, Vault, Sites, Groups, Contacts and Classroom while managing their domain with the Admin Console. Google App Engine is a Platform-as-a-Service (PaaS) cloud deployment model, providing customers an environment to easily build, run and manage their applications on Google's infrastructure.

G-STE is assessed and authorized (A&A) under the FedRAMP program, administered by the US GSA. It is authorized as a MODERATE Impact system which is adequate for the NOAA owned data processed and stored there. NOAA1200 users are not authorized to use G-STE for processing and storage of sensitive PII/BII, which is covered in the annual NOAA Information Technology Security Awareness Course (cyber security training).

Mobile Device Management (MDM) / IBM MaaS360

The IBM MaaS360 is a comprehensive, cloud-based security and management platform for NOAA mobile devices, applications and content. NOAA uses MaaS360 to protect data and optimize productivity, enabling employees to work anytime and anywhere through trusted mobile interactions. MaaS360 provides a cloud based, on-demand software-as-a-service (SaaS) delivery model, built on a secure, multi-tenant architecture.

The Mobile Device Management IBM MaaS360 platform currently allows the use of facial recognition for unlocking mobile devices. This technology utilizes iris and retina scans, and other facial features including the depth, contour and shape of the face, as well as one's gaze to unlock mobile devices. However, users must also establish a passcode which can be used to bypass the facial data to unlock the devices. The biometric data collected by the device is stored, processed and encrypted locally on each device. The collection of the facial images is incidental to the device use. This data will not be collected in a system of record and will not be shared or retrieved by anyone within or outside the bureau. The only exception to this is in cases where the phone data, including the PII data collected by the phone is shared, if necessary, with law enforcement.

MDM Federal Information Security Management Act (FISMA) Risk Management Framework (RMF) Assessment and Authorization (A&A) are met via the Federal Risk and Authorization Management Program (FedRAMP).

AODocs

AODocs is a document management system that will allow NOAA to collaborate on its Google services solution to organize business critical documents, migrate files from legacy document management systems, implement business workflows, manage documents with metadata and apply document retention policies entity-wide. This solution is not yet in use at NOAA, however, in the future it will be used to distribute Standard Operating Procedures, manage

quality control processes, and assist in the coordination of contract management, procurements, intranet publication and incident reporting. AODocs will not store any NOAA data on its servers, it will only leverage the Google cloud platform (Google App engine and Google Datastore). Google Drive data will remain in the G suite environment. While AODocs is not FedRAMP certified, it will rely on Google infrastructure to deliver its product (G Suite) and backend (Google Cloud Platform). Google is FedRAMP certified.

Skyhigh

NOAA has acquired Skyhigh Cloud Access Security Broker (CASB) to implement Data Loss Prevention (DLP), which will be utilized to enforce PII policies for data at rest stored on NOAA's Google Drive. Skyhigh will perform scans of data files stored on the Google Drive to identify data in violation of privacy policy. SDD DLP Administrator and NOAA POCs are working with the SOC and NCIRT to determine what actions will be taken upon notification of a PII policy violation from the DLP engine. PII policy violation log information will be sent to Arcsight in real time in collaboration with the NOAA SOC. Skyhigh Federal Information Security Management Act (FISMA) Risk Management Framework (RMF) Assessment and Authorization (A&A) requirements are met via the Federal Risk and Authorization Management Program (FedRAMP).

g. Information will be shared only within the bureau, with the case by case exception that information may be disclosed to another Federal agency in connection with the assignment, hiring or retention of an individual, the issuance of a security clearance, the reporting of an investigation of an individual.

h. Statutory authorities:

1. 5 U.S.C 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
2. America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science (COMPETES) Act (Public Law 110-69, Section 4002).
3. From NOAA-14: National Marine Sanctuaries Amendments Act of 2000 (Public Law 106-513 Section 318).
4. From DEPT-1: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309.
5. From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
6. From DEPT-18: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
7. From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

8. From OPM/GOVT-2: Sections 1104, 3321, 4305, and 5405 of title 5, U.S. Code, and Executive Order 12107.
9. From DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 (HSPD 12), Federal Property and Administrative Services Act of 1949, as amended.

i. This system has a FIPS 199 moderate impact level.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X*
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	

* The existing changes to the NOAA1200 will result in an increase in the sensitive PII, facial and biometric data processed by the system. The sensitive PII data reside within the hosted system networks and locally on users workstations. The facial data from the mobile devices will be stored on mobile devices if selected. Skyhigh and AODocs are future subsystems not yet operational.

In addition, Trusted Agents and other users access privacy systems with CorpSrv workstations. Trusted Agents and other users may store Form CD591 (PIV request form) used for government issued identification cards on corpsrv systems for archival purposes. These records which are submitted and processed in other government privacy systems of record may include fingerprints and a photograph, driver's license and passport numbers. OF-306 Declaration for Federal Employment may be archived in CorpSrv when scanned for submission to a personal security office.

____ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID	X	i. Credit Card	

b. Taxpayer ID (TIN)	X	f. Driver's License		j. Financial Account	X
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Storage is not duplicative among hosted offices: acquisition and grants, workforce management, financial, and security collect and store SSNs in their different capacities, from different populations: employees, contractors, non-NOAA customers. Authorities are those from DEPT-18 and OPM/GOVT-1, listed in the system description.

Sensitive information is stored and processed in NOAA1200 as a result of routine business processes within the NOAA organizations supported, authorized under 1. 5 U.S.C 301. There is also temporary storage of the OF-306 before transmitting to the security office.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	X*
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify): Education level, school transcripts, field of study, references, performance measure results while in scholarship program, and postgraduate activities, national origin, disability.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance information, FBI Name Checks and arrest records, foreign travel forms, accident/incident reports.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	X
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify): Facial features					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): Passcodes Audit data specific to when sensitive PII/BII is processed or stored in NOAA1200 is not collected. Audit information should be collected by applicable privacy systems of records when NOAA1200 users access those systems using NOAA1200 workstations.					

*Religion data is being collected from The Office of Civil Rights for NOAA complaints of discrimination, demographic reports, investigations, civil rights reports, etc.

Other Information (specify)
The Mobile Device Management IBM MaaS360 platform currently allows the use of facial recognition for unlocking mobile devices. This technology utilizes iris and retina scans, and other facial features including the depth, contour and shape of the face, as well as one's gaze to unlock mobile devices. However, users must also establish a passcode which can be used to bypass the facial data to unlock the devices. The biometric data collected by the device is stored, processed and encrypted locally on each device. The collection of the facial images is incidental to the device use. This data will not be collected in a system of record and will not be shared or retrieved by anyone within or outside the bureau. The only exception to this is in cases where the phone data, including the PII data collected by the phone is shared, if necessary, with law enforcement.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): PII received from DOC Bureaus is incidental to NOAA1200 support function for the SO/LOs.					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3. Describe how the accuracy of the information in the system is ensured.

Edit checks are in place within NOAA1200 to ensure accuracy of data input. Otherwise, for applications hosted on NOAA1200, information may verified or rejected by application users. Some applications use automated means and some human intervention.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. Some of the information is covered under OMB Control No. 0648-0568, National Oceanic and Atmospheric Administration: (1) Office of Education, Educational Partnership Program (EPP), (2) Ernest F. Hollings Undergraduate Scholarship Program amd (3) Dr. Nancy Foster Scholarship Program
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	X
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			
There are no technologies used that contain PII/BII in ways that have not been previously deployed.			

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	X
Video surveillance		Electronic purchase transactions	
Other (specify): Facial recognition			
There are no IT system supported activities which raise privacy risks/concerns.			

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Financial, education/training			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

1. Names, addresses, e-mail addresses, age, race, national origin, disability, gender, maiden name, alias, SSNs, photographs, place of birth, and date of birth are collected and maintained to enable NOAA to identify to whom we are issuing a badge (employees and contractors).
2. Names, addresses, e-mail addresses, SSNs, place of birth and date of birth, photographs, fingerprints, FBI Name Checks and arrest records, foreign travel forms and passport numbers are used to create and support records for the submission of security investigations, for potential employees or contractors (members of the public).
3. Names, addresses, e-mail addresses, race, national origin, disability, gender, home phone number, education, medical information, military service, work history, email address, and SSNs are used for eligibility for hiring employees (members of the public).
4. Names, occupations, job titles, salaries and performance information are used to create and maintain federal employee performance reviews (federal employees)
5. Names, addresses, e-mail addresses age, race, religion, national origin, disability, gender, employee ID, employee case number and SSNs are collected for labor issues, civil enforcement activities and litigations (federal employees).
6. Names, addresses, age, financial account, financial transactions and SSNs are collected and maintained to facilitate payroll information and records (federal employees).
7. Names, addresses, e-mail addresses, age, race/ethnicity, gender, DOB, citizenship, education level, school transcripts, field of study, references, performance measure results while in program, and postgraduate activities are used to determine awards and track students in the (1) Office of Education, Educational Partnership Program; (2) Ernest F. Hollings Undergraduate Scholarship Program; (3) Dr. Nancy Foster Scholarship Program; and (4) National Marine Fisheries Service Recruitment, Training, and Research Program (members of the public).
8. User ID, IP Address, Date/Time of Access, Queries Run, ID Files Accessed and Passcodes are collected for system administration, including system security (federal employees).
9. The Mobile Device Management IBM MaaS360 platform currently allows the use of facial recognition for unlocking mobile devices. This technology utilizes iris and retina scans, and other facial features including the depth, contour and shape of the face, as well as one's gaze to unlock mobile devices. However, users must also establish a passcode which can be used to bypass the facial data to unlock the devices. The biometric data collected by the device is stored, processed and encrypted locally on each device. The collection of the facial images is incidental to the device use. This data will not be collected in a system of record and will not be shared or retrieved by anyone within or outside the bureau. The only exception to this is in cases where the phone data, including the PII data collected by the phone is shared, if necessary, with law enforcement.
10. The Trusted Agents collect and store Form CD591 (PIV request form) for government issued IDs, LDAP and Active Directory. The Trusted Agents process security and badging forms for contractors only, not Federal employees. The processing package may include fingerprints and a photograph, both taken by the badging office (*but not stored in the system*), driver's license and passport number. This information is stored locally for each user on the CorpSrv NOAA1200 workstations. However, the Trusted Agents roles and responsibilities remain with the subject system. Once the Eastern Region Security Office approves a contractor for a CAC, it returns the CD-591s for the sponsored contractors and they are stored electronically. Trusted agents are instructed to complete only Section A of the CD-591. They do not include the I-9 form and have never been requested to do so by OSY.

    OF-306 Declaration for Federal Employment is stored temporarily when the form needs to be scanned and saved to a drive prior to uploading into Accellion Secure File transfer to send to the Security Office. A paper copy of the Security Coversheet/Request for Investigation Coversheet is also stored after removing Birth Date and SSN. The only forms stored are redacted Coversheets and CD-591s which do not contain PII.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place

to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There is the potential threat that the privacy data being processed by the NOAA1200 users could be intentionally or unintentionally disclosed or shared with other unauthorized users. However, this risk is low because of the access, physical and logical security controls that are in place to prevent this from happening. NOAA1200 requires the use of CAC cards for physical and network access, and roles and privileges for application authorization. In addition, NOAA1200 users that are involved in the handling or processing of the privacy data for the hosted applications are required to review and sign the Rules of behavior and take mandatory training in order to minimize such risks. The users are required to adhere to NOAA's policies regarding disclosure and separation of duties.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X**		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach.

**In case of breach and to OSY.

	The PII/BII in the system will not be shared

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

The only collections conducted within the boundaries of NOAA1200 consists of the PII collected for the scholarship application program and the facial recognition feature of cellular phones. All other PII collections are conducted within the respective system boundaries of the Staff and Line Offices that own the data which may then be stored and/or processed by that office using NOAA1200. As such, the respective Privacy Act Statements pertaining to those Staff and Line Office collections are maintained within their originating FISMA systems, from which the information may then be stored and/or processed within the NOAA1200 system.

Privacy Act Statement - Facial Recognition Data

Authorities: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations and 44 U.S.C. 3101, Records Management by Agency Heads.

Purpose: The facial recognition feature is for accessing personal hand-held communications devices.

Routine Uses: The individual's access to the device by this means is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a). Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.

Disclosure: Adding this information to the device is voluntary; however, failure to provide accurate information may prevent the individual's device access.

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://oedwebapps.iso.noaa.gov/uspa/Default.aspx https://oedwebapps.iso.noaa.gov/USPA https://oedwebapps.iso.noaa.gov/SSTR/ https://oedwebapps.iso.noaa.gov/studentstracker/VAUS/ https://oedwebapps.iso.noaa.gov/studentstracker/ https://sites.google.com/a/noaa.gov/noaa-ums/ .	
X	Yes, notice is provided by other means.	Specify how: Owners of the hosted systems send notifications to individuals when information is required. Those systems which use federal-wide forms for collection have PASs. Please refer to the Appendix for these owners. For scholarship applicants, scholarship awardees and grantees, notice is given on the Web site and on the application and tracking forms, regarding the purposes and uses of the information given, along with both security and privacy notices. (A procedure required by the system of record and is not specific for NOAA1200) There is a PAS for the cellular phone facial recognition posted on the UMS Web site and posting on the phones is pending. For Trusted Agents Form CD591, the DOC PIV request form, provides notice in that the request for information comes from the sponsor and registrar. The information comes from the applicant, who completes the form and provides it to the sponsor. There is also a privacy act statement on this form.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Members of the public may decline to provide PII/BII directly to the application owners; however, they cannot be employed by NOAA/receive applicable services. NOAA1200 implements necessary controls to protect PII/BII. Information owners are responsible for implementing necessary, operational controls regarding collection, maintenance, and dissemination. Each collection procedure under the respective and applicable SORNs will have the prescribed notification procedures regarding opportunity to decline. The following applies to collection processes supported by NOAA1200: Federal employees and contractors may decline to provide the information, but must provide the information as a condition of employment. In general, information is required for the effective administration of the center, including continuity of operations in case of an emergency. On scholarship applications, not all information is required, and optional fields are marked as such. If required information is not given, applications will be declined. Links to the NOAA privacy policy are provided to employees, contractors and members of the public. For the facial recognition on cellular phones, this is entirely voluntary and not shared

		within the system. For Trusted Agents also, individuals can decline by not providing requested information to receive NOAA ID. However, without a NOAA ID, they cannot work at NOAA as a Federal Employee or Contractor.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: NOAA1200 implements necessary controls to protect PII/BII. Information owners are responsible for implementing necessary, operational controls regarding collection, maintenance, and dissemination. Each collection procedure under the respective and applicable SORNs will have the prescribed notification procedures regarding consent for use of their PII/BII. The following applies to collection processes supported by NOAA1200: Individuals are given an explanation in writing, on the applicable forms, from the application owners, as to why the required information must be provided (i.e. specific uses), as well as a link to the NOAA Privacy Policy. Per the privacy policy, completion of a form or otherwise providing the information implies consent to the particular uses of the information. For the cellular phone facial recognition, this feature is initiated by the cell phone holder and there are no other uses. For Trusted Agents, if no consent is granted, no ID will be issued as in 7.2 above. This is the only purpose for this information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: NOAA1200 implements necessary controls to protect PII/BII. Information owners are responsible for implementing necessary, operational controls regarding collection, maintenance, and dissemination. Each collection procedure under the respective and applicable SORNs will have the prescribed notification procedures regarding review and update of their PII/BII.

		The following applies to collection processes supported by NOAA1200: For scholarship programs, students may request to review their information from their supervisors and submit updates to them at any time. On the Web sites of all other hosted applications/offices, contact information for the staff office manager is given, with the stated purpose of requesting to review and update information. For the cell phone facial recognition feature, any update would be performed by the cell phone holder.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: This refers only to the SAAD data collected.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 3/22/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

1. Multifactor authentication 2. Anti-virus protection 3. Intrusion prevention and detection systems 4. Forensic analysis tools 5. Log analysis tools 6. Trusted Agents (TA) collect and maintain CD591, Declaration of Federal Employment (OF-306), OSY Cover Sheet and Fair Credit Forms. The CD-591 does not have have sensitive PII only name, job title, email address and phone number. The OF-306 and OSY Cover Sheet has sensitive PII. Initially, hard copy records were collected by the TA and stored in a secure location in a locked fireproof filing cabinet. More recently, the information is being sent electronically from Project Managers and users by Accellion, a secured email transfer, to the TA, who transfers it to the Security Office via the same method. The information is also stored locally on the TA's workstation.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: Department-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, Department-13, Investigative and Security Records, DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies, DEPT-25, Access Control and Identity Management System, GSA./GOVT-7, Personal Identity Verification Identity Management System, NOAA-14, Dr. Nancy Foster Scholarship Program, which has been revised to include Ernest F. Hollings Undergraduate Scholarship Program and the National Marine Fisheries Service Recruitment, Training, and Research Program alumni survey. Also, OPM/GOVT-1, General Personnel Records, OPM/GOVT-2, Employees Performance File Records would cover the personnel related records created and maintained by Supervisors, and WFMO, both those that go in the eOPF, and those held by the chain of command.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Requirements for record retention are found in the NOAA Records Schedules:

	100-24 Information Technology Operations and Management Records and 100-27 Records of the Chief Information Officer, p.12 and the (GRS) 24 and 27.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

From 2017 CRB: The combination of credit card info, along with SSNs, and Financial account information, being leveraged for the GSS purposes of NOAA1200, was determined to meet the threshold--not because of the volume of PII, but rather that any breach, under the NIST 800-122 standard, would be catastrophic and lead to a complete compromise of the identity, financial, and security information of the individuals affected. In particular, the System sharing with OSY, CFO, and GC transverses virtually every Sensitive PII field captured in the PIA, and the compromise of that data meets the 800-122 standard (remember that, unlike the FIPS 199 "High" standard, the 800-122 standard is not limited by the number of individuals for whom the compromise would cause catastrophic loss).

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Some individuals could be identified based on the information stored.
X	Quantity of PII	NOAA1200 includes the workstation disks and server file stores for the NOAA headquarters staff, who use their workstations on a daily basis to process and store PII/BII.
X	Data Field Sensitivity	Provide explanation: The confidentiality impact level is set at

		moderate because sensitive PII is present: e.g. SSN, biometrics, etc. in combination with additional non-sensitive PII.
X	Context of Use	Provide explanation: Facial recognition is on cell phones only and is not shared.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: For subject systems The information collected for badging purposes contains two forms of personal identification (ie Passport, Driver's license, etc.) which, if exposed during the course of collection and verification, could have an adverse impact to user confidentiality.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

NOAA1200 is a privacy system required to be compliant with all FISMA cybersecurity controls related to securing privacy systems. Annual assessments / audits by independent assessors provide what is believed to be adequate safeguards for protection of sensitive PII from unauthorized disclosure.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Cameron Shelton Office: NOAA OCIO Phone: (301) 628-5721 Email: cameron.shelton@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.	**Information Technology Security Officer** Name: Jean Apedo Office: NOAA OCIO Phone: (301) 628-5730 Email: Jean.Apedo@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.
SHELTON.CAMERON.L.1365843313 Digitally signed by SHELTON.CAMERON.L.1365843313 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn SHELTON.CAMERON.L.1365843313 Date: 2018.03.01 13:59:44 -05'00' Signature / Date signed	APEDO.JEAN.1188076064 Digitally signed by APEDO JEAN 1188076064 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=APEDO JEAN 1188076064 Date: 2018 03 01 08:38:50 05'00' Signature / Date signed
Authorizing Official Name: Douglas Perry Office: NOAA Deputy OCIO Phone: (301) 713-7673 Email: Douglas.A.Perry@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: (301) 628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.
PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.03.05 08:17:03 -05'00' Signature / Date signed	GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.05 09:09:23 05'00' Signature / Date signed

This page is for internal routing purposes and documentation of approvals.
Upon final approval, this page must be removed prior to publication of the PIA.

Appendix

System Sharing – All users of these systems are internal to the system owner's organization.

Business Function	Application / Resource	Type of PII	Comments
AGO (Acquisition and Grants Office)	Procurement, Grants, and Contract Data; N: drive	DOB; Address; SSN	Applications, Grant, Vendor and procurement information.
CAO - SECO (Office of the Chief Administrator - Safety and Environmental Compliance Office)	Local disk; \\hqs-is-fsvr1\dcao budget; SharePoint:	Personal information, i.e., name, address, DOB, SSN on DD-214, SF-50; employment documents	Resumes, transcripts, employment documents; Accident/ Incident reports; Passport Application
CAO CivRights (Office of Civil Rights)	NOAA Complaints of Discrimination; NOAA Demographic Data Reports; Complaint Investigator Reports; Civil Rights Office Personnel Information; Internally generated reports and databases	Name; address; SSN; age; race; national origin; disability; gender, religion; performance evaluation; etc.	
CAO BAIPS (Business Analysis & Investment Planning Staff)	Local disk; \\hqs-is-fsvr1\dcao budget; SharePoint.	Names & Employee Salary Information	
OCIO	Performance Reviews, SF52, Telework Apps, SF182, CD137, CD505, OGE 450 Financial Disclosure Reports, Various applications in GTOWN	Ratings, DOB, Addresses, SSN	Apps: NRS, Clearance Data, CAC, Epledge, NFC, COD, NOAA CORPS Payroll, POL/SF113, HR Reports, CAMS/BXA/Labor
EPP/OED (Educational Partnership Program-Office of Education)	Scholarship Applications on N: drive	Address, DOB, School & Other PII	
Office of Security	C-Cure	SSN, photographs, fingerprints	SSN, photographs, and fingerprints used for identity check on a single computer in that office for FBI SOR.
	M: drive (shared drive for each division)	DOB, POB, SSN, FBI Name Checks and arrest records, foreign travel forms	
WFMO (Workforce Management Office)	SharePoint Site	Address, Phone Numbers, SSN, User ID, DOB, Passcodes	Resumes, hiring letters, insurance forms, eOPF docs (copies)
NMFS	NMFS SharePoint 2013 DWH/DARRP SharePoint 2013	CD-541 (performance rating), Telework Agreement, Government Purchase Card Statement	
DUS (Department of Undersecretary, **CROM** (Chief, Resource & Operations Management), **EXSEC** (Office of the Executive Secretary)	N: Drive	Personal information, i.e., name, address, DOB, SSN on DD-214, SF-50; employment documents	Resumes, transcripts, employment documents; Accident /Incident reports; Passport Applications
GC (General Counsel)	N: Drive	DOB, POB, SSN	Security Cover Sheets
CFO (Office of the Chief Financial Officer)	CBS vendor, Grant conversion/issue resolution, internal and external data call support	TIN, ABA, SSN, DOB, Bank Info	Most files are Secure Zipped, Encrypted, and password protected
GC SSMC (Silver Spring Metropolitan Campus)	N: and C: Drives	SF-50s, OPFs with DOBs and SSN	

NOTE Re shared drives: Access controls are applied to all systems per DOC CITR-022 Access and Use Policy, NOAA Rules of Behavior, and NOAA IT Security Manual Section 16.0 Access Controls. See DOC / NOAA SORNs that may be applicable at the following weblink: (http://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/).

Version Number: 01-2017

U.S. Department of Commerce
[Bureau Name]

Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):
_____

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____

Privacy Council

From:	Privacy Council
Sent:	Monday, March 5, 2018 10:40 AM
To:	PRIVACY COUNCIL@LISTSERV.GSA.GOV
Subject:	[PRIVACY COUNCIL] Agency Implementation Call TODAY!
Attachments:	2017.12.15 Final Guide to Conducting a PII Breach Table Top Exercise.docx

A word from Becky, Claire and Sam:

The Agency Implementation Committee is hosting our monthly call today at 2pm. We would love to have you call in and join the conversation. Our hope is that the monthly meeting will give you the highlights of the SAOP discussion at the Federal Privacy Council monthly meeting, highlight requirements we all need to meet, and provide a place where the entire privacy community can gather to talk about the opportunities and challenges facing all of us. Our hope is that we can share some of the work that each of our agencies have done, so that other agencies can benefit from that work.

Who should attend? Anyone in the Federal privacy community!

Who can ask questions? Anyone!

Here are our official goals:

The Agency Implementation Committee Goals:
Communicate with Federal Privacy workforce, including sharing information with the federal privacy workforce about the SAOP activities, Identify pressing issues, and Build and foster and collaborative environment to leverage expertise across the privacy community so lessons learned can be shared.
This meeting will be a recurring meeting, providing the privacy community with a briefing from the SAOP monthly meeting and providing a time for communication and collaboration across the privacy community.

Our Agenda for Monday's meeting:

Welcome
AIC listserve changes
Privacy Continuous Monitoring (DHS)
Managing Research Data from a Privacy Perspective (Dept of Education)
Task Force Conversations
- Risk Management
- Breach Response (Table Top Exercise Guide attached)
- Shared Services
- Controlled Unclassified Information

Call for topics for the Privacy Summit
Highlights of SAOP training session on General Data Protection Regulation
Question Time

AIC List Serve

We view the listserve as an online compliment to our monthly meetings and conference calls. We invite all members of the AIC to post and share here, for example any best practices you or your agency have

developed, any knowledge or news you wish to provide to your colleagues, or proposals for further developing a unified approach for addressing Federal privacy challenges. Please do not use this listserve to post personal messages, for example transfer or retirement notices.

Dial in information:
(b)(6) [redacted]

Claire Stapleton
Chief Privacy Officer
Consumer Financial Protection Bureau

1700 G St, 6100

Tel: 202 435 7318
Mob: (b)(6) [redacted]

consumerfinance.gov

Guide to Conducting a PII Breach Table Top Exercise (TTX)

Before you start

1. Ensure the agency's Breach Response Plan is up to date and identifies the Breach Response Team (BRT) members and their respective responsibilities. Also identify potential ad hoc members of the BRT who may be needed depending on the nature of the breach (e.g., medical, financial, third party vendor).
2. Ensure BRT members understand their responsibilities under OMB Memorandum M 17 12*, Preparing for and Responding to a Breach of Personally Identifiable Information*, and have reviewed the agency's Breach Response Plan prior to the TTX. Consider conducting breach response training for BRT members.

Planning

1. Establish the objectives of the TTX. Some of your objectives may be:
    a. Improve the understanding of your Breach Response Plan.
    b. Identify opportunities to improve your Breach Response Plan and the agency's preparedness.
    c. Identify interdependencies among agency organizations and third party service providers.
2. Plan the TTX logistics.
    a. Reserve a space with an appropriate clearance level, as well as any materials or multimedia support you may need, such as computer and display, whiteboard and markers, butcher block paper, handouts, and dial in capabilities.
    b. Set a time limit for the TTX. This will help you choose an appropriate scenario and focus the conversation appropriately during the TTX.
    c. Assign support staff roles.
        i. Determine what role you want your privacy program to play in the exercise. Individuals who are deeply involved in planning the TTX may need to take a step back during the exercise to avoid accidently influencing the course of the exercise. In a TTX, privacy office representatives often act in an advisor or consultant role, responding to questions from other participants, rather than the active leaders they often are in an actual breach.
        ii. Consider using a neutral facilitator.
        iii. In addition to a facilitator, you will also need staff dedicated to:
            1. Taking notes. These notes will form the basis of the after action report.
            2. Tracking "parking lot" issues.
            3. Documenting when Breach Response Plan steps are completed.
    d. Create a participant roster to track attendance at the TTX.
    e. Consider what role you want Senior Executive Service (SES) members and other senior leaders to play. SES member participation may stifle the conversation. Consider using SES members or other senior leaders as floaters who give out real time feedback.

3. Develop a realistic breach scenario.
    a. Choosing a scenario.
        i. Consider which high value assets, applications, or processes you may want to include in the scenario.
            1. You do not have to limit yourself to high value assets, but you want to make sure the scenario has stakes. A high profile system or program, or a scenario that involves risks to the reputation or operations of the agency may be more engaging and offer more avenues for the participants to explore.
        ii. Look at your agency's recent breaches, as well as any major breaches, for ideas.
        iii. Review your agency's breach metrics to see where you have trends that may indicate a weakness or identify an issue about which you receive questions or complaints and consider developing a scenario around those fact patterns.
        iv. Consider breaches that will engage all of the participants. For example, a loss of hardcopy documents may not effectively engage a participant from the cybersecurity team. A scenario that requires cross functional collaboration (e.g., between staff supporting Freedom of Information Act (FOIA), privacy, cybersecurity, and human resources) is often a more effective TTX.
        v. Balance the complexity of the TTX with the knowledge and experience the BRT members have with handling a breach. A too simple scenario may not be an effective use of this training and awareness opportunity; a too complex scenario may make it difficult for participants to engage in the TTX.
    b. Refining the scenario.
        i. After you have chosen the breach you would like to test, speak with the relevant program office and/or system owners to ensure that you understand their data and processes. The scenario should be grounded in reality.
        i. Create a scenario that evolves over time. Create injects that complicate the scenario by adding additional facts. Provide a realistic timestamp for each update to help participants track their compliance with reporting requirements and understand how long actual breach response activities may take.
        ii. You should be able to map your organization's Breach Response Plan steps to the steps in your TTX; this will help you ensure that you have not forgotten any aspects of your Breach Response Plan in the development of the scenario. Consider creating a table or grid citing back to the plan to ensure you know each BRT member's role and responsibility.
        iii. Try to make the TTX as interactive as possible. Break the scenario into modules with injects to keep participant attention and focus the discussion.
4. Create supporting artifacts, such as breach reports, supplemental reports, and after action reports.
    a. If your agency uses breach reporting forms, including supplemental reports and after action reports, create versions for the exercise. Using existing artifacts may highlight areas that need clarification or improvement.
    b. You may want to create additional artifacts, such as dummy data file examples and external press reports.

c. Be sure to label all documents created for the TTX with "For exercise purposes only."
d. It can be helpful to have packets available to the participants that include your agency's breach response policy, the initial scenario, the injects, and any other supporting materials. The participants should not view the injects until they are directed to by the facilitator.

5. Provide an executive summary of the goals of the breach response program, its importance, and the goals and relevance of the TTX for senior leadership prior to TTX.

Execution

1. Share the TTX ground rules with the participants.
   a. Stress that this is a learning exercise and that participants should feel comfortable asking questions or throwing out ideas. There are no wrong answers and everyone's opinion will be considered.
   b. Emphasize that participants should not "fight the scenario." Every effort will have been made to ensure that the scenario is realistic and reflects actual practices.

Examples of TTX Ground Rules
• Silence cell phones and other mobile devices during the exercise. • Accept that the circumstances surrounding the event are real. • This is a "no-fault" environment where varying viewpoints and disagreements are to be expected. There are no wrong answers.

2. Present the initial facts of the scenario to the participants. Use prompts to encourage interaction if the conversation is slow to start.
3. Participants should begin to identify immediate actions that should be taken, including establishing a communications plan and, if appropriate, Congressional notification plan.

Examples of Questions the BRT Should Consider
• Is there a SORN or PIA? • What other agency stakeholders or partners should be made aware of the breach? • Who reports the breach to Congress? • Who will need to approve any notices, notifications, and other communications? • Who would be the source of the notification? Is any official designation required? • How and who will fund identity protection services (IPS)? • Does the CFO need to be engaged before securing IPS? • Is there a vendor engaged for call center and IPS?

4. Start to provide injects to the scenario that reflect the types of information you would learn from a breach investigation.
   a. With each inject, participants should identify the actions that should be taken based on the updated information.
   b. You can also ask questions that explore other potential aspects of the breach. For example, if your breach involves information about members of the public only, you can ask them whether they would do anything differently if employee information was included.
5. Have participants complete a post TTX survey before leaving to get their input on the quality and strengths of the TTX, suggestions for improvement, and recommendations for future TTX scenarios.

Close-out

1. Develop an after action report that documents lessons learned and follow up actions for strengthening your breach response process and/or the system, program, or processes that were tested in the TTX.
    a. Also document lessons learned for your next tabletop exercise. You can include these in the same report or a separate document.
    b. Share the report with the BRT.
2. Review your Breach Response Plan for any needed changes based on the lessons learned from the TTX.
3. If appropriate, conduct an out brief for senior leadership. The briefing should identify any unresolved issues to allow leadership to determine if any unmitigated risks are within the organization's risk tolerance.

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, March 5, 2018 2:35 PM
To:	Mark Graff NOAA Federal
Subject:	Fwd: NOAA4600 PTA Review Coming Due 02/27/18
Attachments:	NOAA4600_PTA_02152018_AM MS (1).pdf

For your signature, thanks

Forwarded message
From: **Tahir Ismail - NOAA Affiliate** <tahir.ismail@noaa.gov>
Date: Mon, Mar 5, 2018 at 2:25 PM
Subject: Re: NOAA4600 PTA Review Coming Due 02/27/18
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
Cc: Shane Yamamoto NOAA Federal <shane.yamamoto@noaa.gov>, Alicia Matter <Alicia.Matter@noaa.gov>, "NMFS.InfoSec@noaa.gov" <NMFS.InfoSec@noaa.gov>

Sarah,

Attached, please find the NOAA4600 PTA for Mark's signature.

Thank you,

Tahir

On Wed, Feb 28, 2018 at 12:49 PM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

> Shane,
>
> Thank you, not a problem. I will get it processed.
>
> Tahir
>
> On Wed, Feb 28, 2018 at 11:30 AM, Shane Yamamoto NOAA Federal <shane.yamamoto@noaa.gov> wrote:
>
> > Hi Tahir,
> >
> > Sorry, I got it signed yesterday but I was not able to send it out. Please see the attached signed document. Thank you
> >
> > On Wed, Feb 28, 2018 at 8:23 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
> >
> > > Shane,
> > >
> > > Please complete this as soon as you can.
> > >
> > > Thank you,

Tahir

On Mon, Feb 26, 2018 at 11:29 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

Thank you Shane,

Tahir

On Mon, Feb 26, 2018 at 11:27 AM, Shane Yamamoto NOAA Federal <shane.yamamoto@noaa.gov> wrote:

Hi Tahir,

Thank you for the reminder. I will work with David on this tomorrow when I am in the office. Thanks

On Mon, Feb 26, 2018 at 6:16 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

Shane,

I wanted to follow up on NOAA4600 PTA. Please complete this as soon you can and send for Catherine's signature.

Thank you,

Tahir

On Thu, Feb 15, 2018 at 10:53 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Sorry, I do forget sometime, especially when I've just been emailing with you. Will try to be more careful. Best at this point to use the new template, since we will have to send to DOC either with an updated PIA, or with a certification that there are no new privacy risks, a re signed PIA and and the PTA.

On Thu, Feb 15, 2018 at 10:40 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

Sarah,

I just wanted to know if some communication was done without CC'in NMFS.InfoSec@noaa.gov. It was not, so I will take care of it. Thank you for verifying for us.

Tahir

On Thu, Feb 15, 2018 at 10:35 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Okay, then please use the template that Tahir just sent you says 1 2017 in upper right corner. thx

On Thu, Feb 15, 2018 at 10:30 AM, David Berklund NOAA Federal <david.e.berklund@noaa.gov> wrote:

During the Q1 SAR in December Mike indicated the PTA was being updated but Shane and I do not have any records of that document.

David

On Thu, Feb 15, 2018 at 7:26 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

I'm sorry, I didn't remember this had been in process for so long. If you still don't have signatures, please use the new template. Otherwise, finish up getting signatures on what I okay'd. Sorry for confusion.

On Thu, Feb 15, 2018 at 10:20 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

Sarah,
Can you please confirm as I do not see a record?

David in addition please make sure we have the updated template signed as there was a change in template as we were working on it. I have attached the updated PTA template.

Thank you,

Tahir

On Thu, Feb 15, 2018 at 10:17 AM, David Berklund NOAA Federal <david.e.berklund@noaa.gov> wrote:

As of 2/12 Sarah Brabson has informed us she is waiting for signatures.

Thanks

David

On Thu, Feb 15, 2018 at 7:01 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

Shane/David,

Please gather signatures on the NOAA4600 PTA. Let me know if you have any questions or concerns.

Thank you,

Tahir

On Tue, Jan 2, 2018 at 11:49 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

Mike,

Happy New Year :)

Just a kind reminder on this. Please start to get signatures on this.

Thanks,

Tahir

On Wed, Dec 6, 2017 at 2:02 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Yes, perfect. thanks. Please gather signatures and return to me for Mark's. sb
>
> On Wed, Dec 6, 2017 at 1:50 PM, Michael McCully NOAA Federal <mike.mccully@noaa.gov> wrote:
>
> > Hi Sarah, Attached is the NOAA4600 PTA for review.
> >
> > Thanks
> >
> > --
> > --
> > Michael J McCully CISSP | CEH
> > Acting WCR Information Services and Technology Branch Chief
> > Information System Security Officer
> > DOC/NOAA/NMFS
> > Northwest Fisheries Science Center
> > West Coast Region
> > 206-518-2347
> >
> > On Mon, Dec 4, 2017 at 8:17 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
> >
> > > Mike,
> > >
> > > In our records NOAA4600 PTA is coming due 02/27/2018. Attached, please find the template for PTA. Please follow the steps below;
> > >
> > > 1) Please fill the template out and reply with the WORD version of file to Sarah Brabson and NMFS.InfoSec@noaa.gov for review and comments;
> > >
> > > 2) Make updates based on comments provided by Sarah and Fisheries IT Security;
> > >
> > > 3) Get SO and AO signatures;
> > >
> > > 4) Email the file to NMFS.InfoSec@noaa.gov for Catherine Amores signature;
> > >
> > > We will then send it to Sarah for NOAA Privacy Officer's signature. Once signed I notify you and upload signed PTA in CSAM for you.
> > >
> > > Please let me know if you have any questions or concerns.
> > >
> > > Thanks,
> > >
> > > Tahir
> > >
> > > Tahir M. Ismail
> > > IT Security Specialist, CISSP, CISA, CRISC
> > > Office of Chief Information Officer
> > > NOAA-Fisheries
> > > Tel: 301 427 8839
> > > Cell (b)(6) [redacted]

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

David Berklund
NOAA Fisheries
U.S. Department of Commerce
Office: 206-302-2416
David.E.Berklund@noaa.gov
www.nmfs.noaa.gov

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

David Berklund
NOAA Fisheries
U.S. Department of Commerce
Office: 206-302-2416
David.E.Berklund@noaa.gov
www.nmfs.noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Shane Yamamoto CISSP
NWFSC Database Administrator / Security Engineer
DOC / NOAA / NWFSC
2725 Montlake Blvd E
Seattle, WA 98112
Phone: (206) 860 3493
Cel (b)(6)
Fax: (206) 325 6363

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Shane Yamamoto CISSP
NWFSC Database Administrator / Security Engineer
DOC / NOAA / NWFSC
2725 Montlake Blvd E
Seattle, WA 98112
Phone: (206) 860 3493
Cel (b)(6)
Fax: (206) 325 6363

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer

NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, March 5, 2018 2:38 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA4600 PTA Review Coming Due 02/27/18
Attachments:	NOAA4600_PTA_02152018_AM MS (1) mhg.pdf

Looks good no issues.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Mon, Mar 5, 2018 at 2:35 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> For your signature, thanks
>
> Forwarded message
> From: **Tahir Ismail - NOAA Affiliate** <tahir.ismail@noaa.gov>
> Date: Mon, Mar 5, 2018 at 2:25 PM
> Subject: Re: NOAA4600 PTA Review Coming Due 02/27/18
> To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
> Cc: Shane Yamamoto NOAA Federal <shane.yamamoto@noaa.gov>, Alicia Matter <Alicia.Matter@noaa.gov>, "NMFS.InfoSec@noaa.gov" <NMFS.InfoSec@noaa.gov>
>
> Sarah,
>
> Attached, please find the NOAA4600 PTA for Mark's signature.
>
> Thank you,
>
> Tahir
>
> On Wed, Feb 28, 2018 at 12:49 PM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
>
> > Shane,
> >
> > Thank you, not a problem. I will get it processed.
> >
> > Tahir

On Wed, Feb 28, 2018 at 11:30 AM, Shane Yamamoto NOAA Federal <shane.yamamoto@noaa.gov> wrote:

> Hi Tahir,
>
> Sorry, I got it signed yesterday but I was not able to send it out. Please see the attached signed document. Thank you
>
> On Wed, Feb 28, 2018 at 8:23 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
>
> > Shane,
> >
> > Please complete this as soon as you can.
> >
> > Thank you,
> > Tahir
> >
> > On Mon, Feb 26, 2018 at 11:29 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
> >
> > > Thank you Shane,
> > >
> > > Tahir
> > >
> > > On Mon, Feb 26, 2018 at 11:27 AM, Shane Yamamoto NOAA Federal <shane.yamamoto@noaa.gov> wrote:
> > >
> > > > Hi Tahir,
> > > >
> > > > Thank you for the reminder. I will work with David on this tomorrow when I am in the office. Thanks
> > > >
> > > > On Mon, Feb 26, 2018 at 6:16 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
> > > >
> > > > > Shane,
> > > > >
> > > > > I wanted to follow up on NOAA4600 PTA. Please complete this as soon you can and send for Catherine's signature.
> > > > >
> > > > > Thank you,
> > > > >
> > > > > Tahir
> > > > >
> > > > > On Thu, Feb 15, 2018 at 10:53 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> > > > >
> > > > > > Sorry, I do forget sometime, especially when I've just been emailing with you. Will try to be more careful. Best at this point to use the new template, since we will have to send to DOC either with an updated PIA, or with a certification that there are no new privacy risks, a re signed PIA and and the PTA.
> > > > > >
> > > > > > On Thu, Feb 15, 2018 at 10:40 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
> > > > > >
> > > > > > > Sarah,
> > > > > > >
> > > > > > > I just wanted to know if some communication was done without CC'in NMFS.InfoSec@noaa.gov. It was not, so I will take care of it. Thank you for verifying for us.

Tahir

On Thu, Feb 15, 2018 at 10:35 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Okay, then please use the template that Tahir just sent you says 1 2017 in upper right corner. thx
>
> On Thu, Feb 15, 2018 at 10:30 AM, David Berklund NOAA Federal <david.e.berklund@noaa.gov> wrote:
>
> > During the Q1 SAR in December Mike indicated the PTA was being updated but Shane and I do not have any records of that document.
> >
> > David
> >
> > On Thu, Feb 15, 2018 at 7:26 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> >
> > > I'm sorry, I didn't remember this had been in process for so long. If you still don't have signatures, please use the new template. Otherwise, finish up getting signatures on what I okay'd. Sorry for confusion.
> > >
> > > On Thu, Feb 15, 2018 at 10:20 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
> > >
> > > > Sarah,
> > > > Can you please confirm as I do not see a record?
> > > >
> > > > David in addition please make sure we have the updated template signed as there was a change in template as we were working on it. I have attached the updated PTA template.
> > > >
> > > > Thank you,
> > > >
> > > > Tahir
> > > >
> > > > On Thu, Feb 15, 2018 at 10:17 AM, David Berklund NOAA Federal <david.e.berklund@noaa.gov> wrote:
> > > >
> > > > > As of 2/12 Sarah Brabson has informed us she is waiting for signatures.
> > > > >
> > > > > Thanks
> > > > >
> > > > > David
> > > > >
> > > > > On Thu, Feb 15, 2018 at 7:01 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
> > > > >
> > > > > > Shane/David,
> > > > > >
> > > > > > Please gather signatures on the NOAA4600 PTA. Let me know if you have any questions or concerns.

Thank you,

Tahir

On Tue, Jan 2, 2018 at 11:49 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

> Mike,
>
> Happy New Year :)
>
> Just a kind reminder on this. Please start to get signatures on this.
>
> Thanks,
>
> Tahir
>
> On Wed, Dec 6, 2017 at 2:02 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Yes, perfect. thanks. Please gather signatures and return to me for Mark's. sb
> >
> > On Wed, Dec 6, 2017 at 1:50 PM, Michael McCully NOAA Federal <mike.mccully@noaa.gov> wrote:
> >
> > > Hi Sarah, Attached is the NOAA4600 PTA for review.
> > >
> > > Thanks
> > >
> > > --
> > > --
> > > Michael J McCully CISSP | CEH
> > > Acting WCR Information Services and Technology Branch Chief
> > > Information System Security Officer
> > > DOC/NOAA/NMFS
> > > Northwest Fisheries Science Center
> > > West Coast Region
> > > 206-518-2347
> > >
> > > On Mon, Dec 4, 2017 at 8:17 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:
> > >
> > > > Mike,
> > > >
> > > > In our records NOAA4600 PTA is coming due 02/27/2018. Attached, please find the template for PTA. Please follow the steps below;
> > > >
> > > > 1) Please fill the template out and reply with the WORD version of file to Sarah Brabson and NMFS.InfoSec@noaa.gov for review and comments;
> > > >
> > > > 2) Make updates based on comments provided by Sarah and Fisheries IT Security;
> > > >
> > > > 3) Get SO and AO signatures;
> > > >
> > > > 4) Email the file to NMFS.InfoSec@noaa.gov for Catherine Amores signature;

We will then send it to Sarah for NOAA Privacy Officer's signature. Once signed I notify you and upload signed PTA in CSAM for you.

Please let me know if you have any questions or concerns.

Thanks,

Tahir

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

David Berklund
NOAA Fisheries
U.S. Department of Commerce
Office: 206-302-2416
David.E.Berklund@noaa.gov
www.nmfs.noaa.gov

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

David Berklund
NOAA Fisheries
U.S. Department of Commerce
Office: 206-302-2416
David.E.Berklund@noaa.gov
www.nmfs.noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Shane Yamamoto CISSP
NWFSC Database Administrator / Security Engineer
DOC / NOAA / NWFSC
2725 Montlake Blvd E
Seattle, WA 98112
Phone: (206) 860 3493
Cel (b)(6)
Fax: (206) 325 6363

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Shane Yamamoto CISSP
NWFSC Database Administrator / Security Engineer
DOC / NOAA / NWFSC
2725 Montlake Blvd E
Seattle, WA 98112
Phone: (206) 860 3493
Cel (b)(6)
Fax: (206) 325 6363

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Tahir M. Ismail
IT Security Specialist, CISSP, CISA, CRISC
Office of Chief Information Officer
NOAA-Fisheries
Tel: 301 427 8839
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Northwest Fisheries Science Center
NOAA4600

U.S. Department of Commerce Privacy Threshold Analysis

NOAA4600

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
NOAA4600 supports the mission of the Northwest Fisheries Science Center (NWFSC). "Scientists at the NWFSC conduct leading-edge research and analyses that provide the foundation for management decisions to protect, recover, restore, and sustain ecosystems and living marine resources in the Pacific Northwest." NWFSC researchers are dedicated to producing scientific products that will strengthen decision-making at all levels, enhance socio-economic benefits, support sustainable resource use, and conserve biological diversity.

The NWFSC supports 4 major science and research themes:
1. Ecosystem Approach to Management for the California Current Large Marine Ecosystem
2. Habitats to Support Sustainable Fisheries and Recovered Populations
3. Recovery, Rebuilding and Sustainability of Marine and Anadromous Species
4. Oceans and Human Health Key Roles:

- Provide current, relevant information to support science-based stewardship of natural resources. The primary mission of the NWFSC is to provide multi-disciplinary scientific and technical information to the West Coast Regional Office of NOAA Fisheries, other NOAA line offices, co-managers, stakeholders and other constituents to inform decision and policy-making processes.
- Foster scientific literacy and expertise. In order to achieve the national missions of NOAA, the NWFSC must ensure that Center research results reach the broader science, education, and public communities within the region and beyond. The Center has the additional responsibility to help train the next generation of fisheries scientists.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

__X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__**X**__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__**X**__ Companies
____ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__**X**__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
_**X**__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__**X**__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_**X** ___ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X___ I certify the criteria implied by one or more of the questions above **apply** to the NOAA4600 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Alicia Matter, NOAA4600 System Owner

Signature of ISSO or SO: MATTER.ALICIA.L.1365880014 Digitally signed by MATTER.ALICIA.L.1365880014 Date: 2018.02.27 11:34:54 -08'00' Date: 02/27/2018

Name of Information Technology Security Officer (ITSO): Catherine Amores

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2018.03.05 13:49:58 -05'00' Date: 3/5/2018

Name of Authorizing Official (AO): Mark Strom, Authorizing Official

Signature of AO: STROM.MARK.STEPHEN.DR.1365882890 Digitally signed by STROM.MARK.STEPHEN.DR.1365882890 Date: 2018.02.27 12:55:01 -08'00' Date: 02/27/2018

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.05 14:37:00 -05'00' Date: 3.5.18

Sarah Brabson NOAA Federal

From: Sarah Brabson NOAA Federal
Sent: Monday, March 5, 2018 2:54 PM
To: Lorna Martin Gross NOAA Federal
Cc: Mark Graff NOAA Federal; Logan Gregory NOAA Federal
Subject: Re: OLD BI Weekly
Attachments: NOAA 5 SORN in new template v2 docx

(b)(5)

On Mon, Mar 5, 2018 at 2:49 PM, Lorna Martin Gross NOAA Federal <lorna.martin.gross@noaa.gov> wrote:
Hi Mark,

(b)(5)

Lorna

On Mon, Mar 5, 2018 at 2:35 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
Hi Lorna,

(b)(5)

Mark H Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Confidentiality Notice Th s e ma l message s ntended only for the named recipients It conta ns nfo mation that may be confidential p ivileged atto ney work product or o he wise exempt from d sclosure under applicable law If you have rece ved his message in er or are not a named recipient or a e not the employee or agent respons ble for del vering this message to a named rec p ent be adv sed that any review d sclosure use dissem nation distr but on or reproduction of th s message or its contents s st ctly proh b ted Please not fy us immediately that you have rece ved his message in er or and delete the message

On Mon, Mar 5, 2018 at 2:26 PM, Lorna Martin Gross NOAA Federal <lorna.martin.gross@noaa.gov> wrote:
Mark and Sarah,

(b)(5)

Kind regards,

Lorna

Forwarded message
From: **Andre Sivels NOAA Federal** <andre.sivels@noaa.gov>
Date: Mon, Mar 5, 2018 at 2:12 PM
Subject: Re: OLD BI Weekly
To: Lorna Martin Gross NOAA Federal <lorna.martin.gross@noaa.gov>

Lorna

(b)(5)

Lorna
Forwarded message
From: **Logan Gregory** <logan.gregory@noaa.gov>
Date: Mon, Mar 5, 2018 at 12:22 PM
Subject: Re: OLD BI Weekly
To: Lorna Martin Gross NOAA Federal <lorna.martin.gross@noaa.gov>

(b)(5)

Logan Gregory
Deputy Director, Office of Law Enforcement
U S Department of Commerce
National Oceanic and Atmospheric Administration
1315 East West Highway, SSMC3, Suite 3301
Silver Spring, MD 20910
301.427.8266
www.fisheries.noaa.gov/ole

On Mon, Mar 5, 2018 at 11:56 AM, Lorna Martin Gross NOAA Federal <lorna.martin.gross@noaa.gov> wrote:
Logan,

See Andre's question

Forwarded message
From: **Andre Sivels NOAA Federal** <andre.sivels@noaa.gov>
Date: Mon, Mar 5, 2018 at 11:55 AM
Subject: Re: OLD BI Weekly
To: Lorna Martin Gross NOAA Federal <lorna.martin.gross@noaa.gov>

Lorna

(b)(5)

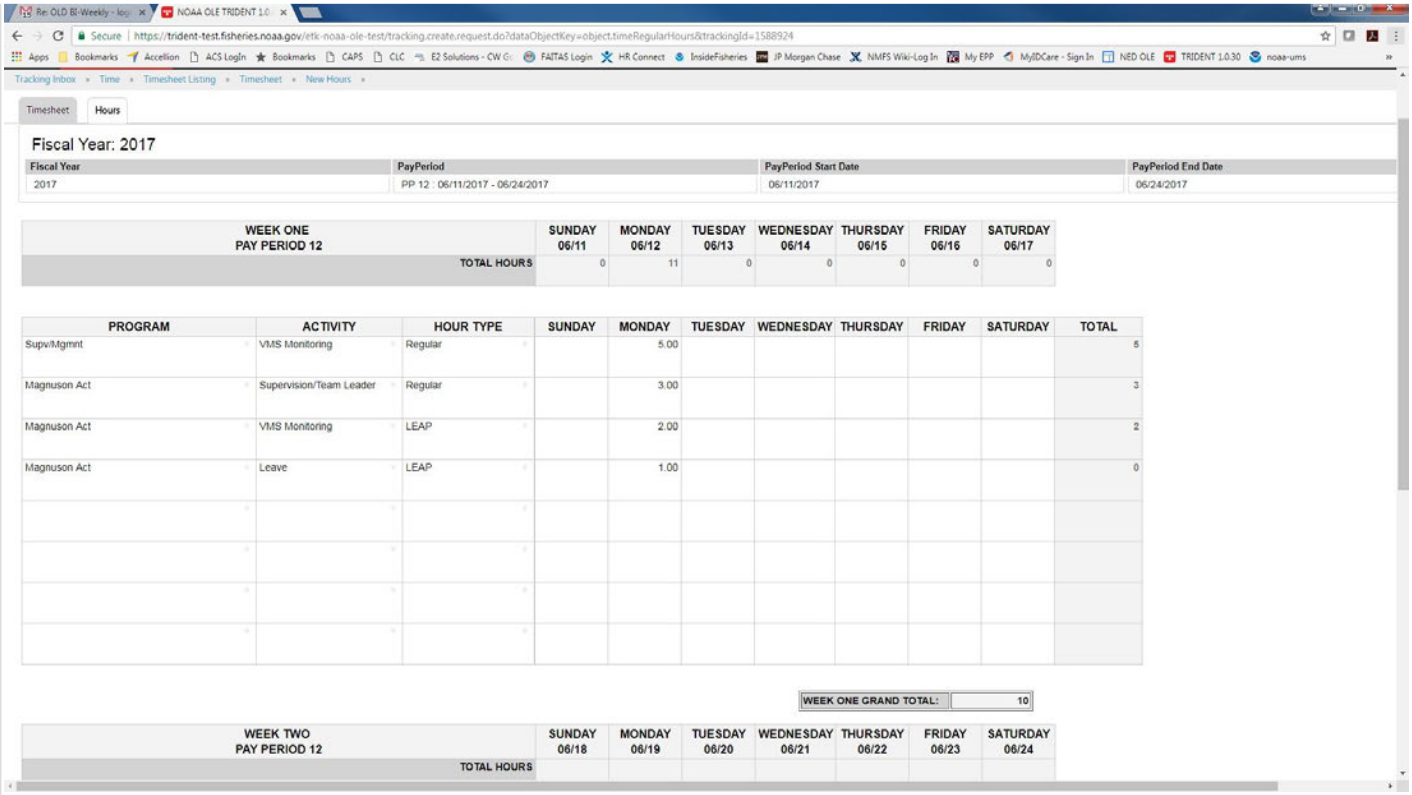
On Mon, Mar 5, 2018 at 9:52 AM, Lorna Martin Gross NOAA Federal <lorna.martin.gross@noaa.gov> wrote:
Hi Chaz and Andre,

(b)(5)

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instructions
203-01	Time and Attendance Records.	Sign-in/sign-out records, time cards, leave applications and approvals of all types (annual, sick, family medical, military service, jury duty, leave donations, etc.); overtime, compensatory, and credit time requests and approvals, premium pay authorizations, and other records documenting employees' presence at or absence from work. **Legal citation:** 29 U.S.C. 516.5a ***Note:*** *Every office involved in documenting employees' time worked is responsible for retaining the records it receives and creates for 3 years.* *Timekeepers in individual offices need to be able to document that the time and attendance information they sent to the payroll system provider was accurate. Only total hours of time worked and leave taken is forwarded to the payroll system provider.*	DAA-GRS- 2016-0015- 0003 **(GRS 2.4, item 030)** **Supersedes** *NOAA Schedule item* 203-01 *(GRS 2, item 8)* **Previously**, *NOAA Schedule item* 205-31.	**TEMPORARY.** Destroy after GAO audit or when 3 years old, whichever is sooner.
203-02	Time and Attendance Source Records	All time and attendance records upon which leave input data is based.	DAA-GRS- 2016-0015- 0003 **(GRS 2.4, item 030)** **Supersedes** *NOAA Schedule item* 203-01 *(GRS 2, item 7)* **Previously** , *NOAA Schedule item* 200-32.	**TEMPORARY.** Follow disposition instructions for 203-01 above.

Kind regards,
Lorna

On Tue, Feb 27, 2018 at 5:27 PM, Logan Gregory <logan.gregory@noaa.gov> wrote:
Picture faster than words



Re: OLD BI-Weekly - log... | NOAA OLE TRIDENT 1.0...

https://trident-test.fisheries.noaa.gov/etk-noaa-ole-test/tracking.create.request.do?dataObjectKey=object.timeRegularHours&trackingId=1588924

Tracking Inbox » Time » Timesheet Listing » Timesheet » New Hours »

Timesheet | Hours

Fiscal Year: 2017

Fiscal Year	PayPeriod	PayPeriod Start Date	PayPeriod End Date
2017	PP 12 : 06/11/2017 - 06/24/2017	06/11/2017	06/24/2017

WEEK ONE PAY PERIOD 12	SUNDAY 06/11	MONDAY 06/12	TUESDAY 06/13	WEDNESDAY 06/14	THURSDAY 06/15	FRIDAY 06/16	SATURDAY 06/17
TOTAL HOURS	0	11	0	0	0	0	0

PROGRAM	ACTIVITY	HOUR TYPE	SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	TOTAL
Supv/Mgmnt	VMS Monitoring	Regular		5.00						5
Magnuson Act	Supervision/Team Leader	Regular		3.00						3
Magnuson Act	VMS Monitoring	LEAP		2.00						2
Magnuson Act	Leave	LEAP		1.00						0

WEEK ONE GRAND TOTAL: 10

WEEK TWO PAY PERIOD 12	SUNDAY 06/18	MONDAY 06/19	TUESDAY 06/20	WEDNESDAY 06/21	THURSDAY 06/22	FRIDAY 06/23	SATURDAY 06/24
TOTAL HOURS							

Logan Gregory
Deputy Director, O ffice of Law Enforcement
U S Department of Commerce
Nat onal Ocean c and Atmospher c Adm nistrat on
1315 East West H gh...ay, SSMC3, Su te 3301
Silver Spring, MD 20910
301 427 8266
www f sher es noaa gov/o e

On Tue, Feb 27, 2018 at 1:57 PM, Lorna Martin Gross NOAA Federal <lorna martin gross@noaa gov> wrote:

Thanks Logan,

(b)(5)

Thanks,

Lorna

On Tue, Feb 27, 2018 at 12:52 PM, Logan Gregory <logan gregory@noaa gov> wrote:

Answers below Hope this helps

Logan Gregory
Deputy D rector, Office of Law Enforcement
U S Depar ment of Commerce
National Oceanic and Atmospheric Admn strat on
1315 East West H ghway, SSMC3, Suite 3301
S lver Spr ng, MD 20910
301 427 8266
www f sheries noaa gov/o e

On Tue, Feb 27, 2018 at 10:01 AM, Lorna Martin Gross NOAA Federal <lorna martin gross@noaa gov> wrote:

Logan and Will,

(b)(5)

This will give me a better idea of what steps we need to take (if any)

Thanks,

Lorna

On Mon, Feb 26, 2018 at 5:12 PM, Logan Gregory <logan gregory@noaa gov> wrote:

(b)(5)

Logan Gregory
Deputy Director, Office of Law Enforcement
U S Department of Commerce
Nat onal Ocean c and Atmospher c Administrat on
1315 East West Highway, SSMC3, Su te 3301
Silver Spring, MD 20910
301 427 8266
www f sher es noaa gov/o e

On Mon, Feb 26, 2018 at 12:47 PM, Lorna Martin Gross NOAA Federal <lorna martin gross@noaa gov> wrote:

All,

See the attached from the NOAA Records Schedule excerpt

Let me know if you need further information

Lorna

On Mon, Feb 26, 2018 at 12:29 PM, Robyn Holloway NOAA Federal <robyn holloway@noaa gov> wrote:

Will

I've included Lorna Martin Gross as a cc to this email because she is our Records Manager She can answer any question you have regarding retention of our old DB

r

Robyn Holloway, PMP

NOAA F sheries Off ce of Law Enforcement

Direct: 301 427.8252 / Fax: 301 427.2313

><(((°> ><(((°> >< (((°> ><((((°> ><(((°> ><(((°> ><(((° °> ><(((°>

From: William Swann NOAA Affiliate [mailto:w lliam swann@noaa gov]
Sent: Monday, February 26, 2018 12:12 PM
To: Robyn Holloway NOAA Federal <robyn holloway@noaa gov>
Cc: Samir Mehta NOAA Federal <samir mehta@noaa gov>; Sean Stanley NOAA Federal <sean stanley@noaa gov>
Subject: OLD BI Weekly

Sean / Robyn:

(b)(5)

Thanks,

Will

Ms Lorna Martin Gross
Records Manager
O fice of Law Enforcement
NOAA Fisheries
U S Department of Commerce
O fice 301 27 8244
lorna martin gross@noaa gov

Ms Lorna Martin Gross
Records Manager
Office of Law Enforcement
NOAA Fisheries
U S Department of Commerce
Office 301 427 8244
lorna mar in gross@noaa gov

Ms Lorna Martin Gross
Records Manager
Of ice of Law Enforcement
NOAA Fisheries
U S Department of Commerce
Office 301 427 8244
lorna martin gross@noaa gov

Ms Lorna Martin Gross
Records Manager
Office of Law Enforcement
NOAA Fisheries
U S Department of Commerce
Office 301 427 8244
lorna martin gross@noaa gov

Andre Sivels
NOAA Records Officer
U S Department of Commerce
1305 East West Highway Rm 7439
Silver Spring MD 20910
Phone: 301628 0946
Fax: 301 713 1169

Ms Lorna Martin Gross
Records Manager
Office of Law Enforcement
NOAA Fisheries
U S Department of Commerce
Office 301 427 8244
l si @

Ms Lorna Martin Gross
Records Manager
Of ice of Law Enforcement
NOAA Fisheries
U S Department of Commerce
Office 301 427 8244
lorna martin gross@noaa gov

Andre Sivels
NOAA Records Officer
U S Department of Commerce
1305 East West Highway Rm 7439
Silver Spring MD 20910
Phone: 301628 0946
Fax: 301 713 1169

Ms Lorna Martin Gross
Records Manager
O fice of Law Enforcement
NOAA Fisheries
U S Department of Commerce
O fice 301 427 8244
lorna martin gross@noaa gov

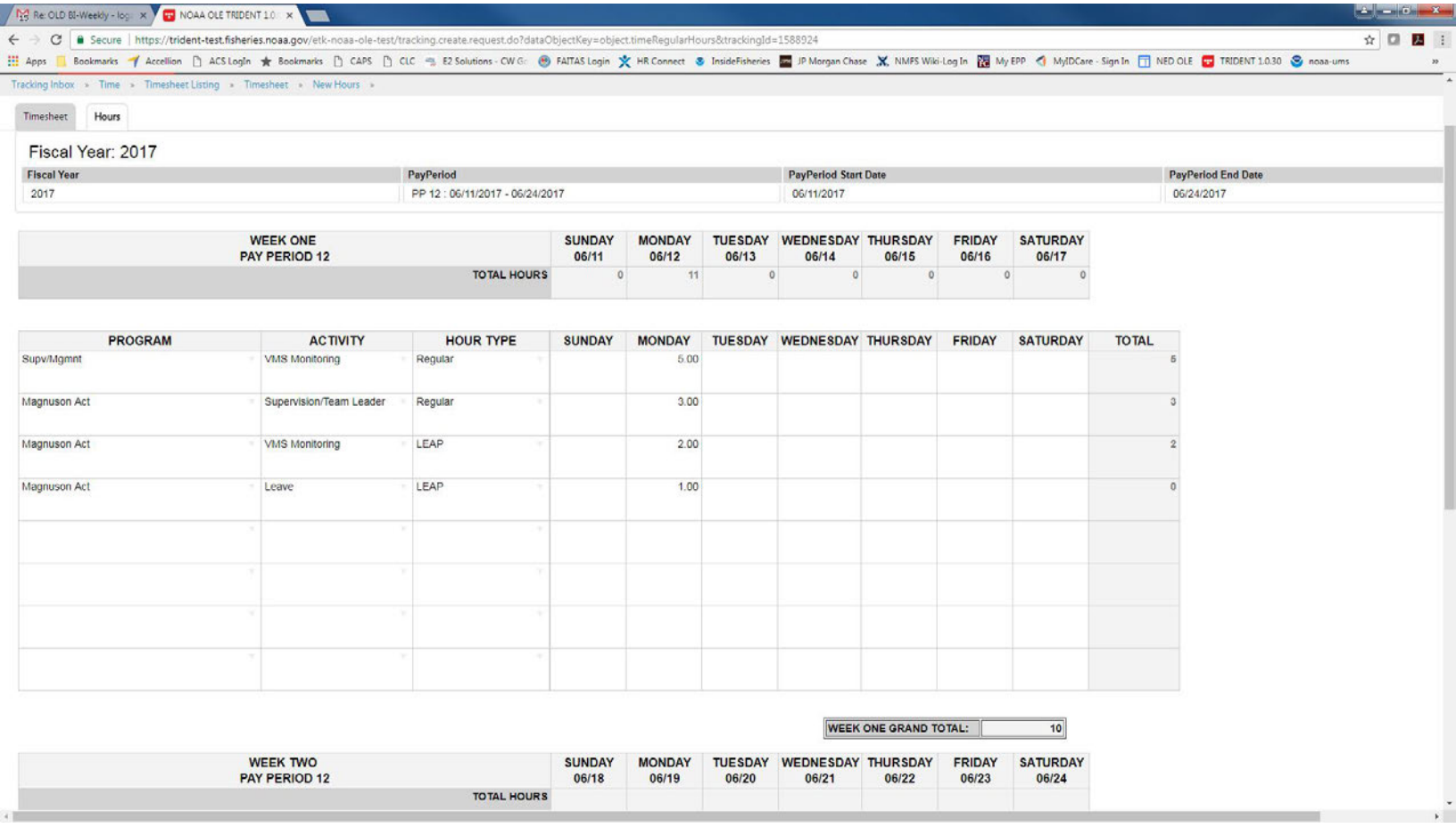
Ms Lorna Martin Gross

Records Manager
Office of Law Enforcement
NOAA Fisheries
U S Department of Commerce
Office 301 427 8244
lorna.merlin.gross@noaa.gov

Sarah D Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Series #	Records Series Title	Records Description	Disposition Authority	Disposition Instructions
203-01	**Time and Attendance Records.**	Sign-in/sign-out records, time cards, leave applications and approvals of all types (annual, sick, family medical, military service, jury duty, leave donations, etc.); overtime, compensatory, and credit time requests and approvals; premium pay authorizations; and other records documenting employees' presence at or absence from work. **Legal citation:** 29 U.S.C. 516.5a ***Note:*** *Every office involved in documenting employees' time worked is responsible for retaining the records it receives and creates for 3 years.* *Timekeepers in individual offices need to be able to document that the time and attendance information they sent to the payroll system provider was accurate. Only total hours of time worked and leave taken is forwarded to the payroll system provider.*	DAA-GRS- 2016-0015- 0003 **(GRS 2.4, item 030)** ***Supersedes*** *NOAA Schedule Item* ***203-01*** *(GRS 2, item 8)* ***Previously,*** *NOAA Schedule Item* ***205-31*** *.*	**TEMPORARY.** Destroy after GAO audit or when 3 years old, whichever is sooner.
203-02	**Time and Attendance Source Records**	All time and attendance records upon which leave input data is based.	DAA-GRS- 2016-0015- 0003 **(GRS 2.4, item 030)** ***Supersedes*** *NOAA Schedule Item* ***203-01*** *(GRS 2, item 7)* ***Previously*** *, NOAA Schedule Item* ***200-32.***	**TEMPORARY.** Follow disposition instructions for 203-01 above.



Fiscal Year: 2017

Fiscal Year	PayPeriod	PayPeriod Start Date	PayPeriod End Date
2017	PP 12 : 06/11/2017 - 06/24/2017	06/11/2017	06/24/2017

WEEK ONE PAY PERIOD 12	SUNDAY 06/11	MONDAY 06/12	TUESDAY 06/13	WEDNESDAY 06/14	THURSDAY 06/15	FRIDAY 06/16	SATURDAY 06/17
TOTAL HOURS	0	11	0	0	0	0	0

PROGRAM	ACTIVITY	HOUR TYPE	SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	TOTAL
Supv/Mgmnt	VMS Monitoring	Regular		5.00						5
Magnuson Act	Supervision/Team Leader	Regular		3.00						3
Magnuson Act	VMS Monitoring	LEAP		2.00						2
Magnuson Act	Leave	LEAP		1.00						0

WEEK ONE GRAND TOTAL:	10

WEEK TWO PAY PERIOD 12	SUNDAY 06/18	MONDAY 06/19	TUESDAY 06/20	WEDNESDAY 06/21	THURSDAY 06/22	FRIDAY 06/23	SATURDAY 06/24
TOTAL HOURS							

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

James Cooperman - NOAA Affiliate

From:	James Cooperman NOAA Affiliate
Sent:	Tuesday, March 6, 2018 8:20 AM
To:	Sarah Brabson NOAA Federal; John D. Parker NOAA Federal; Jonathan Gordon NOAA Federal; Mark Graff NOAA Federal
Subject:	PTA
Attachments:	NOAA6602 PTA_V2 03 06 2018.docx

Sarah

Attached is the most recent PTA.

Thank You

Jim

James Cooperman CTR
Information System Security Office
Office of National Marine Sanctuaries
Desk 240-533-0680
Cell (b)(6) [redacted]

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Andre Sivels - NOAA Federal

From:	Andre Sivels NOAA Federal
Sent:	Wednesday, March 7, 2018 10:15 AM
To:	Mark Graff NOAA Federal
Subject:	2017 Records Management Assessment
Attachments:	2017 RMSA Questionnaire.docx

Hi Mark

I am in the process of review the questions for the NARA annual records management assessment and noticed they have 6 questions related to FOIA. Can you provide answers to questions 33 to 38 on the attached questionnaire and return to Monday March 12th, Thanks

Andre

Andre Sivels
NOAA Records Officer
U.S. Department of Commerce
1305 East West Highway Rm 7439
Silver Spring, MD 20910
Phone: 301628 0946
Fax: 301 713 1169

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)
2017 RECORDS MANAGEMENT SELF-ASSESSMENT

Welcome to the 2017 Records Management Self-Assessment!

Before you begin, please note the following information.

Except where indicated, the questions in this survey are intended to cover all records regardless of format, as defined in 44 U.S.C. 3301.

The questions apply regardless of whether your agency's work processes are conducted manually or electronically.

Unless otherwise indicated, the following questions refer to FY 2017 (October 1, 2016, through September 30, 2017).

Your answers to the self-assessment questions must be specific to records management activities in your agency. We have added a "not applicable" answer option to some questions. In general, use this option only if a question references an activity or action that is not conducted in your agency because of its size or if you are a Departmental Records Officer and are not responsible for the activity or action. In some cases, if the activity is being done by a departmental records management program, component agencies of that department may answer "Yes."

NOTE: Please note that your responses to questions in this assessment may be subject to public release pursuant to FOIA. However, we will not release responses to questions that contain detailed descriptions of agency activities.

NARA reserves the right to follow up with agencies to obtain additional information and/or documentation that supports their answers to the questions in this self-assessment.

As in previous years we will be conducting a validation process. Your agency may be selected at random to provide additional documentation and/or take part in interviews to discuss your records management program activities.

If you have any questions about this self-assessment or need additional information to answer a question(s), please send an email message to rmselfassessment@nara.gov.

Section I: Records Management Program - Activities

The next series of questions relate to administration of the records management program.

1. Is there a person in your agency who is responsible for coordinating and overseeing the implementation of the records management program? (36 CFR 1220.34(a))

☐ Yes
☐ No
☐ Do not know

2. If Yes: Please provide the person's name, position title, and office.

3. If Yes: How long has this person been responsible for coordinating and overseeing the implementation of the records management program?

☐ 5 or more years
☐ 3 to 4 years
☐ 1 to 2 years
☐ Less than a year

4. Does your agency have a Senior Agency Official for Records Management (SAORM)? (If you are a component of a department, you may answer "Yes," even if this is not being done at the component level.)

☐ Yes
☐ No
☐ Do not know

5. If Yes: Does your Agency Records Officer meet regularly (four or more times a year) with the SAORM to discuss the agency records management program's goals?

☐ Yes
☐ No
☐ Do not know

6. Does your agency use the Records and Information Management Series, 0308, (job series) released by the Office of Personnel Management in 2015?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, my agency does not use the General Schedule (GS) job classification

7. Does your agency have a network of designated employees within each program and administrative area who are assigned records management responsibilities? These individuals are often called Records Liaison Officers (RLOs), though their titles may vary. (36 CFR 1220.34(d))

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency has less than 100 employees
☐ Not applicable, Departmental Records Officer - this is done at the component level

8. Of the following, please select the one that best describes your records management staff. This includes only those specifically assigned to the records management program.

☐ All records management staff are agency personnel
☐ All records management staff are contractors
☐ Records management staff includes both agency personnel and contractors

In general, an FTE is equivalent to one full-time employee who is assigned full-time to records management (2,080 hours per year). An employee who works part-time or is assigned records management as one of several unrelated responsibilities should be counted as a fraction of an FTE, representing the estimated number of hours worked on records management per year as a percentage of 2,080 hours.

9. How many FTE agency personnel (non-contractors) are specifically assigned records management responsibilities? (These are individuals directly responsible for records management program implementation, not contacts within mission areas with minimal records management duties.)*

*For Department Records Officers, please include only the staff at the Department level, not agency components, as component agency records officers will be answering for their agencies.

☐ <1
☐ 1
☐ 2 - 10
☐ 10 - 20
☐ More than 20
☐ Do not know
☐ Not available
☐ Not applicable, all records management staff are contractors

10. If your agency uses contractors, how many contractor FTE are specifically assigned records management responsibilities? (These are individuals directly responsible for records management program implementation, not general contacts within mission areas with minimal records management duties.)*

*For Department Records Officers, please include only the staff at the Department level, not agency components, as component agency records officers will be answering for their agencies.

☐ <1
☐ 1
☐ 2 - 10
☐ 10 - 20
☐ More than 20
☐ Do not know
☐ Not available
☐ Not applicable, all records management staff are agency personnel

The next series of questions relate to records management directives.

11. Does your agency have a documented and approved records management directive(s)? (36 CFR 1220.34(c))

☐ Yes
☐ No, pending final approval
☐ No, under development
☐ No
☐ Do not know

12. When was your agency's directive(s) last reviewed and/or revised to ensure it includes all new records management policy issuances and guidance?

☐ FY 2017 - present
☐ FY 2015 - 2016
☐ FY 2013 - 2014
☐ FY 2012 or earlier
☐ Do not know
☐ Not applicable, agency does not have a records management directive

The next series of questions relate to records management training.

Formal records management training is the communication of standardized information that improves the records management knowledge, skills, and/or awareness of agency employees. Training can be either in a classroom setting or distance-based (e.g., web-based training), but it *must:*

- **be regular (occurring more than just once);**
- **be repeatable and formal (all instructors must provide the same message, not in an ad hoc way); and**

- **communicate the agency's vision of records management.**

13. Does your agency have internal records management training*, based on agency policies and directives, for employees assigned records management responsibilities? (36 CFR 1220.34(f))

*Includes NARA's records management training workshops that were ***customized*** specifically for your agency or use of an ***agency-customized*** version of the Federal Records Officer Network (FRON) RM 101 course.

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know
☐ Not applicable, please explain

14. Has your agency developed mandatory internal, staff-wide, formal training*, based on agency policy and directives, covering records in all formats, including electronic communications such as email, text messages, chat, or other messaging platforms or apps, such as social media or mobile device applications, which helps agency employees and contractors fulfill their recordkeeping responsibilities?** (36 CFR 1220.34(f))

*Includes NARA's records management training workshops that were ***customized*** specifically for your agency or use of an ***agency-customized*** version of the Federal Records Officer Network (FRON) RM 101 course.

**Components of departmental agencies may answer "Yes" if this is handled by the department. Department Records Officers may answer "Yes" if this is handled at the component level.

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

Senior officials are the heads of departments and independent agencies; their deputies and assistants; the heads of program offices and staff offices including assistant secretaries, administrators, and commissioners; directors of offices, bureaus, or equivalent; principal regional officials; staff assistants to those aforementioned officials, such as special assistants, confidential assistants, and administrative assistants; and career Federal employees, political appointees, and officers of the Armed Forces serving in equivalent or comparable positions. (General Records Schedule (GRS) 6.1, item 010)

15. Does your agency require that all senior and appointed officials, including those incoming and newly promoted, receive training on the importance of appropriately managing records under their immediate control? (36 CFR 1220.34(f))

☐ Yes
☐ No
☐ Do not know

16. Is records management training included in the in-processing for new employees in your agency?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

17. Please add any additional comments about your agency for Section I: Activities. (Optional)

Section II: Records Management Program – Oversight and Compliance

Agency records management programs must provide for effective controls over the creation, maintenance, and use of records in the conduct of current business. (36 CFR 1220.30(c)(1))

Internal controls are integral components of an organization's management that provide reasonable assurance of the effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. ("Standards for Internal Control in the Federal Government" (GAO-14-704G), U.S. Government Accountability Office, September 2014.)

Internal controls are:

- **Geared to the achievement of objectives in one or more categories—operations, reporting, and compliance;**
- **Processes consisting of ongoing tasks and activities—a means to an end, not an end in itself;**
- **Carried out by people—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to effect internal control;**
- **Able to provide reasonable assurance, but not absolute assurance, to an entity's senior management;**
- **Adaptable to the organization's entire structure—flexible in application for the entire entity or for a particular regional office, division, operating unit, or business process.**

Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews/audits of operating performance, security of assets (limited access to inventories or equipment), and segregation of duties (separate personnel with authority to authorize a transaction, process the transaction, and review the transaction). Monitoring the effectiveness of internal controls should occur in the normal course of business. Periodic assessments should be integrated as part of management's continuous monitoring of internal control, which should be ingrained in the agency's operations. ("2013 Internal Control - Integrated Framework," Committee of Sponsoring Organizations (COSO) Executive Summary, May 14, 2013; and OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016.)

18. In addition to your agency's established records management policies and records schedules, has your agency's records management program developed and implemented internal controls to ensure that all eligible, permanent agency records in all media are transferred to NARA according to approved records schedules? (36 CFR 1222.26(e))

> **These controls must be internal to your agency. Reliance on information from external agencies (e.g., NARA's Federal Records Centers) or other organizations should not be considered when responding to this question.

*Examples of records management internal controls include but are not limited to:

- Regular briefings and other meetings with records creators
- Monitoring and testing of file plans
- Regular review of records inventories
- Internal tracking database of permanent record authorities and dates

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

19. In addition to your agency's established policies and records schedules, has your agency developed and implemented internal controls to ensure that Federal records are not destroyed before the end of their retention period? (36 CFR 1222.26(e))

> **These controls must be internal to your agency. Reliance on information from external agencies (e.g., NARA's Federal Records Centers) or other organizations should not be considered when responding to this question.

*Examples of records management internal controls include but are not limited to:

- Regular review of records inventories
- Approval process for disposal notices from off-site storage

- Require certificates of destruction
- Monitoring shredding services
- Performance testing for email
- Monitoring and testing of file plans
- Pre-authorization from records management program before records are destroyed
- Ad hoc monitoring of trash and recycle bins
- Notification from facilities staff when large trash bins or removal of boxes are requested
- Annual records clean-out activities sponsored and monitored by records management staff

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

An evaluation is an inspection, audit, or review of one or more records management programs for effectiveness and for compliance with applicable laws and regulations. An evaluation contains recommendations for correcting or improving records management practices, policies, and procedures as well as follow-up activities, including reporting on and implementing recommendations. Evaluations may be comprehensive (agency-wide) or specific to a program area or organizational unit. (36 CFR 1220.18)

20. Does your agency evaluate, by conducting inspections/audits/reviews, its records management program to ensure that it is efficient, effective, and compliant with all applicable records management laws and regulations?

> ******For this question, your agency's records management program, or a major component of the program (e.g., vital records identification and management, the records disposition process, records management training, or the management of your agency's electronic records) must be the primary focus of the inspection/audit/review.

☐ Yes, evaluations are conducted by the Records Management Program
☐ Yes, evaluations are conducted by the Office of Inspector General
☐ Yes, evaluations are conducted by the Records Management Program AND the Office of Inspector General
☐ Yes, evaluations are conducted by: (fill in the blank)
☐ No, please explain
☐ Do not know

21. How often is your records management program, or a major component of your program, evaluated for compliance with agency records management policies and procedures?

☐ Annually

☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

22. Was a formal written report prepared as part of the most recent inspection/audit/review?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

23**.** Do your agency's evaluation procedures include creating plans of corrective action that are monitored for implementation?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

An essential control for any records management program is the establishment of performance goals and associated performance targets and performance measures.

Performance goals are the target levels of performance. Performance goals should be specific, measurable, attainable, results-oriented, and time-bound.

24. Has your agency established performance goals for its records management program?

*Examples of performance goals include but are not limited to:

- Identifying and scheduling all paper and non-electronic records by the end of FY 2017
- Developing computer-based records management training modules by the end of FY 2017
- Planning and piloting an electronic records management solution for email by the end of FY 2018
- Updating records management policies by the end of the year
- Conducting records management evaluations of at least one program area each quarter

☐ Yes
☐ No
☐ Pending final approval
☐ Currently under development
☐ Do not know

Performance measures are the indicators or metrics against which a program's performance can be gauged. Performance measures should provide a basis for comparing actual results with established performance goals. ("Performance Measurement Challenges and Strategies," June 18, 2003, white paper associated with the Office of Management and Budget's Program Assessment Rating Tool (PART); and "Government Performance and Results Modernization Act of 2010," Section 4, Performance Reporting Amendments.)

25. Has your agency's records management program identified performance measures for records management activities such as training, records scheduling, permanent records transfers, etc.?

*Examples of performance measures include but are not limited to:

- Percentage of agency employees that receive records management training in a year
- A reduction in the volume of inactive records stored in office space
- Percentage of eligible permanent records transferred to NARA in a year
- Percentage of records scheduled
- Percentage of offices evaluated/inspected for records management compliance
- Percentage of email management auto-classification rates
- Development of new records management training modules
- Audits of internal systems
- Annual updates of file plans
- Performance testing for email applications to ensure records are captured
- Percentage of records successfully retrieved by Agency FOIA Officer in response to FOIA requests

☐ Yes
☐ No
☐ Pending final approval
☐ Currently under development
☐ Do not know

26. Does your agency's records management program have **documented and approved** policies and procedures that instruct staff on how your agency's permanent records in all formats must be managed and stored? (36 CFR 1222.34(e))

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

27. Is your agency subject to laws or regulations that require you to conduct business using paper or analog records?*

*Components of departmental agencies may answer "Yes" if this is handled by the department. Department Records Officers may answer "Yes" if this is handled at the component level.

☐ Yes
☐ No
☐ Do not know

28. If Yes: Which of the following possible examples of requirements for paper or analog records apply to your agency's needs? (Choose all that apply)

☐ Wet signatures are required for transactions with non-Federal entities (including the public)
☐ Wet signatures are required for transactions between Federal agencies
☐ Transactions are required to be conducted using paper / hard copy
☐ Agency is required to offer paper / hard copy as an available option for transactions
☐ Other, please be specific:
☐ Do not know
☐ Comments: (Optional)

Vital records* (also known as Essential Records) are records needed to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records). (36 CFR 1223.2)

***pending updates to regulations, the Records Management Self-Assessment still uses this terminology**

A program area is responsible for mission-related activities. An administrative area is responsible for activities not specific to the mission of the agency. (36 CFR 1220.34(d))

29. Has your agency identified the vital records of all its program and administrative areas? (36 CFR 1223.16)

*Components of departmental agencies may answer "Yes" if this is handled by the department.

☐ Yes
☐ No
☐ Do not know

30. How often does your agency review and update its vital records inventory? (36 CFR 1223.14)

☐ Annually

☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Never
☐ Do not know

31. Is your vital records plan part of the Continuity of Operations (COOP) plan?

☐ Yes
☐ No
☐ Do not know

32. Does your agency have policies in place to protect records and information from internal and external risks?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

Agencies are required to have a Freedom of Information Act (FOIA) program (5 U.S.C. 552). The ability to find records is essential for a successful FOIA program. The following questions related to your agency's FOIA program may require consultation with your agency's FOIA Officer.

33. The Agency Records Officer and the FOIA Officer:

☐ Are the same person
☐ Coordinate closely together
☐ Work together sometimes
☐ Never work together

34. Are the Agency Records Officer and the FOIA Officer in the same office/division within your agency?

☐ Yes
☐ No
☐ Do not know
☐ Agency Records Officer and the FOIA Officer are the same person

35. Records needed to respond to a FOIA request are readily accessible and located by staff responsible for FOIA:

☐ Always
☐ Most of the time
☐ Some of the time
☐ Never
☐ Do not know

36. Staff responsible for FOIA can search for records without contacting others (i.e. program offices):

☐ Always
☐ Most of the time
☐ Some of the time
☐ Never
☐ Do not know

37. At what point in the FOIA process does your agency inform requesters of the Office of Government Information Services' (OGIS) dispute resolution services? (Choose all that apply)

☐ When there is an adverse determination
☐ When notifying the requester that the agency needs more than 10 additional days to process a request
☐ When responding to the requester's appeal
☐ Never
☐ Do not know
☐ Other, please explain

38. What mode does your agency most often use to release records under FOIA?

☐ Email
☐ Online portal
☐ U.S. mail
☐ Other, please explain

39. In 2015, NARA and the Federal Records Management Council introduced the *Federal RIM Program Maturity Model*. Are you familiar with this or other maturity models?

☐ Yes
☐ No
☐ Comments: (Optional)

40. If Yes: Are you using the *Federal RIM Program Maturity Model* or other maturity models to measure the maturity of the records management program?

☐ Yes
☐ No
☐ Comments: (Optional)

41. Does your agency use your Records Management Self-Assessment scores to measure the effectiveness of the records management program?

☐ Yes
☐ No
☐ Do not know
☐ Comments (Optional): Please include in your comments how you use the Records Management Self-Assessment.

42. Please add any additional comments about your agency for Section II: Oversight and Compliance. (Optional)

Section III: Records Management Program - Records Disposition

Records disposition refers to actions taken with regard to Federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure. Disposition is a comprehensive term that includes both destruction and transfer of Federal records to the National Archives of the United States. (36 CFR Parts 1222, 1224, 1225 and 1226)

The next series of questions relate to your agency's efforts to schedule its records.

43. Are records and information in your agency managed throughout the lifecycle [creation/capture, classification, maintenance, retention, and disposition] by being properly identified, classified using a taxonomy, inventoried, and scheduled? (36 CFR 1222.34, 36 CFR 1224.10, and 36 CFR 1225.12)

☐ Yes
☐ No
☐ To some extent
☐ Do not know

44. Are records and information in your agency easily retrievable and accessible when needed for agency business? (36 CFR 1220.32(c))

☐ Yes, all records are easily retrievable and accessible when needed

☐ Most records can be retrieved and accessed in a timely manner
☐ Some records can be retrieved and accessed in a timely manner
☐ No
☐ Do not know

45. Does your agency disseminate *every* approved disposition authority (including newly approved records schedules and General Records Schedule items) to agency staff within six months of approval? (36 CFR 1226.12(a))

☐ Yes
☐ No
☐ Do not know

46. If Yes: What method(s) does your agency use? (Choose all that apply)

☐ Post to internal website or other shared information location
☐ Memorandum or email notification
☐ Update training materials
☐ Update records management policies and/or handbooks
☐ Other, please explain

47. Does your agency have a method of continually identifying new and unscheduled records?

☐ Yes
☐ No
☐ Do not know

48. If Yes: Which method(s) does your agency use? (Choose all that apply)

☐ Regular surveys
☐ Regular inventories
☐ Records management evaluations, site assessments, or audits of program offices
☐ Work with program managers to identify new programs and related records
☐ Work with Privacy Officer and review SORNs (Systems of Records Notices)
☐ Work with FOIA Officer
☐ Records Liaison Officers notify Agency Records Officer of new record series
☐ Require use and annual update of file plans
☐ Participate in design and retirement of information systems and note changes in records
☐ Outreach and awareness
☐ Other, please explain

The next series of questions relate to permanent records.

49. Does your agency have permanent records that are 30 years old or older that are located in agency office space, agency-operated records centers and/or commercial records centers? (36 CFR 1235.12(b) and M-12-18)

☐ Yes
☐ No
☐ Do not know

50. Are you aware of the requirement to formally request permission from NARA to retain permanent records beyond that specified in your agency's NARA-approved records schedules as outlined in 36 CFR 1235.14 and 1235.16?

☐ Yes
☐ No

51. Did your agency transfer permanent non-electronic records to NARA during FY 2017? (36 CFR 1235.12)

☐ Yes
☐ No
☐ No - No records were eligible for transfer during FY 2017
☐ No - New agency, records are not yet old enough to transfer
☐ No - My agency does not have any permanent non-electronic records
☐ Do not know
☐ Other, please explain

52. Did your agency transfer permanent electronic records to NARA during FY 2017? (36 CFR 1235.12)

☐ Yes
☐ No
☐ No - No electronic records/systems were eligible for transfer during FY 2017
☐ No - New agency, electronic records/systems are not old enough to transfer
☐ No - My agency does not have any permanent electronic records
☐ Do not know
☐ Other, please explain

53. Does your agency track when its permanent records (regardless of format) are due to be transferred to NARA?

☐ Yes
☐ No
☐ Do not know

☐ Not applicable, please explain

54. If Yes: What method(s) does your agency use to track its permanent records? (Choose all that apply)

☐ Rely on Federal Records Center notifications
☐ Maintain an inventory
☐ Database or other automated tracking
☐ Manual tracking
☐ Other, please explain

The next series of questions relate to your agency's handling of records for senior officials.

Senior officials are the heads of departments and independent agencies; their deputies and assistants; the heads of program offices and staff offices including assistant secretaries, administrators, and commissioners; directors of offices, bureaus, or equivalent; principal regional officials; staff assistants to those aforementioned officials, such as special assistants, confidential assistants, and administrative assistants; and career Federal employees, political appointees, and officers of the Armed Forces serving in equivalent or comparable positions.

55. Does your agency conduct and document for accountability purposes training and/or other briefings as part of the on-boarding process for senior officials on their records management roles and responsibilities, including the appropriate disposition of records and the use of personal and unofficial email accounts? (36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b))

☐ Yes
☐ Yes, but not documented
☐ No
☐ Do not know
☐ Not applicable, please explain

56. If Yes or Yes, but not documented: Is the Agency Records Officer and/or Senior Agency Official for Records Management involved in on-boarding briefings or other processes for newly appointed senior officials?

☐ Yes
☐ No
☐ Do not know

57. Does your agency conduct and document for accountability purposes exit briefings for departing senior officials on the appropriate disposition of the records, including email, under their immediate control? (36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b))

☐ Yes
☐ Yes, but not documented
☐ No
☐ Do not know
☐ Not applicable, please explain

58. If Yes or Yes, but not documented: Is the Agency Records Officer and/or Senior Agency Official for Records Management involved in exit briefings or other exit clearance processes for departing senior officials?

☐ Yes
☐ No
☐ Do not know

59. If Yes or Yes, but not documented: Does the exit or separation process for departing senior officials include records management program staff or other designated official(s) reviewing and approving the removal of personal papers and copies of records by those senior officials? (36 CFR 1222.24(a)(6))

☐ Yes
☐ No, please explain
☐ Do not know

The next series of questions relate to where your agency stores its inactive temporary and/or permanent records, regardless of format.

Commercial records storage facilities are private sector commercial facilities that offer records storage, retrieval, and disposition services.

An agency records center is a records storage facility, operated by a Federal agency and capable of storing more than 25,000 cubic feet of records.

Records staging or holding areas are areas designated within the agency's office space that are used for the temporary storage of records. The term does not include off-site storage such as commercial or agency records storage facilities. Records staging or holding areas may be established by an agency for maintaining records no longer needed in office space but whose volume or retention periods are insufficient to warrant transfer to a records center before final disposition.

60. Does your agency store inactive temporary and/or permanent records in a commercial records storage facility?

☐ Yes
☐ No

☐ Do not know

61. If Yes: Does the facility comply with the standards prescribed by 36 CFR 1234?

☐ Yes
☐ No
☐ Do not know

62. Does your agency store inactive temporary and/or permanent records in an agency records center? (Note: This does NOT include agency staging areas and temporary holding areas.)

☐ Yes
☐ No
☐ Do not know

63. If Yes: Does the records center comply with the standards prescribed by 36 CFR 1234?

☐ Yes
☐ No
☐ Do not know

64. Does your agency store inactive temporary and/or permanent records in an agency records staging or holding area?

☐ Yes
☐ No
☐ Do not know

65. If Yes: Does the staging or holding area(s) comply with the standards prescribed by 36 CFR 1234.10, 36 CFR 1234.12, and 36 CFR 1234.14?*

*It is not required but encouraged that staging or holding areas comply with 36 CFR 1234.

☐ Yes
☐ No
☐ Do not know

66. If Yes to Q60, 62, or 64: Please estimate the volume of inactive temporary records, in cubic feet, that your agency is storing in a non-NARA storage facility. (A cubic foot is equivalent to one records storage box.)

☐ 0 - 1,000
☐ 1,000 - 5,000

☐ 5,000 - 15,000
☐ 15,000 - 25,000
☐ 25,000 - 50,000
☐ 50,000 - 100,000
☐ 100,000 - 250,000
☐ 250,000 or greater

67. If Yes to Q60, 62, or 64: Please estimate the volume of inactive permanent records, in cubic feet, that your agency is storing in a non-NARA storage facility. (A cubic foot is equivalent to one records storage box.)

☐ 0 - 1,000
☐ 1,000 - 5,000
☐ 5,000 - 15,000
☐ 15,000 - 25,000
☐ 25,000 - 50,000
☐ 50,000 - 100,000
☐ 100,000 - 250,000
☐ 250,000 or greater

NARA annually provides agencies storing records in a Federal Records Center with transfer requests populated in the Electronic Records Archives (ERA) for permanent records eligible for transfer to the National Archives. (This is known as the Annual Move.) Agencies are then responsible to submit those transfer requests based on these lists in order to complete the cycle.

68. Did your agency receive a list of permanent records eligible for transfer in FY 2017?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, my agency does not store records in the Federal Records Centers

69. If Yes: Did your agency submit transfer requests in FY 2017 based on the Annual Move list of eligible permanent records to be accessioned by the National Archives?

☐ Yes
☐ No, please explain
☐ Do not know

70. Please add any additional comments about your agency for Section III: Records Disposition. (Optional)

Section IV: Records Management Program - Electronic Records

Electronic information system means an information system that contains and provides access to computerized Federal records and other information. (36 CFR 1236.2)

The following types of records management controls are needed to ensure that Federal records in electronic information systems can provide adequate and proper documentation of agency business for as long as the information is needed. Agencies must incorporate controls into the electronic information system or integrate them into a recordkeeping system that is external to the information system itself. (36 CFR 1236.10)

(a) Reliability: Controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

(b) Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

(c) Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.

(d) Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

(e) Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.

(f) Context: Mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity.

(g) Structure: Controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

71. Has your agency incorporated and/or integrated internal controls to ensure the reliability, authenticity, integrity, and usability of agency electronic records maintained in electronic information systems? (36 CFR 1236.10)

☐ Yes
☐ To some extent
☐ No
☐ Do not know
☐ Not applicable, please explain

Migration is a set of organized tasks designed to achieve periodic transfer of digital materials from one hardware/software configuration to another, or from one generation of computer technology to a subsequent generation.

Metadata consists of preserved contextual information describing the history, tracking, and/or management of an electronic document. (36 CFR 1236.2)

72. Does your agency have **documented and approved** procedures to enable the migration of records and associated metadata to new storage media or formats so that records are retrievable and usable as long as needed to conduct agency business and to meet NARA-approved dispositions? (36 CFR 1236.20(b)(6))

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

73. Are records management staff involved in developing procedures to ensure that records are properly migrated from retired systems? (36 CFR 1235.20(b)(6))

☐ Yes
☐ No
☐ To some extent
☐ Do not know
☐ Not applicable, please explain

74. Does your agency maintain an inventory of electronic information systems that indicates whether or not each system is covered by an approved NARA disposition authority? (36 CFR 1236.26(a))

☐ Yes
☐ No, please explain
☐ Do not know

75. Does your agency ensure that records management functionality, including the capture, retrieval, and retention of records according to agency business needs and NARA-approved records schedules, is incorporated into the design, development, and implementation of its electronic information systems? (36 CFR 1236.12)

*Components of departmental agencies may answer "Yes" if this is handled by the department.

☐ Yes
☐ No, please explain
☐ Do not know
☐ Not applicable, please explain

76. Does your agency's records management program staff participate in the design, development, and implementation of new electronic information systems?

☐ Yes
☐ No, please explain
☐ To some extent
☐ Do not know
☐ Not applicable, please explain

77**.** If Yes or To some extent: Which of these activities does your agency's records management program staff participate in to ensure that records requirements are part of the recommended solution? (Choose all that apply)

☐ Participate in review and acceptance of proposals for new systems
☐ Participate as stakeholder in requirements gathering
☐ Participate as stakeholder in design phase
☐ Participate as stakeholder in development phase including testing the system
☐ Provide sign off authority for the implementation of new systems
☐ Monitor system for adherence to standards, policies, and procedures
☐ Provide information only
☐ Do not know
☐ Other, please explain

78. Does your agency have documented and approved policies requiring permanent electronic records be managed in an electronic format for eventual transfer to NARA?

☐ Yes
☐ No
☐ No, under development
☐ Do not know

79. Does your agency have protections against unauthorized use, alteration, alienation or deletion of all electronic records?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

80. Does your agency have the capability to place legal holds on all electronic records until disposition is authorized?

☐ Yes

☐ No
☐ To some extent
☐ Do not know

Executive Order 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Under 32 CFR 2001.50, the Office of Information Security and Oversight provides further definition and guidance. (https://www.archives.gov/isoo/about)

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes in 32 CFR 2002 the way the executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. (https://www.archives.gov/cuiza/about)

81. Does your agency comply with the requirements under Executive Orders 13526 and 13556 for managing classified and controlled unclassified information in systems that contain electronic records?

☐ Yes
☐ No
☐ To some extent
☐ Do not know
☐ Not applicable, not an executive branch agency

82. Does your agency have the ability to search across all systems to find electronic records needed for agency business, FOIA and other information requests?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

83. Does your agency have a digitization strategy to reformat permanent records created in hard copy or other analog formats (e.g., microfiche, microfilm, analog video, and analog audio)?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

Web content is the textual, visual, or aural content that is encountered as part of the user experience on websites. It may include text, images, sounds, videos, animations, and more.

A Web Content Record is defined as information that meets the definition of Federal record and is provided via an agency's website.

84. Does your agency manage your web content as records?

☐ Yes
☐ No
☐ Do not know

85. If Yes: How does your agency capture web content managed as records? (Choose all that apply)

☐ Content is printed and filed
☐ Content is captured manually through periodic web snapshots
☐ Content is automatically harvested using specific tools
☐ Do not know
☐ Other, please explain

86. If Yes: Web content management includes: (Choose all that apply)

☐ Identification of record copy whether online or off-line
☐ Identifying the program office responsible for official record copy
☐ Records retention scheduling of web content
☐ Preservation of record copy in accordance with retention schedule
☐ Migration of content when website is updated
☐ Maintaining access throughout the life-cycle even if removed from the website
☐ Managing convenience copies as duplicates and applying disposition as needed
☐ Transfer of permanent web records to the National Archives
☐ Other, please explain

87. Does your agency use cloud services?

☐ Yes
☐ No
☐ Do not know

88. If Yes: For what purpose(s) is your agency using cloud services? (Choose all that apply)

☐ Email
☐ Administrative functions such as payroll, purchasing, and financial management
☐ Mission/program-related functions
☐ Other, please explain
☐ Do not know

89. If Yes: Are recordkeeping requirements included?

☐ Yes
☐ No
☐ Do not know

90. Is the records management program and related requirements included in your agency's Information Resource Management Plan or an equivalent information management plan? (OMB Circular A-130, Managing Information as a Strategic Resource)

☐ Yes
☐ No
☐ Do not know

The next series of questions relate to email.

An electronic mail system is a computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers, and word processing documents not transmitted on an email system. (36 CFR 1236.2)

91. Does your agency have **documented and approved** policies and procedures in place to handle email records that have a retention period longer than 180 days? (36 CFR 1236.22)

☐ Yes
☐ No, please explain
☐ Do not know

92. Does your agency have **documented and approved** policies and procedures to implement the guidelines for the transfer of permanent email records to NARA described in NARA Bulletin 2014-04: Revised Format Guidance for the Transfer of Permanent Electronic Records Appendix A: Tables of File Formats, Section 9 - Email? (36 CFR 1236.22(e))

☐ Yes
☐ No
☐ Do not know

Regardless of how many Federal email accounts individuals use to conduct official business, agencies must ensure that all accounts are managed, accessible and identifiable according to Federal recordkeeping requirements. (36 CFR 1236.22)

93. Do employees in your agency have more than one agency-administered email account? (NARA Bulletin 2013-03)

*Examples of business needs may include but are not limited to:

- Using separate accounts for public and internal correspondence
- Creating accounts for a specific agency initiative which may have multiple users
- Using separate accounts for classified information and unclassified information

☐ Yes
☐ No
☐ Do not know

94. Does your agency have **documented and approved** policies that address these types of accounts and that state that email records must be preserved in an appropriate agency recordkeeping system? (36 CFR 1236.22)

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

95. Does your agency allow the use of personal email accounts to conduct official business? (36 CFR 1236.22(b))

☐ Yes
☐ No
☐ Do not know

96. Does your agency have **documented and approved** policies that address the use of personal email accounts, whether or not allowed, that state that all emails created and received by such accounts must be preserved in an appropriate agency recordkeeping system and that a complete copy of all email records created and received by users of these accounts must be forwarded to an official electronic messaging account of the officer or employee no later than 20 days after the original creation or transmission of the record? (36 CFR 1236.22(b) and P.L. 113-187)

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

97. Does your agency's email system(s) retain the intelligent full names on directories or distribution lists to ensure identification of the sender and addressee(s) for those email messages that are Federal records? (36 CFR 1236.22(a)(3))

☐ Yes
☐ No
☐ Do not know

98. What method(s) does your agency employ to capture and manage email records? (Choose all that apply)

☐ Captured and stored in an email archiving system
☐ Captured and stored in an electronic records management system
☐ Captured and stored as personal storage table (.PST) files
☐ Print and file
☐ Not captured and email is managed by the end-user in the native system
☐ Other, please be specific

99. Does your agency evaluate, monitor, or audit staff compliance with the agency's email preservation policies? (36 CFR 1220.18)

☐ Yes
☐ No
☐ Do not know

100. If Yes: How often does your agency evaluate, monitor, or audit staff compliance with the agency's email preservation policies?

☐ Annually
☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Do not know

101. Which of the following has your agency chosen for retention scheduling of email?

☐ GRS 6.1: Email Managed under a Capstone Approach
☐ Agency-specific schedule
☐ Combination of agency-specific schedule and GRS 6.1
☐ Email retention has not been scheduled
☐ Do not know
☐ Other, please explain

102. Is your agency able to access email from departed employees in a usable format?

☐ Yes
☐ No

☐ To some extent
☐ Do not know

103. Is your agency able to prevent unauthorized access, modification, or destruction of emails?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

104. Can your agency transfer permanent email records to the National Archives in accordance with agency records schedules or General Records Schedules and NARA regulations and guidance?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

105. Is your agency able to decrypt permanent email records before they are accessioned by NARA?

☐ Yes
☐ No
☐ Do not know

106. Does your agency have an approved records schedule covering electronic messages including text messages, chat/instant messages, voice messages, and messages created in social media tools or applications that meet the definition of a Federal record?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

107. Does your agency have **documented and approved** policies and procedures in place to manage electronic messages including text messages, chat/instant messages, voice messages, and messages created in social media tools or applications?

☐ Yes
☐ No
☐ No, pending final approval

☐ No, under development
☐ Do not know
☐ Other, please explain

108. Please add any additional comments about your agency for Section IV: Electronic Records. (Optional)

Section V: Agency Demographics

109. Does the records management program have a dedicated budget?

☐ Yes
☐ No
☐ Do not know

110. Please report actual obligations for records management purposes incurred in FY 2017 for each of the following categories.

Personnel Compensation and Benefits (Federal employees only) for records management purposes:

$_____
☐ Do not know
☐ Prefer not to answer

Records Storage Contracts and Inter-Agency Agreements (paper and analog formats):

$_____
☐ Do not know
☐ Prefer not to answer

Records Management IT Systems and Electronic Records Storage:

$_____
☐ Do not know
☐ Prefer not to answer

Travel and Transportation for records management purposes:

$_____
☐ Do not know
☐ Prefer not to answer

Records Management Training:

$_____
☐ Do not know
☐ Prefer not to answer

Other: (Please be specific)

$_____

☐ Do not know

☐ Prefer not to answer

Comments: (Optional)

111. How many full-time equivalents (FTE) are in your agency/organization?

☐ 500,000 or more FTEs
☐ 100,000 499,999 FTEs
☐ 10,000 99,999 FTEs
☐ 1,000 9,999 FTEs
☐ 100 999 FTEs
☐ 1 99 FTEs
☐ Not Available

112. What other staff, offices, or program areas did you consult when you completed this self-assessment? (Choose all that apply)

☐ Senior Agency Official
☐ Office of the General Counsel
☐ Program Managers
☐ FOIA Officer
☐ Information Technology staff
☐ Records Liaison Officers or similar
☐ Administrative staff
☐ Other, please be specific:
☐ None

113. How much time did it take you to gather the information to complete this self-assessment?

☐ Under 3 hours
☐ More than 3 hours but less than 6 hours
☐ More than 6 hours but less than 10 hours
☐ Over 10 hours

114. Did your agency's senior management review and concur with your responses to the 2017 Records Management Self-Assessment?

☐ Yes
☐ No
☐ Do not know

115. Please provide your contact information.

Name:
Agency, Bureau, or Office:
Job Title:
Email Address:
Phone Number:

116. Are you the Agency Records Officer?

☐ Yes
☐ No

117. If No: Please provide the Agency Records Officer's contact information.

Name:
Email Address:
Phone Number:

118. Do you have any suggestions for improving the Records Management Self-Assessment next year?

NARA reserves the right to request additional documentation or a follow-up meeting to verify your responses. If you wish to provide supporting documentation for your answers or other information to NARA, please send it to rmselfassessment@nara.gov.

Thank you for completing the 2017 Records Management Self-Assessment! If you have any questions about the self-assessment, please send a message to rmselfassessment@nara.gov.

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, March 7, 2018 10:47 AM
To:	Andre Sivels NOAA Federal
Cc:	Robert Swisher NOAA Federal; Lola Stith NOAA Affiliate; Dennis Morgan NOAA Federal
Subject:	Re: 2017 Records Management Assessment
Attachments:	2017 RMSA Questionnaire.docx

Hi Andre

No problem. Here are NOAA FOIA's input for the portions of the RMSA Questionnaire.

Looping in Rob, Lola, and Dennis for data call tracking. We consider this data call complete.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Wed, Mar 7, 2018 at 10:15 AM, Andre Sivels NOAA Federal <andre.sivels@noaa.gov> wrote:

> Hi Mark
>
> I am in the process of review the questions for the NARA annual records management assessment and noticed they have 6 questions related to FOIA. Can you provide answers to questions 33 to 38 on the attached questionnaire and return to Monday March 12th, Thanks
>
> Andre
>
> Andre Sivels
> NOAA Records Officer
> U.S. Department of Commerce
> 1305 East West Highway Rm 7439
> Silver Spring, MD 20910
> Phone: 301628 0946
> Fax: 301 713 1169

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)
2017 RECORDS MANAGEMENT SELF-ASSESSMENT

Welcome to the 2017 Records Management Self-Assessment!

Before you begin, please note the following information.

Except where indicated, the questions in this survey are intended to cover all records regardless of format, as defined in 44 U.S.C. 3301.

The questions apply regardless of whether your agency's work processes are conducted manually or electronically.

Unless otherwise indicated, the following questions refer to FY 2017 (October 1, 2016, through September 30, 2017).

Your answers to the self-assessment questions must be specific to records management activities in your agency. We have added a "not applicable" answer option to some questions. In general, use this option only if a question references an activity or action that is not conducted in your agency because of its size or if you are a Departmental Records Officer and are not responsible for the activity or action. In some cases, if the activity is being done by a departmental records management program, component agencies of that department may answer "Yes."

NOTE: Please note that your responses to questions in this assessment may be subject to public release pursuant to FOIA. However, we will not release responses to questions that contain detailed descriptions of agency activities.

NARA reserves the right to follow up with agencies to obtain additional information and/or documentation that supports their answers to the questions in this self-assessment.

As in previous years we will be conducting a validation process. Your agency may be selected at random to provide additional documentation and/or take part in interviews to discuss your records management program activities.

If you have any questions about this self-assessment or need additional information to answer a question(s), please send an email message to rmselfassessment@nara.gov.

Section I: Records Management Program - Activities

The next series of questions relate to administration of the records management program.

1. Is there a person in your agency who is responsible for coordinating and overseeing the implementation of the records management program? (36 CFR 1220.34(a))

☐ Yes
☐ No
☐ Do not know

2. If Yes: Please provide the person's name, position title, and office.

3. If Yes: How long has this person been responsible for coordinating and overseeing the implementation of the records management program?

☐ 5 or more years
☐ 3 to 4 years
☐ 1 to 2 years
☐ Less than a year

4. Does your agency have a Senior Agency Official for Records Management (SAORM)? (If you are a component of a department, you may answer "Yes," even if this is not being done at the component level.)

☐ Yes
☐ No
☐ Do not know

5. If Yes: Does your Agency Records Officer meet regularly (four or more times a year) with the SAORM to discuss the agency records management program's goals?

☐ Yes
☐ No
☐ Do not know

6. Does your agency use the Records and Information Management Series, 0308, (job series) released by the Office of Personnel Management in 2015?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, my agency does not use the General Schedule (GS) job classification

7. Does your agency have a network of designated employees within each program and administrative area who are assigned records management responsibilities? These individuals are often called Records Liaison Officers (RLOs), though their titles may vary. (36 CFR 1220.34(d))

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency has less than 100 employees
☐ Not applicable, Departmental Records Officer - this is done at the component level

8. Of the following, please select the one that best describes your records management staff. This includes only those specifically assigned to the records management program.

☐ All records management staff are agency personnel
☐ All records management staff are contractors
☐ Records management staff includes both agency personnel and contractors

In general, an FTE is equivalent to one full-time employee who is assigned full-time to records management (2,080 hours per year). An employee who works part-time or is assigned records management as one of several unrelated responsibilities should be counted as a fraction of an FTE, representing the estimated number of hours worked on records management per year as a percentage of 2,080 hours.

9. How many FTE agency personnel (non-contractors) are specifically assigned records management responsibilities? (These are individuals directly responsible for records management program implementation, not contacts within mission areas with minimal records management duties.)*

*For Department Records Officers, please include only the staff at the Department level, not agency components, as component agency records officers will be answering for their agencies.

☐ <1
☐ 1
☐ 2 - 10
☐ 10 - 20
☐ More than 20
☐ Do not know
☐ Not available
☐ Not applicable, all records management staff are contractors

10. If your agency uses contractors, how many contractor FTE are specifically assigned records management responsibilities? (These are individuals directly responsible for records management program implementation, not general contacts within mission areas with minimal records management duties.)*

*For Department Records Officers, please include only the staff at the Department level, not agency components, as component agency records officers will be answering for their agencies.

☐ <1
☐ 1
☐ 2 - 10
☐ 10 - 20
☐ More than 20
☐ Do not know
☐ Not available
☐ Not applicable, all records management staff are agency personnel

The next series of questions relate to records management directives.

11. Does your agency have a documented and approved records management directive(s)? (36 CFR 1220.34(c))

☐ Yes
☐ No, pending final approval
☐ No, under development
☐ No
☐ Do not know

12. When was your agency's directive(s) last reviewed and/or revised to ensure it includes all new records management policy issuances and guidance?

☐ FY 2017 - present
☐ FY 2015 - 2016
☐ FY 2013 - 2014
☐ FY 2012 or earlier
☐ Do not know
☐ Not applicable, agency does not have a records management directive

The next series of questions relate to records management training.

Formal records management training is the communication of standardized information that improves the records management knowledge, skills, and/or awareness of agency employees. Training can be either in a classroom setting or distance-based (e.g., web-based training), but it *must:*

- **be regular (occurring more than just once);**
- **be repeatable and formal (all instructors must provide the same message, not in an ad hoc way); and**

- **communicate the agency's vision of records management.**

13. Does your agency have internal records management training*, based on agency policies and directives, for employees assigned records management responsibilities? (36 CFR 1220.34(f))

*Includes NARA's records management training workshops that were ***customized*** specifically for your agency or use of an ***agency-customized*** version of the Federal Records Officer Network (FRON) RM 101 course.

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know
☐ Not applicable, please explain

14. Has your agency developed mandatory internal, staff-wide, formal training*, based on agency policy and directives, covering records in all formats, including electronic communications such as email, text messages, chat, or other messaging platforms or apps, such as social media or mobile device applications, which helps agency employees and contractors fulfill their recordkeeping responsibilities?** (36 CFR 1220.34(f))

*Includes NARA's records management training workshops that were ***customized*** specifically for your agency or use of an ***agency-customized*** version of the Federal Records Officer Network (FRON) RM 101 course.

**Components of departmental agencies may answer "Yes" if this is handled by the department. Department Records Officers may answer "Yes" if this is handled at the component level.

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

Senior officials are the heads of departments and independent agencies; their deputies and assistants; the heads of program offices and staff offices including assistant secretaries, administrators, and commissioners; directors of offices, bureaus, or equivalent; principal regional officials; staff assistants to those aforementioned officials, such as special assistants, confidential assistants, and administrative assistants; and career Federal employees, political appointees, and officers of the Armed Forces serving in equivalent or comparable positions. (General Records Schedule (GRS) 6.1, item 010)

15. Does your agency require that all senior and appointed officials, including those incoming and newly promoted, receive training on the importance of appropriately managing records under their immediate control? (36 CFR 1220.34(f))

☐ Yes
☐ No
☐ Do not know

16. Is records management training included in the in-processing for new employees in your agency?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

17. Please add any additional comments about your agency for Section I: Activities. (Optional)

Section II: Records Management Program – Oversight and Compliance

Agency records management programs must provide for effective controls over the creation, maintenance, and use of records in the conduct of current business. (36 CFR 1220.30(c)(1))

Internal controls are integral components of an organization's management that provide reasonable assurance of the effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. ("Standards for Internal Control in the Federal Government" (GAO-14-704G), U.S. Government Accountability Office, September 2014.)

Internal controls are:

- **Geared to the achievement of objectives in one or more categories—operations, reporting, and compliance;**
- **Processes consisting of ongoing tasks and activities—a means to an end, not an end in itself;**
- **Carried out by people—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to effect internal control;**
- **Able to provide reasonable assurance, but not absolute assurance, to an entity's senior management;**
- **Adaptable to the organization's entire structure—flexible in application for the entire entity or for a particular regional office, division, operating unit, or business process.**

Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews/audits of operating performance, security of assets (limited access to inventories or equipment), and segregation of duties (separate personnel with authority to authorize a transaction, process the transaction, and review the transaction). Monitoring the effectiveness of internal controls should occur in the normal course of business. Periodic assessments should be integrated as part of management's continuous monitoring of internal control, which should be ingrained in the agency's operations. ("2013 Internal Control - Integrated Framework," Committee of Sponsoring Organizations (COSO) Executive Summary, May 14, 2013; and OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016.)

18. In addition to your agency's established records management policies and records schedules, has your agency's records management program developed and implemented internal controls to ensure that all eligible, permanent agency records in all media are transferred to NARA according to approved records schedules? (36 CFR 1222.26(e))

> **These controls must be internal to your agency. Reliance on information from external agencies (e.g., NARA's Federal Records Centers) or other organizations should not be considered when responding to this question.

*Examples of records management internal controls include but are not limited to:

- Regular briefings and other meetings with records creators
- Monitoring and testing of file plans
- Regular review of records inventories
- Internal tracking database of permanent record authorities and dates

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

19. In addition to your agency's established policies and records schedules, has your agency developed and implemented internal controls to ensure that Federal records are not destroyed before the end of their retention period? (36 CFR 1222.26(e))

> **These controls must be internal to your agency. Reliance on information from external agencies (e.g., NARA's Federal Records Centers) or other organizations should not be considered when responding to this question.

*Examples of records management internal controls include but are not limited to:

- Regular review of records inventories
- Approval process for disposal notices from off-site storage

- Require certificates of destruction
- Monitoring shredding services
- Performance testing for email
- Monitoring and testing of file plans
- Pre-authorization from records management program before records are destroyed
- Ad hoc monitoring of trash and recycle bins
- Notification from facilities staff when large trash bins or removal of boxes are requested
- Annual records clean-out activities sponsored and monitored by records management staff

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

An evaluation is an inspection, audit, or review of one or more records management programs for effectiveness and for compliance with applicable laws and regulations. An evaluation contains recommendations for correcting or improving records management practices, policies, and procedures as well as follow-up activities, including reporting on and implementing recommendations. Evaluations may be comprehensive (agency-wide) or specific to a program area or organizational unit. (36 CFR 1220.18)

20. Does your agency evaluate, by conducting inspections/audits/reviews, its records management program to ensure that it is efficient, effective, and compliant with all applicable records management laws and regulations?

> ******For this question, your agency's records management program, or a major component of the program (e.g., vital records identification and management, the records disposition process, records management training, or the management of your agency's electronic records) must be the primary focus of the inspection/audit/review.

☐ Yes, evaluations are conducted by the Records Management Program
☐ Yes, evaluations are conducted by the Office of Inspector General
☐ Yes, evaluations are conducted by the Records Management Program AND the Office of Inspector General
☐ Yes, evaluations are conducted by: (fill in the blank)
☐ No, please explain
☐ Do not know

21. How often is your records management program, or a major component of your program, evaluated for compliance with agency records management policies and procedures?

☐ Annually

☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

22. Was a formal written report prepared as part of the most recent inspection/audit/review?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

23**.** Do your agency's evaluation procedures include creating plans of corrective action that are monitored for implementation?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

An essential control for any records management program is the establishment of performance goals and associated performance targets and performance measures.

Performance goals are the target levels of performance. Performance goals should be specific, measurable, attainable, results-oriented, and time-bound.

24. Has your agency established performance goals for its records management program?

*Examples of performance goals include but are not limited to:

- Identifying and scheduling all paper and non-electronic records by the end of FY 2017
- Developing computer-based records management training modules by the end of FY 2017
- Planning and piloting an electronic records management solution for email by the end of FY 2018
- Updating records management policies by the end of the year
- Conducting records management evaluations of at least one program area each quarter

☐ Yes
☐ No
☐ Pending final approval
☐ Currently under development
☐ Do not know

Performance measures are the indicators or metrics against which a program's performance can be gauged. Performance measures should provide a basis for comparing actual results with established performance goals. ("Performance Measurement Challenges and Strategies," June 18, 2003, white paper associated with the Office of Management and Budget's Program Assessment Rating Tool (PART); and "Government Performance and Results Modernization Act of 2010," Section 4, Performance Reporting Amendments.)

25. Has your agency's records management program identified performance measures for records management activities such as training, records scheduling, permanent records transfers, etc.?

*Examples of performance measures include but are not limited to:

- Percentage of agency employees that receive records management training in a year
- A reduction in the volume of inactive records stored in office space
- Percentage of eligible permanent records transferred to NARA in a year
- Percentage of records scheduled
- Percentage of offices evaluated/inspected for records management compliance
- Percentage of email management auto-classification rates
- Development of new records management training modules
- Audits of internal systems
- Annual updates of file plans
- Performance testing for email applications to ensure records are captured
- Percentage of records successfully retrieved by Agency FOIA Officer in response to FOIA requests

☐ Yes
☐ No
☐ Pending final approval
☐ Currently under development
☐ Do not know

26. Does your agency's records management program have **documented and approved** policies and procedures that instruct staff on how your agency's permanent records in all formats must be managed and stored? (36 CFR 1222.34(e))

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

27. Is your agency subject to laws or regulations that require you to conduct business using paper or analog records?*

*Components of departmental agencies may answer "Yes" if this is handled by the department. Department Records Officers may answer "Yes" if this is handled at the component level.

☐ Yes
☐ No
☐ Do not know

28. If Yes: Which of the following possible examples of requirements for paper or analog records apply to your agency's needs? (Choose all that apply)

☐ Wet signatures are required for transactions with non-Federal entities (including the public)
☐ Wet signatures are required for transactions between Federal agencies
☐ Transactions are required to be conducted using paper / hard copy
☐ Agency is required to offer paper / hard copy as an available option for transactions
☐ Other, please be specific:
☐ Do not know
☐ Comments: (Optional)

Vital records* (also known as Essential Records) are records needed to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records). (36 CFR 1223.2)

***pending updates to regulations, the Records Management Self-Assessment still uses this terminology**

A program area is responsible for mission-related activities. An administrative area is responsible for activities not specific to the mission of the agency. (36 CFR 1220.34(d))

29. Has your agency identified the vital records of all its program and administrative areas? (36 CFR 1223.16)

*Components of departmental agencies may answer "Yes" if this is handled by the department.

☐ Yes
☐ No
☐ Do not know

30. How often does your agency review and update its vital records inventory? (36 CFR 1223.14)

☐ Annually

☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Never
☐ Do not know

31. Is your vital records plan part of the Continuity of Operations (COOP) plan?

☐ Yes
☐ No
☐ Do not know

32. Does your agency have policies in place to protect records and information from internal and external risks?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

Agencies are required to have a Freedom of Information Act (FOIA) program (5 U.S.C. 552). The ability to find records is essential for a successful FOIA program. The following questions related to your agency's FOIA program may require consultation with your agency's FOIA Officer.

33. The Agency Records Officer and the FOIA Officer:

34. Are the Agency Records Officer and the FOIA Officer in the same office/division within your agency?

35. Records needed to respond to a FOIA request are readily accessible and located by staff responsible for FOIA:

36. Staff responsible for FOIA can search for records without contacting others (i.e. program offices):

37. At what point in the FOIA process does your agency inform requesters of the Office of Government Information Services' (OGIS) dispute resolution services? (Choose all that apply)

38. What mode does your agency most often use to release records under FOIA?

39. In 2015, NARA and the Federal Records Management Council introduced the *Federal RIM Program Maturity Model*. Are you familiar with this or other maturity models?

☐ Yes
☐ No
☐ Comments: (Optional)

40. If Yes: Are you using the *Federal RIM Program Maturity Model* or other maturity models to measure the maturity of the records management program?

☐ Yes
☐ No
☐ Comments: (Optional)

41. Does your agency use your Records Management Self-Assessment scores to measure the effectiveness of the records management program?

☐ Yes
☐ No
☐ Do not know
☐ Comments (Optional): Please include in your comments how you use the Records Management Self-Assessment.

42. Please add any additional comments about your agency for Section II: Oversight and Compliance. (Optional)

Section III: Records Management Program - Records Disposition

Records disposition refers to actions taken with regard to Federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure. Disposition is a comprehensive term that includes both destruction and transfer of Federal records to the National Archives of the United States. (36 CFR Parts 1222, 1224, 1225 and 1226)

The next series of questions relate to your agency's efforts to schedule its records.

43. Are records and information in your agency managed throughout the lifecycle [creation/capture, classification, maintenance, retention, and disposition] by being properly identified, classified using a taxonomy, inventoried, and scheduled? (36 CFR 1222.34, 36 CFR 1224.10, and 36 CFR 1225.12)

☐ Yes
☐ No
☐ To some extent
☐ Do not know

44. Are records and information in your agency easily retrievable and accessible when needed for agency business? (36 CFR 1220.32(c))

☐ Yes, all records are easily retrievable and accessible when needed

☐ Most records can be retrieved and accessed in a timely manner
☐ Some records can be retrieved and accessed in a timely manner
☐ No
☐ Do not know

45. Does your agency disseminate *every* approved disposition authority (including newly approved records schedules and General Records Schedule items) to agency staff within six months of approval? (36 CFR 1226.12(a))

☐ Yes
☐ No
☐ Do not know

46. If Yes: What method(s) does your agency use? (Choose all that apply)

☐ Post to internal website or other shared information location
☐ Memorandum or email notification
☐ Update training materials
☐ Update records management policies and/or handbooks
☐ Other, please explain

47. Does your agency have a method of continually identifying new and unscheduled records?

☐ Yes
☐ No
☐ Do not know

48. If Yes: Which method(s) does your agency use? (Choose all that apply)

☐ Regular surveys
☐ Regular inventories
☐ Records management evaluations, site assessments, or audits of program offices
☐ Work with program managers to identify new programs and related records
☐ Work with Privacy Officer and review SORNs (Systems of Records Notices)
☐ Work with FOIA Officer
☐ Records Liaison Officers notify Agency Records Officer of new record series
☐ Require use and annual update of file plans
☐ Participate in design and retirement of information systems and note changes in records
☐ Outreach and awareness
☐ Other, please explain

The next series of questions relate to permanent records.

49. Does your agency have permanent records that are 30 years old or older that are located in agency office space, agency-operated records centers and/or commercial records centers? (36 CFR 1235.12(b) and M-12-18)

☐ Yes
☐ No
☐ Do not know

50. Are you aware of the requirement to formally request permission from NARA to retain permanent records beyond that specified in your agency's NARA-approved records schedules as outlined in 36 CFR 1235.14 and 1235.16?

☐ Yes
☐ No

51. Did your agency transfer permanent non-electronic records to NARA during FY 2017? (36 CFR 1235.12)

☐ Yes
☐ No
☐ No - No records were eligible for transfer during FY 2017
☐ No - New agency, records are not yet old enough to transfer
☐ No - My agency does not have any permanent non-electronic records
☐ Do not know
☐ Other, please explain

52. Did your agency transfer permanent electronic records to NARA during FY 2017? (36 CFR 1235.12)

☐ Yes
☐ No
☐ No - No electronic records/systems were eligible for transfer during FY 2017
☐ No - New agency, electronic records/systems are not old enough to transfer
☐ No - My agency does not have any permanent electronic records
☐ Do not know
☐ Other, please explain

53. Does your agency track when its permanent records (regardless of format) are due to be transferred to NARA?

☐ Yes
☐ No
☐ Do not know

☐ Not applicable, please explain

54. If Yes: What method(s) does your agency use to track its permanent records? (Choose all that apply)

☐ Rely on Federal Records Center notifications
☐ Maintain an inventory
☐ Database or other automated tracking
☐ Manual tracking
☐ Other, please explain

The next series of questions relate to your agency's handling of records for senior officials.

Senior officials are the heads of departments and independent agencies; their deputies and assistants; the heads of program offices and staff offices including assistant secretaries, administrators, and commissioners; directors of offices, bureaus, or equivalent; principal regional officials; staff assistants to those aforementioned officials, such as special assistants, confidential assistants, and administrative assistants; and career Federal employees, political appointees, and officers of the Armed Forces serving in equivalent or comparable positions.

55. Does your agency conduct and document for accountability purposes training and/or other briefings as part of the on-boarding process for senior officials on their records management roles and responsibilities, including the appropriate disposition of records and the use of personal and unofficial email accounts? (36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b))

☐ Yes
☐ Yes, but not documented
☐ No
☐ Do not know
☐ Not applicable, please explain

56. If Yes or Yes, but not documented: Is the Agency Records Officer and/or Senior Agency Official for Records Management involved in on-boarding briefings or other processes for newly appointed senior officials?

☐ Yes
☐ No
☐ Do not know

57. Does your agency conduct and document for accountability purposes exit briefings for departing senior officials on the appropriate disposition of the records, including email, under their immediate control? (36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b))

☐ Yes
☐ Yes, but not documented
☐ No
☐ Do not know
☐ Not applicable, please explain

58. If Yes or Yes, but not documented: Is the Agency Records Officer and/or Senior Agency Official for Records Management involved in exit briefings or other exit clearance processes for departing senior officials?

☐ Yes
☐ No
☐ Do not know

59. If Yes or Yes, but not documented: Does the exit or separation process for departing senior officials include records management program staff or other designated official(s) reviewing and approving the removal of personal papers and copies of records by those senior officials? (36 CFR 1222.24(a)(6))

☐ Yes
☐ No, please explain
☐ Do not know

The next series of questions relate to where your agency stores its inactive temporary and/or permanent records, regardless of format.

Commercial records storage facilities are private sector commercial facilities that offer records storage, retrieval, and disposition services.

An agency records center is a records storage facility, operated by a Federal agency and capable of storing more than 25,000 cubic feet of records.

Records staging or holding areas are areas designated within the agency's office space that are used for the temporary storage of records. The term does not include off-site storage such as commercial or agency records storage facilities. Records staging or holding areas may be established by an agency for maintaining records no longer needed in office space but whose volume or retention periods are insufficient to warrant transfer to a records center before final disposition.

60. Does your agency store inactive temporary and/or permanent records in a commercial records storage facility?

☐ Yes
☐ No

☐ Do not know

61. If Yes: Does the facility comply with the standards prescribed by 36 CFR 1234?

☐ Yes
☐ No
☐ Do not know

62. Does your agency store inactive temporary and/or permanent records in an agency records center? (Note: This does NOT include agency staging areas and temporary holding areas.)

☐ Yes
☐ No
☐ Do not know

63. If Yes: Does the records center comply with the standards prescribed by 36 CFR 1234?

☐ Yes
☐ No
☐ Do not know

64. Does your agency store inactive temporary and/or permanent records in an agency records staging or holding area?

☐ Yes
☐ No
☐ Do not know

65. If Yes: Does the staging or holding area(s) comply with the standards prescribed by 36 CFR 1234.10, 36 CFR 1234.12, and 36 CFR 1234.14?*

*It is not required but encouraged that staging or holding areas comply with 36 CFR 1234.

☐ Yes
☐ No
☐ Do not know

66. If Yes to Q60, 62, or 64: Please estimate the volume of inactive temporary records, in cubic feet, that your agency is storing in a non-NARA storage facility. (A cubic foot is equivalent to one records storage box.)

☐ 0 - 1,000
☐ 1,000 - 5,000

☐ 5,000 - 15,000
☐ 15,000 - 25,000
☐ 25,000 - 50,000
☐ 50,000 - 100,000
☐ 100,000 - 250,000
☐ 250,000 or greater

67. If Yes to Q60, 62, or 64: Please estimate the volume of inactive permanent records, in cubic feet, that your agency is storing in a non-NARA storage facility. (A cubic foot is equivalent to one records storage box.)

☐ 0 - 1,000
☐ 1,000 - 5,000
☐ 5,000 - 15,000
☐ 15,000 - 25,000
☐ 25,000 - 50,000
☐ 50,000 - 100,000
☐ 100,000 - 250,000
☐ 250,000 or greater

NARA annually provides agencies storing records in a Federal Records Center with transfer requests populated in the Electronic Records Archives (ERA) for permanent records eligible for transfer to the National Archives. (This is known as the Annual Move.) Agencies are then responsible to submit those transfer requests based on these lists in order to complete the cycle.

68. Did your agency receive a list of permanent records eligible for transfer in FY 2017?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, my agency does not store records in the Federal Records Centers

69. If Yes: Did your agency submit transfer requests in FY 2017 based on the Annual Move list of eligible permanent records to be accessioned by the National Archives?

☐ Yes
☐ No, please explain
☐ Do not know

70. Please add any additional comments about your agency for Section III: Records Disposition. (Optional)

Section IV: Records Management Program - Electronic Records

Electronic information system means an information system that contains and provides access to computerized Federal records and other information. (36 CFR 1236.2)

The following types of records management controls are needed to ensure that Federal records in electronic information systems can provide adequate and proper documentation of agency business for as long as the information is needed. Agencies must incorporate controls into the electronic information system or integrate them into a recordkeeping system that is external to the information system itself. (36 CFR 1236.10)

(a) Reliability: Controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

(b) Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

(c) Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.

(d) Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

(e) Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.

(f) Context: Mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity.

(g) Structure: Controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

71. Has your agency incorporated and/or integrated internal controls to ensure the reliability, authenticity, integrity, and usability of agency electronic records maintained in electronic information systems? (36 CFR 1236.10)

☐ Yes
☐ To some extent
☐ No
☐ Do not know
☐ Not applicable, please explain

Migration is a set of organized tasks designed to achieve periodic transfer of digital materials from one hardware/software configuration to another, or from one generation of computer technology to a subsequent generation.

Metadata consists of preserved contextual information describing the history, tracking, and/or management of an electronic document. (36 CFR 1236.2)

72. Does your agency have **documented and approved** procedures to enable the migration of records and associated metadata to new storage media or formats so that records are retrievable and usable as long as needed to conduct agency business and to meet NARA-approved dispositions? (36 CFR 1236.20(b)(6))

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

73. Are records management staff involved in developing procedures to ensure that records are properly migrated from retired systems? (36 CFR 1235.20(b)(6))

☐ Yes
☐ No
☐ To some extent
☐ Do not know
☐ Not applicable, please explain

74. Does your agency maintain an inventory of electronic information systems that indicates whether or not each system is covered by an approved NARA disposition authority? (36 CFR 1236.26(a))

☐ Yes
☐ No, please explain
☐ Do not know

75. Does your agency ensure that records management functionality, including the capture, retrieval, and retention of records according to agency business needs and NARA-approved records schedules, is incorporated into the design, development, and implementation of its electronic information systems? (36 CFR 1236.12)

*Components of departmental agencies may answer "Yes" if this is handled by the department.

☐ Yes
☐ No, please explain
☐ Do not know
☐ Not applicable, please explain

76. Does your agency's records management program staff participate in the design, development, and implementation of new electronic information systems?

☐ Yes
☐ No, please explain
☐ To some extent
☐ Do not know
☐ Not applicable, please explain

77**.** If Yes or To some extent: Which of these activities does your agency's records management program staff participate in to ensure that records requirements are part of the recommended solution? (Choose all that apply)

☐ Participate in review and acceptance of proposals for new systems
☐ Participate as stakeholder in requirements gathering
☐ Participate as stakeholder in design phase
☐ Participate as stakeholder in development phase including testing the system
☐ Provide sign off authority for the implementation of new systems
☐ Monitor system for adherence to standards, policies, and procedures
☐ Provide information only
☐ Do not know
☐ Other, please explain

78. Does your agency have documented and approved policies requiring permanent electronic records be managed in an electronic format for eventual transfer to NARA?

☐ Yes
☐ No
☐ No, under development
☐ Do not know

79. Does your agency have protections against unauthorized use, alteration, alienation or deletion of all electronic records?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

80. Does your agency have the capability to place legal holds on all electronic records until disposition is authorized?

☐ Yes

☐ No
☐ To some extent
☐ Do not know

Executive Order 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Under 32 CFR 2001.50, the Office of Information Security and Oversight provides further definition and guidance. (https://www.archives.gov/isoo/about)

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes in 32 CFR 2002 the way the executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. (https://www.archives.gov/cuiza/about)

81. Does your agency comply with the requirements under Executive Orders 13526 and 13556 for managing classified and controlled unclassified information in systems that contain electronic records?

☐ Yes
☐ No
☐ To some extent
☐ Do not know
☐ Not applicable, not an executive branch agency

82. Does your agency have the ability to search across all systems to find electronic records needed for agency business, FOIA and other information requests?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

83. Does your agency have a digitization strategy to reformat permanent records created in hard copy or other analog formats (e.g., microfiche, microfilm, analog video, and analog audio)?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

Web content is the textual, visual, or aural content that is encountered as part of the user experience on websites. It may include text, images, sounds, videos, animations, and more.

A Web Content Record is defined as information that meets the definition of Federal record and is provided via an agency's website.

84. Does your agency manage your web content as records?

☐ Yes
☐ No
☐ Do not know

85. If Yes: How does your agency capture web content managed as records? (Choose all that apply)

☐ Content is printed and filed
☐ Content is captured manually through periodic web snapshots
☐ Content is automatically harvested using specific tools
☐ Do not know
☐ Other, please explain

86. If Yes: Web content management includes: (Choose all that apply)

☐ Identification of record copy whether online or off-line
☐ Identifying the program office responsible for official record copy
☐ Records retention scheduling of web content
☐ Preservation of record copy in accordance with retention schedule
☐ Migration of content when website is updated
☐ Maintaining access throughout the life-cycle even if removed from the website
☐ Managing convenience copies as duplicates and applying disposition as needed
☐ Transfer of permanent web records to the National Archives
☐ Other, please explain

87. Does your agency use cloud services?

☐ Yes
☐ No
☐ Do not know

88. If Yes: For what purpose(s) is your agency using cloud services? (Choose all that apply)

☐ Email
☐ Administrative functions such as payroll, purchasing, and financial management
☐ Mission/program-related functions
☐ Other, please explain
☐ Do not know

89. If Yes: Are recordkeeping requirements included?

☐ Yes
☐ No
☐ Do not know

90. Is the records management program and related requirements included in your agency's Information Resource Management Plan or an equivalent information management plan? (OMB Circular A-130, Managing Information as a Strategic Resource)

☐ Yes
☐ No
☐ Do not know

The next series of questions relate to email.

An electronic mail system is a computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers, and word processing documents not transmitted on an email system. (36 CFR 1236.2)

91. Does your agency have **documented and approved** policies and procedures in place to handle email records that have a retention period longer than 180 days? (36 CFR 1236.22)

☐ Yes
☐ No, please explain
☐ Do not know

92. Does your agency have **documented and approved** policies and procedures to implement the guidelines for the transfer of permanent email records to NARA described in NARA Bulletin 2014-04: Revised Format Guidance for the Transfer of Permanent Electronic Records Appendix A: Tables of File Formats, Section 9 - Email? (36 CFR 1236.22(e))

☐ Yes
☐ No
☐ Do not know

Regardless of how many Federal email accounts individuals use to conduct official business, agencies must ensure that all accounts are managed, accessible and identifiable according to Federal recordkeeping requirements. (36 CFR 1236.22)

93. Do employees in your agency have more than one agency-administered email account? (NARA Bulletin 2013-03)

*Examples of business needs may include but are not limited to:

- Using separate accounts for public and internal correspondence
- Creating accounts for a specific agency initiative which may have multiple users
- Using separate accounts for classified information and unclassified information

☐ Yes
☐ No
☐ Do not know

94. Does your agency have **documented and approved** policies that address these types of accounts and that state that email records must be preserved in an appropriate agency recordkeeping system? (36 CFR 1236.22)

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

95. Does your agency allow the use of personal email accounts to conduct official business? (36 CFR 1236.22(b))

☐ Yes
☐ No
☐ Do not know

96. Does your agency have **documented and approved** policies that address the use of personal email accounts, whether or not allowed, that state that all emails created and received by such accounts must be preserved in an appropriate agency recordkeeping system and that a complete copy of all email records created and received by users of these accounts must be forwarded to an official electronic messaging account of the officer or employee no later than 20 days after the original creation or transmission of the record? (36 CFR 1236.22(b) and P.L. 113-187)

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

97. Does your agency's email system(s) retain the intelligent full names on directories or distribution lists to ensure identification of the sender and addressee(s) for those email messages that are Federal records? (36 CFR 1236.22(a)(3))

☐ Yes
☐ No
☐ Do not know

98. What method(s) does your agency employ to capture and manage email records? (Choose all that apply)

☐ Captured and stored in an email archiving system
☐ Captured and stored in an electronic records management system
☐ Captured and stored as personal storage table (.PST) files
☐ Print and file
☐ Not captured and email is managed by the end-user in the native system
☐ Other, please be specific

99. Does your agency evaluate, monitor, or audit staff compliance with the agency's email preservation policies? (36 CFR 1220.18)

☐ Yes
☐ No
☐ Do not know

100. If Yes: How often does your agency evaluate, monitor, or audit staff compliance with the agency's email preservation policies?

☐ Annually
☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Do not know

101. Which of the following has your agency chosen for retention scheduling of email?

☐ GRS 6.1: Email Managed under a Capstone Approach
☐ Agency-specific schedule
☐ Combination of agency-specific schedule and GRS 6.1
☐ Email retention has not been scheduled
☐ Do not know
☐ Other, please explain

102. Is your agency able to access email from departed employees in a usable format?

☐ Yes
☐ No

☐ To some extent
☐ Do not know

103. Is your agency able to prevent unauthorized access, modification, or destruction of emails?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

104. Can your agency transfer permanent email records to the National Archives in accordance with agency records schedules or General Records Schedules and NARA regulations and guidance?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

105. Is your agency able to decrypt permanent email records before they are accessioned by NARA?

☐ Yes
☐ No
☐ Do not know

106. Does your agency have an approved records schedule covering electronic messages including text messages, chat/instant messages, voice messages, and messages created in social media tools or applications that meet the definition of a Federal record?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

107. Does your agency have **documented and approved** policies and procedures in place to manage electronic messages including text messages, chat/instant messages, voice messages, and messages created in social media tools or applications?

☐ Yes
☐ No
☐ No, pending final approval

☐ No, under development
☐ Do not know
☐ Other, please explain

108. Please add any additional comments about your agency for Section IV: Electronic Records. (Optional)

Section V: Agency Demographics

109. Does the records management program have a dedicated budget?

☐ Yes
☐ No
☐ Do not know

110. Please report actual obligations for records management purposes incurred in FY 2017 for each of the following categories.

Personnel Compensation and Benefits (Federal employees only) for records management purposes:

$_____
☐ Do not know
☐ Prefer not to answer

Records Storage Contracts and Inter-Agency Agreements (paper and analog formats):

$_____
☐ Do not know
☐ Prefer not to answer

Records Management IT Systems and Electronic Records Storage:

$_____
☐ Do not know
☐ Prefer not to answer

Travel and Transportation for records management purposes:

$_____
☐ Do not know
☐ Prefer not to answer

Records Management Training:

$_____
☐ Do not know
☐ Prefer not to answer

Other: (Please be specific)

$_____

☐ Do not know

☐ Prefer not to answer

Comments: (Optional)

111. How many full-time equivalents (FTE) are in your agency/organization?

☐ 500,000 or more FTEs
☐ 100,000 499,999 FTEs
☐ 10,000 99,999 FTEs
☐ 1,000 9,999 FTEs
☐ 100 999 FTEs
☐ 1 99 FTEs
☐ Not Available

112. What other staff, offices, or program areas did you consult when you completed this self-assessment? (Choose all that apply)

☐ Senior Agency Official
☐ Office of the General Counsel
☐ Program Managers
☐ FOIA Officer
☐ Information Technology staff
☐ Records Liaison Officers or similar
☐ Administrative staff
☐ Other, please be specific:
☐ None

113. How much time did it take you to gather the information to complete this self-assessment?

☐ Under 3 hours
☐ More than 3 hours but less than 6 hours
☐ More than 6 hours but less than 10 hours
☐ Over 10 hours

114. Did your agency's senior management review and concur with your responses to the 2017 Records Management Self-Assessment?

☐ Yes
☐ No
☐ Do not know

115. Please provide your contact information.

Name:
Agency, Bureau, or Office:
Job Title:
Email Address:
Phone Number:

116. Are you the Agency Records Officer?

☐ Yes
☐ No

117. If No: Please provide the Agency Records Officer's contact information.

Name:
Email Address:
Phone Number:

118. Do you have any suggestions for improving the Records Management Self-Assessment next year?

NARA reserves the right to request additional documentation or a follow-up meeting to verify your responses. If you wish to provide supporting documentation for your answers or other information to NARA, please send it to rmselfassessment@nara.gov.

Thank you for completing the 2017 Records Management Self-Assessment! If you have any questions about the self-assessment, please send a message to rmselfassessment@nara.gov.

Dennis Morgan - NOAA Federal

From:	Dennis Morgan NOAA Federal
Sent:	Wednesday, March 7, 2018 10:50 AM
To:	Lola Stith NOAA Affiliate
Cc:	Graff Mark; Swisher Robert; Morgan Dennis
Subject:	Fwd: 2017 Records Management Assessment
Attachments:	2017 RMSA Questionnaire.docx

Lola: Please add this action and response to our data call tracking records. Thx. Dennis

Forwarded message
From: **Mark Graff - NOAA Federal** <mark.graff@noaa.gov>
Date: Wed, Mar 7, 2018 at 10:46 AM
Subject: Re: 2017 Records Management Assessment
To: Andre Sivels NOAA Federal <andre.sivels@noaa.gov>
Cc: Robert Swisher NOAA Federal <robert.swisher@noaa.gov>, Lola Stith NOAA Affiliate <lola.m.stith@noaa.gov>, Dennis Morgan NOAA Federal <dennis.morgan@noaa.gov>

Hi Andre

No problem. Here are NOAA FOIA's input for the portions of the RMSA Questionnaire.

Looping in Rob, Lola, and Dennis for data call tracking. We consider this data call complete.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Wed, Mar 7, 2018 at 10:15 AM, Andre Sivels NOAA Federal <andre.sivels@noaa.gov> wrote:

> Hi Mark
>
> I am in the process of review the questions for the NARA annual records management assessment and noticed they have 6 questions related to FOIA. Can you provide answers to questions 33 to 38 on the attached questionnaire and return to Monday March 12th, Thanks

Andre

Andre Sivels
NOAA Records Officer
U.S. Department of Commerce
1305 East West Highway Rm 7439
Silver Spring, MD 20910
Phone: 301628 0946
Fax: 301 713 1169

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)
2017 RECORDS MANAGEMENT SELF-ASSESSMENT

Welcome to the 2017 Records Management Self-Assessment!

Before you begin, please note the following information.

Except where indicated, the questions in this survey are intended to cover all records regardless of format, as defined in 44 U.S.C. 3301.

The questions apply regardless of whether your agency's work processes are conducted manually or electronically.

Unless otherwise indicated, the following questions refer to FY 2017 (October 1, 2016, through September 30, 2017).

Your answers to the self-assessment questions must be specific to records management activities in your agency. We have added a "not applicable" answer option to some questions. In general, use this option only if a question references an activity or action that is not conducted in your agency because of its size or if you are a Departmental Records Officer and are not responsible for the activity or action. In some cases, if the activity is being done by a departmental records management program, component agencies of that department may answer "Yes."

NOTE: Please note that your responses to questions in this assessment may be subject to public release pursuant to FOIA. However, we will not release responses to questions that contain detailed descriptions of agency activities.

NARA reserves the right to follow up with agencies to obtain additional information and/or documentation that supports their answers to the questions in this self-assessment.

As in previous years we will be conducting a validation process. Your agency may be selected at random to provide additional documentation and/or take part in interviews to discuss your records management program activities.

If you have any questions about this self-assessment or need additional information to answer a question(s), please send an email message to rmselfassessment@nara.gov.

Section I: Records Management Program - Activities

The next series of questions relate to administration of the records management program.

1. Is there a person in your agency who is responsible for coordinating and overseeing the implementation of the records management program? (36 CFR 1220.34(a))

☐ Yes
☐ No
☐ Do not know

2. If Yes: Please provide the person's name, position title, and office.

3. If Yes: How long has this person been responsible for coordinating and overseeing the implementation of the records management program?

☐ 5 or more years
☐ 3 to 4 years
☐ 1 to 2 years
☐ Less than a year

4. Does your agency have a Senior Agency Official for Records Management (SAORM)? (If you are a component of a department, you may answer "Yes," even if this is not being done at the component level.)

☐ Yes
☐ No
☐ Do not know

5. If Yes: Does your Agency Records Officer meet regularly (four or more times a year) with the SAORM to discuss the agency records management program's goals?

☐ Yes
☐ No
☐ Do not know

6. Does your agency use the Records and Information Management Series, 0308, (job series) released by the Office of Personnel Management in 2015?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, my agency does not use the General Schedule (GS) job classification

7. Does your agency have a network of designated employees within each program and administrative area who are assigned records management responsibilities? These individuals are often called Records Liaison Officers (RLOs), though their titles may vary. (36 CFR 1220.34(d))

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency has less than 100 employees
☐ Not applicable, Departmental Records Officer - this is done at the component level

8. Of the following, please select the one that best describes your records management staff. This includes only those specifically assigned to the records management program.

☐ All records management staff are agency personnel
☐ All records management staff are contractors
☐ Records management staff includes both agency personnel and contractors

In general, an FTE is equivalent to one full-time employee who is assigned full-time to records management (2,080 hours per year). An employee who works part-time or is assigned records management as one of several unrelated responsibilities should be counted as a fraction of an FTE, representing the estimated number of hours worked on records management per year as a percentage of 2,080 hours.

9. How many FTE agency personnel (non-contractors) are specifically assigned records management responsibilities? (These are individuals directly responsible for records management program implementation, not contacts within mission areas with minimal records management duties.)*

*For Department Records Officers, please include only the staff at the Department level, not agency components, as component agency records officers will be answering for their agencies.

☐ <1
☐ 1
☐ 2 - 10
☐ 10 - 20
☐ More than 20
☐ Do not know
☐ Not available
☐ Not applicable, all records management staff are contractors

10. If your agency uses contractors, how many contractor FTE are specifically assigned records management responsibilities? (These are individuals directly responsible for records management program implementation, not general contacts within mission areas with minimal records management duties.)*

*For Department Records Officers, please include only the staff at the Department level, not agency components, as component agency records officers will be answering for their agencies.

☐ <1
☐ 1
☐ 2 - 10
☐ 10 - 20
☐ More than 20
☐ Do not know
☐ Not available
☐ Not applicable, all records management staff are agency personnel

The next series of questions relate to records management directives.

11. Does your agency have a documented and approved records management directive(s)? (36 CFR 1220.34(c))

☐ Yes
☐ No, pending final approval
☐ No, under development
☐ No
☐ Do not know

12. When was your agency's directive(s) last reviewed and/or revised to ensure it includes all new records management policy issuances and guidance?

☐ FY 2017 - present
☐ FY 2015 - 2016
☐ FY 2013 - 2014
☐ FY 2012 or earlier
☐ Do not know
☐ Not applicable, agency does not have a records management directive

The next series of questions relate to records management training.

Formal records management training is the communication of standardized information that improves the records management knowledge, skills, and/or awareness of agency employees. Training can be either in a classroom setting or distance-based (e.g., web-based training), but it *must:*

- **be regular (occurring more than just once);**
- **be repeatable and formal (all instructors must provide the same message, not in an ad hoc way); and**

- **communicate the agency's vision of records management.**

13. Does your agency have internal records management training*, based on agency policies and directives, for employees assigned records management responsibilities? (36 CFR 1220.34(f))

*Includes NARA's records management training workshops that were ***customized*** specifically for your agency or use of an ***agency-customized*** version of the Federal Records Officer Network (FRON) RM 101 course.

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know
☐ Not applicable, please explain

14. Has your agency developed mandatory internal, staff-wide, formal training*, based on agency policy and directives, covering records in all formats, including electronic communications such as email, text messages, chat, or other messaging platforms or apps, such as social media or mobile device applications, which helps agency employees and contractors fulfill their recordkeeping responsibilities?** (36 CFR 1220.34(f))

*Includes NARA's records management training workshops that were ***customized*** specifically for your agency or use of an ***agency-customized*** version of the Federal Records Officer Network (FRON) RM 101 course.

**Components of departmental agencies may answer "Yes" if this is handled by the department. Department Records Officers may answer "Yes" if this is handled at the component level.

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

Senior officials are the heads of departments and independent agencies; their deputies and assistants; the heads of program offices and staff offices including assistant secretaries, administrators, and commissioners; directors of offices, bureaus, or equivalent; principal regional officials; staff assistants to those aforementioned officials, such as special assistants, confidential assistants, and administrative assistants; and career Federal employees, political appointees, and officers of the Armed Forces serving in equivalent or comparable positions. (General Records Schedule (GRS) 6.1, item 010)

15. Does your agency require that all senior and appointed officials, including those incoming and newly promoted, receive training on the importance of appropriately managing records under their immediate control? (36 CFR 1220.34(f))

☐ Yes
☐ No
☐ Do not know

16. Is records management training included in the in-processing for new employees in your agency?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

17. Please add any additional comments about your agency for Section I: Activities. (Optional)

Section II: Records Management Program – Oversight and Compliance

Agency records management programs must provide for effective controls over the creation, maintenance, and use of records in the conduct of current business. (36 CFR 1220.30(c)(1))

Internal controls are integral components of an organization's management that provide reasonable assurance of the effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. ("Standards for Internal Control in the Federal Government" (GAO-14-704G), U.S. Government Accountability Office, September 2014.)

Internal controls are:

- **Geared to the achievement of objectives in one or more categories—operations, reporting, and compliance;**
- **Processes consisting of ongoing tasks and activities—a means to an end, not an end in itself;**
- **Carried out by people—not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to effect internal control;**
- **Able to provide reasonable assurance, but not absolute assurance, to an entity's senior management;**
- **Adaptable to the organization's entire structure—flexible in application for the entire entity or for a particular regional office, division, operating unit, or business process.**

Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews/audits of operating performance, security of assets (limited access to inventories or equipment), and segregation of duties (separate personnel with authority to authorize a transaction, process the transaction, and review the transaction). Monitoring the effectiveness of internal controls should occur in the normal course of business. Periodic assessments should be integrated as part of management's continuous monitoring of internal control, which should be ingrained in the agency's operations. ("2013 Internal Control - Integrated Framework," Committee of Sponsoring Organizations (COSO) Executive Summary, May 14, 2013; and OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016.)

18. In addition to your agency's established records management policies and records schedules, has your agency's records management program developed and implemented internal controls to ensure that all eligible, permanent agency records in all media are transferred to NARA according to approved records schedules? (36 CFR 1222.26(e))

> **These controls must be internal to your agency. Reliance on information from external agencies (e.g., NARA's Federal Records Centers) or other organizations should not be considered when responding to this question.

*Examples of records management internal controls include but are not limited to:

- Regular briefings and other meetings with records creators
- Monitoring and testing of file plans
- Regular review of records inventories
- Internal tracking database of permanent record authorities and dates

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

19. In addition to your agency's established policies and records schedules, has your agency developed and implemented internal controls to ensure that Federal records are not destroyed before the end of their retention period? (36 CFR 1222.26(e))

> **These controls must be internal to your agency. Reliance on information from external agencies (e.g., NARA's Federal Records Centers) or other organizations should not be considered when responding to this question.

*Examples of records management internal controls include but are not limited to:

- Regular review of records inventories
- Approval process for disposal notices from off-site storage

- Require certificates of destruction
- Monitoring shredding services
- Performance testing for email
- Monitoring and testing of file plans
- Pre-authorization from records management program before records are destroyed
- Ad hoc monitoring of trash and recycle bins
- Notification from facilities staff when large trash bins or removal of boxes are requested
- Annual records clean-out activities sponsored and monitored by records management staff

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

An evaluation is an inspection, audit, or review of one or more records management programs for effectiveness and for compliance with applicable laws and regulations. An evaluation contains recommendations for correcting or improving records management practices, policies, and procedures as well as follow-up activities, including reporting on and implementing recommendations. Evaluations may be comprehensive (agency-wide) or specific to a program area or organizational unit. (36 CFR 1220.18)

20. Does your agency evaluate, by conducting inspections/audits/reviews, its records management program to ensure that it is efficient, effective, and compliant with all applicable records management laws and regulations?

> ******For this question, your agency's records management program, or a major component of the program (e.g., vital records identification and management, the records disposition process, records management training, or the management of your agency's electronic records) must be the primary focus of the inspection/audit/review.

☐ Yes, evaluations are conducted by the Records Management Program
☐ Yes, evaluations are conducted by the Office of Inspector General
☐ Yes, evaluations are conducted by the Records Management Program AND the Office of Inspector General
☐ Yes, evaluations are conducted by: (fill in the blank)
☐ No, please explain
☐ Do not know

21. How often is your records management program, or a major component of your program, evaluated for compliance with agency records management policies and procedures?

☐ Annually

☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

22. Was a formal written report prepared as part of the most recent inspection/audit/review?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

23**.** Do your agency's evaluation procedures include creating plans of corrective action that are monitored for implementation?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, agency does not evaluate its records management program

An essential control for any records management program is the establishment of performance goals and associated performance targets and performance measures.

Performance goals are the target levels of performance. Performance goals should be specific, measurable, attainable, results-oriented, and time-bound.

24. Has your agency established performance goals for its records management program?

*Examples of performance goals include but are not limited to:

- Identifying and scheduling all paper and non-electronic records by the end of FY 2017
- Developing computer-based records management training modules by the end of FY 2017
- Planning and piloting an electronic records management solution for email by the end of FY 2018
- Updating records management policies by the end of the year
- Conducting records management evaluations of at least one program area each quarter

☐ Yes
☐ No
☐ Pending final approval
☐ Currently under development
☐ Do not know

Performance measures are the indicators or metrics against which a program's performance can be gauged. Performance measures should provide a basis for comparing actual results with established performance goals. ("Performance Measurement Challenges and Strategies," June 18, 2003, white paper associated with the Office of Management and Budget's Program Assessment Rating Tool (PART); and "Government Performance and Results Modernization Act of 2010," Section 4, Performance Reporting Amendments.)

25. Has your agency's records management program identified performance measures for records management activities such as training, records scheduling, permanent records transfers, etc.?

*Examples of performance measures include but are not limited to:

- Percentage of agency employees that receive records management training in a year
- A reduction in the volume of inactive records stored in office space
- Percentage of eligible permanent records transferred to NARA in a year
- Percentage of records scheduled
- Percentage of offices evaluated/inspected for records management compliance
- Percentage of email management auto-classification rates
- Development of new records management training modules
- Audits of internal systems
- Annual updates of file plans
- Performance testing for email applications to ensure records are captured
- Percentage of records successfully retrieved by Agency FOIA Officer in response to FOIA requests

☐ Yes
☐ No
☐ Pending final approval
☐ Currently under development
☐ Do not know

26. Does your agency's records management program have **documented and approved** policies and procedures that instruct staff on how your agency's permanent records in all formats must be managed and stored? (36 CFR 1222.34(e))

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

27. Is your agency subject to laws or regulations that require you to conduct business using paper or analog records?*

*Components of departmental agencies may answer "Yes" if this is handled by the department. Department Records Officers may answer "Yes" if this is handled at the component level.

☐ Yes
☐ No
☐ Do not know

28. If Yes: Which of the following possible examples of requirements for paper or analog records apply to your agency's needs? (Choose all that apply)

☐ Wet signatures are required for transactions with non-Federal entities (including the public)
☐ Wet signatures are required for transactions between Federal agencies
☐ Transactions are required to be conducted using paper / hard copy
☐ Agency is required to offer paper / hard copy as an available option for transactions
☐ Other, please be specific:
☐ Do not know
☐ Comments: (Optional)

Vital records* (also known as Essential Records) are records needed to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records). (36 CFR 1223.2)

***pending updates to regulations, the Records Management Self-Assessment still uses this terminology**

A program area is responsible for mission-related activities. An administrative area is responsible for activities not specific to the mission of the agency. (36 CFR 1220.34(d))

29. Has your agency identified the vital records of all its program and administrative areas? (36 CFR 1223.16)

*Components of departmental agencies may answer "Yes" if this is handled by the department.

☐ Yes
☐ No
☐ Do not know

30. How often does your agency review and update its vital records inventory? (36 CFR 1223.14)

☐ Annually

☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Never
☐ Do not know

31. Is your vital records plan part of the Continuity of Operations (COOP) plan?

☐ Yes
☐ No
☐ Do not know

32. Does your agency have policies in place to protect records and information from internal and external risks?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

Agencies are required to have a Freedom of Information Act (FOIA) program (5 U.S.C. 552). The ability to find records is essential for a successful FOIA program. The following questions related to your agency's FOIA program may require consultation with your agency's FOIA Officer.

33. The Agency Records Officer and the FOIA Officer:

34. Are the Agency Records Officer and the FOIA Officer in the same office/division within your agency?

35. Records needed to respond to a FOIA request are readily accessible and located by staff responsible for FOIA:

36. Staff responsible for FOIA can search for records without contacting others (i.e. program offices):

37. At what point in the FOIA process does your agency inform requesters of the Office of Government Information Services' (OGIS) dispute resolution services? (Choose all that apply)

38. What mode does your agency most often use to release records under FOIA?

39. In 2015, NARA and the Federal Records Management Council introduced the *Federal RIM Program Maturity Model*. Are you familiar with this or other maturity models?

☐ Yes
☐ No
☐ Comments: (Optional)

40. If Yes: Are you using the *Federal RIM Program Maturity Model* or other maturity models to measure the maturity of the records management program?

☐ Yes
☐ No
☐ Comments: (Optional)

41. Does your agency use your Records Management Self-Assessment scores to measure the effectiveness of the records management program?

☐ Yes
☐ No
☐ Do not know
☐ Comments (Optional): Please include in your comments how you use the Records Management Self-Assessment.

42. Please add any additional comments about your agency for Section II: Oversight and Compliance. (Optional)

Section III: Records Management Program - Records Disposition

Records disposition refers to actions taken with regard to Federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure. Disposition is a comprehensive term that includes both destruction and transfer of Federal records to the National Archives of the United States. (36 CFR Parts 1222, 1224, 1225 and 1226)

The next series of questions relate to your agency's efforts to schedule its records.

43. Are records and information in your agency managed throughout the lifecycle [creation/capture, classification, maintenance, retention, and disposition] by being properly identified, classified using a taxonomy, inventoried, and scheduled? (36 CFR 1222.34, 36 CFR 1224.10, and 36 CFR 1225.12)

☐ Yes
☐ No
☐ To some extent
☐ Do not know

44. Are records and information in your agency easily retrievable and accessible when needed for agency business? (36 CFR 1220.32(c))

☐ Yes, all records are easily retrievable and accessible when needed

☐ Most records can be retrieved and accessed in a timely manner
☐ Some records can be retrieved and accessed in a timely manner
☐ No
☐ Do not know

45. Does your agency disseminate *every* approved disposition authority (including newly approved records schedules and General Records Schedule items) to agency staff within six months of approval? (36 CFR 1226.12(a))

☐ Yes
☐ No
☐ Do not know

46. If Yes: What method(s) does your agency use? (Choose all that apply)

☐ Post to internal website or other shared information location
☐ Memorandum or email notification
☐ Update training materials
☐ Update records management policies and/or handbooks
☐ Other, please explain

47. Does your agency have a method of continually identifying new and unscheduled records?

☐ Yes
☐ No
☐ Do not know

48. If Yes: Which method(s) does your agency use? (Choose all that apply)

☐ Regular surveys
☐ Regular inventories
☐ Records management evaluations, site assessments, or audits of program offices
☐ Work with program managers to identify new programs and related records
☐ Work with Privacy Officer and review SORNs (Systems of Records Notices)
☐ Work with FOIA Officer
☐ Records Liaison Officers notify Agency Records Officer of new record series
☐ Require use and annual update of file plans
☐ Participate in design and retirement of information systems and note changes in records
☐ Outreach and awareness
☐ Other, please explain

The next series of questions relate to permanent records.

49. Does your agency have permanent records that are 30 years old or older that are located in agency office space, agency-operated records centers and/or commercial records centers? (36 CFR 1235.12(b) and M-12-18)

☐ Yes
☐ No
☐ Do not know

50. Are you aware of the requirement to formally request permission from NARA to retain permanent records beyond that specified in your agency's NARA-approved records schedules as outlined in 36 CFR 1235.14 and 1235.16?

☐ Yes
☐ No

51. Did your agency transfer permanent non-electronic records to NARA during FY 2017? (36 CFR 1235.12)

☐ Yes
☐ No
☐ No - No records were eligible for transfer during FY 2017
☐ No - New agency, records are not yet old enough to transfer
☐ No - My agency does not have any permanent non-electronic records
☐ Do not know
☐ Other, please explain

52. Did your agency transfer permanent electronic records to NARA during FY 2017? (36 CFR 1235.12)

☐ Yes
☐ No
☐ No - No electronic records/systems were eligible for transfer during FY 2017
☐ No - New agency, electronic records/systems are not old enough to transfer
☐ No - My agency does not have any permanent electronic records
☐ Do not know
☐ Other, please explain

53. Does your agency track when its permanent records (regardless of format) are due to be transferred to NARA?

☐ Yes
☐ No
☐ Do not know

☐ Not applicable, please explain

54. If Yes: What method(s) does your agency use to track its permanent records? (Choose all that apply)

☐ Rely on Federal Records Center notifications
☐ Maintain an inventory
☐ Database or other automated tracking
☐ Manual tracking
☐ Other, please explain

The next series of questions relate to your agency's handling of records for senior officials.

Senior officials are the heads of departments and independent agencies; their deputies and assistants; the heads of program offices and staff offices including assistant secretaries, administrators, and commissioners; directors of offices, bureaus, or equivalent; principal regional officials; staff assistants to those aforementioned officials, such as special assistants, confidential assistants, and administrative assistants; and career Federal employees, political appointees, and officers of the Armed Forces serving in equivalent or comparable positions.

55. Does your agency conduct and document for accountability purposes training and/or other briefings as part of the on-boarding process for senior officials on their records management roles and responsibilities, including the appropriate disposition of records and the use of personal and unofficial email accounts? (36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b))

☐ Yes
☐ Yes, but not documented
☐ No
☐ Do not know
☐ Not applicable, please explain

56. If Yes or Yes, but not documented: Is the Agency Records Officer and/or Senior Agency Official for Records Management involved in on-boarding briefings or other processes for newly appointed senior officials?

☐ Yes
☐ No
☐ Do not know

57. Does your agency conduct and document for accountability purposes exit briefings for departing senior officials on the appropriate disposition of the records, including email, under their immediate control? (36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b))

☐ Yes
☐ Yes, but not documented
☐ No
☐ Do not know
☐ Not applicable, please explain

58. If Yes or Yes, but not documented: Is the Agency Records Officer and/or Senior Agency Official for Records Management involved in exit briefings or other exit clearance processes for departing senior officials?

☐ Yes
☐ No
☐ Do not know

59. If Yes or Yes, but not documented: Does the exit or separation process for departing senior officials include records management program staff or other designated official(s) reviewing and approving the removal of personal papers and copies of records by those senior officials? (36 CFR 1222.24(a)(6))

☐ Yes
☐ No, please explain
☐ Do not know

The next series of questions relate to where your agency stores its inactive temporary and/or permanent records, regardless of format.

Commercial records storage facilities are private sector commercial facilities that offer records storage, retrieval, and disposition services.

An agency records center is a records storage facility, operated by a Federal agency and capable of storing more than 25,000 cubic feet of records.

Records staging or holding areas are areas designated within the agency's office space that are used for the temporary storage of records. The term does not include off-site storage such as commercial or agency records storage facilities. Records staging or holding areas may be established by an agency for maintaining records no longer needed in office space but whose volume or retention periods are insufficient to warrant transfer to a records center before final disposition.

60. Does your agency store inactive temporary and/or permanent records in a commercial records storage facility?

☐ Yes
☐ No

☐ Do not know

61. If Yes: Does the facility comply with the standards prescribed by 36 CFR 1234?

☐ Yes
☐ No
☐ Do not know

62. Does your agency store inactive temporary and/or permanent records in an agency records center? (Note: This does NOT include agency staging areas and temporary holding areas.)

☐ Yes
☐ No
☐ Do not know

63. If Yes: Does the records center comply with the standards prescribed by 36 CFR 1234?

☐ Yes
☐ No
☐ Do not know

64. Does your agency store inactive temporary and/or permanent records in an agency records staging or holding area?

☐ Yes
☐ No
☐ Do not know

65. If Yes: Does the staging or holding area(s) comply with the standards prescribed by 36 CFR 1234.10, 36 CFR 1234.12, and 36 CFR 1234.14?*

*It is not required but encouraged that staging or holding areas comply with 36 CFR 1234.

☐ Yes
☐ No
☐ Do not know

66. If Yes to Q60, 62, or 64: Please estimate the volume of inactive temporary records, in cubic feet, that your agency is storing in a non-NARA storage facility. (A cubic foot is equivalent to one records storage box.)

☐ 0 - 1,000
☐ 1,000 - 5,000

☐ 5,000 - 15,000
☐ 15,000 - 25,000
☐ 25,000 - 50,000
☐ 50,000 - 100,000
☐ 100,000 - 250,000
☐ 250,000 or greater

67. If Yes to Q60, 62, or 64: Please estimate the volume of inactive permanent records, in cubic feet, that your agency is storing in a non-NARA storage facility. (A cubic foot is equivalent to one records storage box.)

☐ 0 - 1,000
☐ 1,000 - 5,000
☐ 5,000 - 15,000
☐ 15,000 - 25,000
☐ 25,000 - 50,000
☐ 50,000 - 100,000
☐ 100,000 - 250,000
☐ 250,000 or greater

NARA annually provides agencies storing records in a Federal Records Center with transfer requests populated in the Electronic Records Archives (ERA) for permanent records eligible for transfer to the National Archives. (This is known as the Annual Move.) Agencies are then responsible to submit those transfer requests based on these lists in order to complete the cycle.

68. Did your agency receive a list of permanent records eligible for transfer in FY 2017?

☐ Yes
☐ No
☐ Do not know
☐ Not applicable, my agency does not store records in the Federal Records Centers

69. If Yes: Did your agency submit transfer requests in FY 2017 based on the Annual Move list of eligible permanent records to be accessioned by the National Archives?

☐ Yes
☐ No, please explain
☐ Do not know

70. Please add any additional comments about your agency for Section III: Records Disposition. (Optional)

Section IV: Records Management Program - Electronic Records

Electronic information system means an information system that contains and provides access to computerized Federal records and other information. (36 CFR 1236.2)

The following types of records management controls are needed to ensure that Federal records in electronic information systems can provide adequate and proper documentation of agency business for as long as the information is needed. Agencies must incorporate controls into the electronic information system or integrate them into a recordkeeping system that is external to the information system itself. (36 CFR 1236.10)

(a) Reliability: Controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

(b) Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

(c) Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.

(d) Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

(e) Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.

(f) Context: Mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity.

(g) Structure: Controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

71. Has your agency incorporated and/or integrated internal controls to ensure the reliability, authenticity, integrity, and usability of agency electronic records maintained in electronic information systems? (36 CFR 1236.10)

☐ Yes
☐ To some extent
☐ No
☐ Do not know
☐ Not applicable, please explain

Migration is a set of organized tasks designed to achieve periodic transfer of digital materials from one hardware/software configuration to another, or from one generation of computer technology to a subsequent generation.

Metadata consists of preserved contextual information describing the history, tracking, and/or management of an electronic document. (36 CFR 1236.2)

72. Does your agency have **documented and approved** procedures to enable the migration of records and associated metadata to new storage media or formats so that records are retrievable and usable as long as needed to conduct agency business and to meet NARA-approved dispositions? (36 CFR 1236.20(b)(6))

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

73. Are records management staff involved in developing procedures to ensure that records are properly migrated from retired systems? (36 CFR 1235.20(b)(6))

☐ Yes
☐ No
☐ To some extent
☐ Do not know
☐ Not applicable, please explain

74. Does your agency maintain an inventory of electronic information systems that indicates whether or not each system is covered by an approved NARA disposition authority? (36 CFR 1236.26(a))

☐ Yes
☐ No, please explain
☐ Do not know

75. Does your agency ensure that records management functionality, including the capture, retrieval, and retention of records according to agency business needs and NARA-approved records schedules, is incorporated into the design, development, and implementation of its electronic information systems? (36 CFR 1236.12)

*Components of departmental agencies may answer "Yes" if this is handled by the department.

☐ Yes
☐ No, please explain
☐ Do not know
☐ Not applicable, please explain

76. Does your agency's records management program staff participate in the design, development, and implementation of new electronic information systems?

☐ Yes
☐ No, please explain
☐ To some extent
☐ Do not know
☐ Not applicable, please explain

77**.** If Yes or To some extent: Which of these activities does your agency's records management program staff participate in to ensure that records requirements are part of the recommended solution? (Choose all that apply)

☐ Participate in review and acceptance of proposals for new systems
☐ Participate as stakeholder in requirements gathering
☐ Participate as stakeholder in design phase
☐ Participate as stakeholder in development phase including testing the system
☐ Provide sign off authority for the implementation of new systems
☐ Monitor system for adherence to standards, policies, and procedures
☐ Provide information only
☐ Do not know
☐ Other, please explain

78. Does your agency have documented and approved policies requiring permanent electronic records be managed in an electronic format for eventual transfer to NARA?

☐ Yes
☐ No
☐ No, under development
☐ Do not know

79. Does your agency have protections against unauthorized use, alteration, alienation or deletion of all electronic records?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

80. Does your agency have the capability to place legal holds on all electronic records until disposition is authorized?

☐ Yes

☐ No
☐ To some extent
☐ Do not know

Executive Order 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Under 32 CFR 2001.50, the Office of Information Security and Oversight provides further definition and guidance. (https://www.archives.gov/isoo/about)

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes in 32 CFR 2002 the way the executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. (https://www.archives.gov/cuiza/about)

81. Does your agency comply with the requirements under Executive Orders 13526 and 13556 for managing classified and controlled unclassified information in systems that contain electronic records?

☐ Yes
☐ No
☐ To some extent
☐ Do not know
☐ Not applicable, not an executive branch agency

82. Does your agency have the ability to search across all systems to find electronic records needed for agency business, FOIA and other information requests?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

83. Does your agency have a digitization strategy to reformat permanent records created in hard copy or other analog formats (e.g., microfiche, microfilm, analog video, and analog audio)?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

Web content is the textual, visual, or aural content that is encountered as part of the user experience on websites. It may include text, images, sounds, videos, animations, and more.

A Web Content Record is defined as information that meets the definition of Federal record and is provided via an agency's website.

84. Does your agency manage your web content as records?

☐ Yes
☐ No
☐ Do not know

85. If Yes: How does your agency capture web content managed as records? (Choose all that apply)

☐ Content is printed and filed
☐ Content is captured manually through periodic web snapshots
☐ Content is automatically harvested using specific tools
☐ Do not know
☐ Other, please explain

86. If Yes: Web content management includes: (Choose all that apply)

☐ Identification of record copy whether online or off-line
☐ Identifying the program office responsible for official record copy
☐ Records retention scheduling of web content
☐ Preservation of record copy in accordance with retention schedule
☐ Migration of content when website is updated
☐ Maintaining access throughout the life-cycle even if removed from the website
☐ Managing convenience copies as duplicates and applying disposition as needed
☐ Transfer of permanent web records to the National Archives
☐ Other, please explain

87. Does your agency use cloud services?

☐ Yes
☐ No
☐ Do not know

88. If Yes: For what purpose(s) is your agency using cloud services? (Choose all that apply)

☐ Email
☐ Administrative functions such as payroll, purchasing, and financial management
☐ Mission/program-related functions
☐ Other, please explain
☐ Do not know

89. If Yes: Are recordkeeping requirements included?

☐ Yes
☐ No
☐ Do not know

90. Is the records management program and related requirements included in your agency's Information Resource Management Plan or an equivalent information management plan? (OMB Circular A-130, Managing Information as a Strategic Resource)

☐ Yes
☐ No
☐ Do not know

The next series of questions relate to email.

An electronic mail system is a computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers, and word processing documents not transmitted on an email system. (36 CFR 1236.2)

91. Does your agency have **documented and approved** policies and procedures in place to handle email records that have a retention period longer than 180 days? (36 CFR 1236.22)

☐ Yes
☐ No, please explain
☐ Do not know

92. Does your agency have **documented and approved** policies and procedures to implement the guidelines for the transfer of permanent email records to NARA described in NARA Bulletin 2014-04: Revised Format Guidance for the Transfer of Permanent Electronic Records Appendix A: Tables of File Formats, Section 9 - Email? (36 CFR 1236.22(e))

☐ Yes
☐ No
☐ Do not know

Regardless of how many Federal email accounts individuals use to conduct official business, agencies must ensure that all accounts are managed, accessible and identifiable according to Federal recordkeeping requirements. (36 CFR 1236.22)

93. Do employees in your agency have more than one agency-administered email account? (NARA Bulletin 2013-03)

*Examples of business needs may include but are not limited to:

- Using separate accounts for public and internal correspondence
- Creating accounts for a specific agency initiative which may have multiple users
- Using separate accounts for classified information and unclassified information

☐ Yes
☐ No
☐ Do not know

94. Does your agency have **documented and approved** policies that address these types of accounts and that state that email records must be preserved in an appropriate agency recordkeeping system? (36 CFR 1236.22)

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

95. Does your agency allow the use of personal email accounts to conduct official business? (36 CFR 1236.22(b))

☐ Yes
☐ No
☐ Do not know

96. Does your agency have **documented and approved** policies that address the use of personal email accounts, whether or not allowed, that state that all emails created and received by such accounts must be preserved in an appropriate agency recordkeeping system and that a complete copy of all email records created and received by users of these accounts must be forwarded to an official electronic messaging account of the officer or employee no later than 20 days after the original creation or transmission of the record? (36 CFR 1236.22(b) and P.L. 113-187)

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

97. Does your agency's email system(s) retain the intelligent full names on directories or distribution lists to ensure identification of the sender and addressee(s) for those email messages that are Federal records? (36 CFR 1236.22(a)(3))

☐ Yes
☐ No
☐ Do not know

98. What method(s) does your agency employ to capture and manage email records? (Choose all that apply)

☐ Captured and stored in an email archiving system
☐ Captured and stored in an electronic records management system
☐ Captured and stored as personal storage table (.PST) files
☐ Print and file
☐ Not captured and email is managed by the end-user in the native system
☐ Other, please be specific

99. Does your agency evaluate, monitor, or audit staff compliance with the agency's email preservation policies? (36 CFR 1220.18)

☐ Yes
☐ No
☐ Do not know

100. If Yes: How often does your agency evaluate, monitor, or audit staff compliance with the agency's email preservation policies?

☐ Annually
☐ Bi-annually
☐ Once every 3 years
☐ Ad hoc
☐ Do not know

101. Which of the following has your agency chosen for retention scheduling of email?

☐ GRS 6.1: Email Managed under a Capstone Approach
☐ Agency-specific schedule
☐ Combination of agency-specific schedule and GRS 6.1
☐ Email retention has not been scheduled
☐ Do not know
☐ Other, please explain

102. Is your agency able to access email from departed employees in a usable format?

☐ Yes
☐ No

☐ To some extent
☐ Do not know

103. Is your agency able to prevent unauthorized access, modification, or destruction of emails?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

104. Can your agency transfer permanent email records to the National Archives in accordance with agency records schedules or General Records Schedules and NARA regulations and guidance?

☐ Yes
☐ No
☐ To some extent
☐ Do not know

105. Is your agency able to decrypt permanent email records before they are accessioned by NARA?

☐ Yes
☐ No
☐ Do not know

106. Does your agency have an approved records schedule covering electronic messages including text messages, chat/instant messages, voice messages, and messages created in social media tools or applications that meet the definition of a Federal record?

☐ Yes
☐ No
☐ No, pending final approval
☐ No, under development
☐ Do not know

107. Does your agency have **documented and approved** policies and procedures in place to manage electronic messages including text messages, chat/instant messages, voice messages, and messages created in social media tools or applications?

☐ Yes
☐ No
☐ No, pending final approval

☐ No, under development
☐ Do not know
☐ Other, please explain

108. Please add any additional comments about your agency for Section IV: Electronic Records. (Optional)

Section V: Agency Demographics

109. Does the records management program have a dedicated budget?

☐ Yes
☐ No
☐ Do not know

110. Please report actual obligations for records management purposes incurred in FY 2017 for each of the following categories.

Personnel Compensation and Benefits (Federal employees only) for records management purposes:

$_____
☐ Do not know
☐ Prefer not to answer

Records Storage Contracts and Inter-Agency Agreements (paper and analog formats):

$_____
☐ Do not know
☐ Prefer not to answer

Records Management IT Systems and Electronic Records Storage:

$_____
☐ Do not know
☐ Prefer not to answer

Travel and Transportation for records management purposes:

$_____
☐ Do not know
☐ Prefer not to answer

Records Management Training:

$_____
☐ Do not know
☐ Prefer not to answer

Other: (Please be specific)

$_____

☐ Do not know

☐ Prefer not to answer

Comments: (Optional)

111. How many full-time equivalents (FTE) are in your agency/organization?

☐ 500,000 or more FTEs
☐ 100,000 499,999 FTEs
☐ 10,000 99,999 FTEs
☐ 1,000 9,999 FTEs
☐ 100 999 FTEs
☐ 1 99 FTEs
☐ Not Available

112. What other staff, offices, or program areas did you consult when you completed this self-assessment? (Choose all that apply)

☐ Senior Agency Official
☐ Office of the General Counsel
☐ Program Managers
☐ FOIA Officer
☐ Information Technology staff
☐ Records Liaison Officers or similar
☐ Administrative staff
☐ Other, please be specific:
☐ None

113. How much time did it take you to gather the information to complete this self-assessment?

☐ Under 3 hours
☐ More than 3 hours but less than 6 hours
☐ More than 6 hours but less than 10 hours
☐ Over 10 hours

114. Did your agency's senior management review and concur with your responses to the 2017 Records Management Self-Assessment?

☐ Yes
☐ No
☐ Do not know

115. Please provide your contact information.

Name:
Agency, Bureau, or Office:
Job Title:
Email Address:
Phone Number:

116. Are you the Agency Records Officer?

☐ Yes
☐ No

117. If No: Please provide the Agency Records Officer's contact information.

Name:
Email Address:
Phone Number:

118. Do you have any suggestions for improving the Records Management Self-Assessment next year?

NARA reserves the right to request additional documentation or a follow-up meeting to verify your responses. If you wish to provide supporting documentation for your answers or other information to NARA, please send it to rmselfassessment@nara.gov.

Thank you for completing the 2017 Records Management Self-Assessment! If you have any questions about the self-assessment, please send a message to rmselfassessment@nara.gov.

Toland, Michael (Federal)

From:	Toland, Michael (Federal)
Sent:	Thursday, March 8, 2018 12:22 PM
To:	Agyekum, Grace; Arnold, Josephine (Federal); Bogomolny, Michael (Federal); Boston, Louis; Cheney, Stacy; Curry, Vernon E; Fletcher, Catherine; Gioffre, Kathy (Federal); Graff, Mark (Federal); Hitt, Lucas; Kelton, Cindy (Federal); Kong, Stephen (Federal); Kuo, Jennifer; Main, Laura; Moulder, Pamela (Federal); Oliphant, Tashima (Federal); Parsons, Bobbie (Federal); Piel, Jennifer; Pilot, Adrienne; Powers, Victor; Roberson, Jeffrey (Federal); Smith, Kathy; Staunton, Dondi; Stith, Lola (Contractor); Strickland, Wayne
Cc:	Boyd, Harriette (Federal); Crawford, Ayana (Contractor); Davis, James (Contractor); Gitelman, Steve (Contractor); Khalid, Sulma (Contractor)
Subject:	March 8 FOIA Training Presentations
Attachments:	Exemption 5 January 2018 (AAP).pptx; FOIA PA Interface Jan 2018 (AAP).pptx; Litigation Considerations January 2018 (AAP).pptx

Dear FOIA Officers and Contacts:

Please find attached the presentations from the March 8 FOIA training that was conducted by DOJ. While I plan to upload the slide decks to our web site, please feel free to distribute them to your FOIA professionals.

Additionally, I want to thank those of you who were able to attend the training, either in person or via WebEx. I hope that you found the information provided informative and useful.

Regards,

Mike

Michael J. Toland, Ph.D.
Deputy Chief FOIA Officer,
Departmental FOIA Public Liaison Officer,
Departmental Privacy Act Officer, and
Deputy Director FOIA/Privacy Act Operations
U.S. Department of Commerce
Office of Privacy and Open Government
Office: (202) 482-3842
Email: mtoland@doc.gov

UNITED STATES DEPARTMENT of JUSTICE

Exemption 5
The Civil Discovery Privileges

1

Exemption 5

Protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency."

Exemption 5

Incorporates civil discovery privileges into the FOIA.

Prevents requesters from using the FOIA to get documents that would be privileged in discovery.

Exemption 5

Two requirements:

1. Threshold

   and

2. Applicable discovery privilege

Exemption 5

Two requirements:

1. **Threshold**

   and

2. Applicable discovery privilege

Threshold

Basic Definition

- "Inter-agency or intra-agency memorandums or letters"
- This includes all forms of written document—emails, reports, etc.

Threshold

The "Consultant Corollary"

- The Exemption 5 threshold has been expanded to cover **certain** situations in which an agency receives documents from an outside party.

Consultant Corollary: Who is a Consultant?

Covers situations where outsiders are functioning as if they were agency employees.

- Those who have a formal, contractual, paid relationship with an agency
- Those consulted by the agency on an unpaid volunteer basis

8

Consultant Corollary: Who is a Consultant?

Dep't of the Interior v. Klamath Water Users Protective Ass'n

- An outsider cannot be a consultant when the outsider is:
  - Seeking a government benefit
  - At the expense of another party.

Miscellaneous Threshold Issues

Advice from a consultant must be coming into the agency, not from the agency.

Miscellaneous Threshold Issues

An agency can protect advice it receives from Congress.

An agency cannot protect advice it provides to Congress.

Miscellaneous Threshold Issues

Common Interest Doctrine:

- The outside party must have a common interest with the agency,
- After the point at which the agency decides to enter into a common interest agreement.

Miscellaneous Threshold Issues

Common Interest Doctrine:

- Documents created while the outside party is seeking the agreement itself will not meet the threshold.

Exemption 5

Two requirements:

1. Threshold

and

2. **Applicable discovery privilege**

Part II: Discovery Privileges

Exemption 5 incorporates certain civil discovery privileges into the FOIA.

Part II: Discovery Privileges

In practice, only three come up with any degree of regularity:

- Deliberative process privilege
- Attorney work-product privilege
- Attorney-client privilege.

The Deliberative Process Privilege

Purposes of the privilege:

- Encourage open, frank discussion
- Protect against premature disclosure of proposed policies
- Guard against public confusion from release of reasons and rationales that were not ultimately the basis for agency decisions

The Deliberative Process Privilege

Protects Process

- Integrity of agencies' decision-making processes.
- Documents protected where release would harm the decision-making process.

The Deliberative Process Privilege

Elements

Documents must be:

1. **Predecisional**

   and

2. Deliberative

The Deliberative Process Privilege

"Predecisional" Defined

- Antecedent to the adoption of an agency policy.

The Deliberative Process Privilege

Identifying Decisionmaking Processes

- Decisionmaking process that promoted the creation of the withheld documents.
- Final agency decision is not required.

The Deliberative Process Privilege

Eligible Information

- Documents created by the decisionmaker
- Documents that do not end up being considered by the final decisionmaker

The Deliberative Process Privilege

Postdecisional Documents

- Postdecisional documents are not protected by the privilege.
- Public has the right to be informed of official agency positions.

The Deliberative Process Privilege

Postdecisional Documents

- What is postdecisional to one decision may be predecisional to a subsequent decision.

The Deliberative Process Privilege

Losing Predecisional Status

Incorporation & **Adoption** have been defined as the same concept.

The Deliberative Process Privilege

Incorporation

- The decisionmaker expressly cites a previously predecisional document as the rationale for an agency's decision.

The Deliberative Process Privilege

Adoption

- A previously predecisional document comes to be used by the agency as the embodiment of agency policy.

The Deliberative Process Privilege

Retaining Predecisional Status: No Express Approval

- Adoption of a bottom-line recommendation in a document without expressly indicating approval of the rationale(s) for the recommendation is not enough to satisfy this standard.

The Deliberative Process Privilege

Elements

Documents must be:

1. Predecisional

   and

2. **Deliberative**

The Deliberative Process Privilege

"Deliberative" Defined

- Communications that are offered in support of the agency's decisionmaking process.

The Deliberative Process Privilege

Deliberative Information

- Recommendations
- Proffered opinions (e.g. "I believe that," "In my opinion," etc.).

The Deliberative Process Privilege

Duty to Segregate Factual Information

- The deliberative process privilege only applies to deliberative portions of documents.

The Deliberative Process Privilege

Duty to Segregate Factual Information

- Agencies must segregate out and release factual portions of the responsive document(s).

The Deliberative Process Privilege

Duty to Segregate Factual Information

- "Inextricably intertwined"
- Identity of the author is normally not deliberative.
- "Elastic facts"

The Deliberative Process Privilege

Duty to Segregate Factual Information

- Process of selection and inclusion of factual material can constitute deliberation

The Deliberative Process Privilege

Examples of Deliberative Documents

- Briefing materials
- Drafts

The Deliberative Process Privilege

New Sunset Provision

- The privilege "shall not apply to records created 25 years or more before the date on which the records were requested."

The Attorney Work-Product Privilege

Protects documents that were:

1. Prepared by or at the direction of an attorney

AND

2. Created in reasonable anticipation of litigation

The Attorney Work-Product Privilege

Prepared by or at the direction of an attorney

- Attorneys in various capacities
- Non-attorneys who are supervised by attorneys

The Attorney Work-Product Privilege

In Reasonable Anticipation of Litigation

- Though a specific claim need not have been actually filed, the privilege will not apply until an articulable claim likely to lead to litigation has arisen.

The Attorney Work-Product Privilege

Applies to documents created in:

- Civil and criminal litigation
- Administrative proceedings
- An effort to settle claims***
- Recommendations to close a case or to decline prosecution

The Attorney Work-Product Privilege

The privilege does not apply to documents created subsequent to the closing of a claim.

The Attorney Work-Product Privilege

The privilege does not apply to documents created in an agency's normal course of business.

The Attorney Work-Product Privilege

A document must meet the criteria for the privilege at the time of its creation to be covered by the privilege.

The Attorney Work-Product Privilege

Agencies are not required to segregate factual material from documents covered by the privilege.

The Attorney-Client Privilege

Confidential communications between an attorney and his or her client relating to a legal matter for which the client has sought professional advice

The Attorney-Client Privilege

Protects confidential information supplied from client to attorney, as well as the attorney's advice based upon client supplied information.

The Attorney-Client Privilege

The attorney-client privilege is not limited to situations involving litigation.

The Attorney-Client Privilege

For privilege to apply, communications must be:

1. Between an attorney and client

AND

2. Confidential

The Attorney-Client Privilege

Who is "the Client?"

- Can be a federal agency

  and

- Must identify client

The Attorney-Client Privilege

"Confidential" Defined

- Communications can be considered "confidential" when the specific information conveyed is confidential, even though the underlying subject matter is known to third parties.

The Attorney-Client Privilege

As with work-product, the attorney-client privilege applies to both factual and deliberative materials.

Applying the Foreseeable Harm Standard

Should not withhold information under Exemption 5 unless there is a foreseeable harm in disclosure.

Conclusion: The Rule of 2

Always remember that Exemption 5 has two parts:

1. Threshold

   and

2. Applicable Discovery Privilege

Conclusion: The Rule of 2

Also, each of the three main privileges has two parts.

Conclusion: The Rule of 2

Deliberative Process

1. Predecisional

   and

2. Deliberative

Conclusion: The Rule of 2

Attorney Work-Product

1. Prepared by or at the direction of an attorney

AND

2. Created in reasonable anticipation of litigation

Conclusion: The Rule of 2

Attorney-Client

1. Communication between an attorney and client

AND

2. Confidential

UNITED STATES DEPARTMENT of JUSTICE

Freedom of Information Act (FOIA) and Privacy Act Interface

1

Purpose of the Privacy Act

Protect the privacy of the individuals about whom the government maintains records by:

1. Limiting the collection, maintenance, use, and disclosure of personally identifiable information.
2. Allowing individuals to request access to, amendment of, and an accounting of disclosures concerning records about themselves.

General Presumption is Protection

Purpose of the FOIA

- Facilitates government transparency and accountability.
- Provides a means for the public to "know what the government is up to."
- Permits agencies to protect certain records that fall within any of the nine FOIA exemptions.

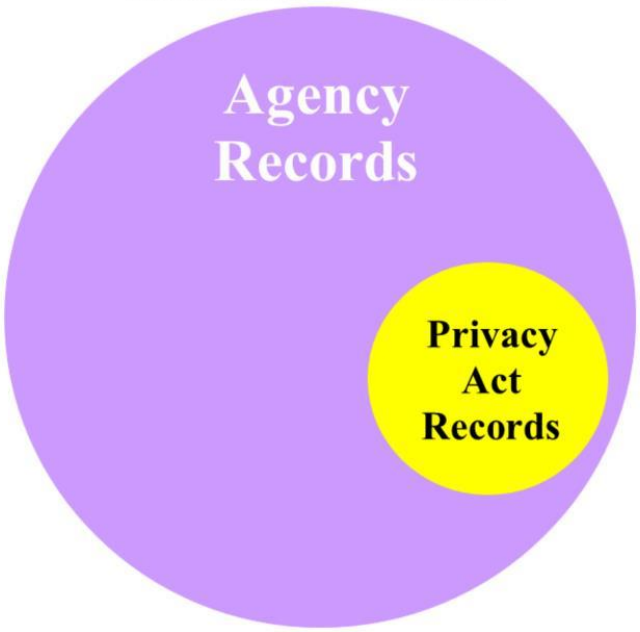
General Presumption is Disclosure

Records Covered

Privacy Act	**FOIA**
Records must be: 1. About an individual, 2. Stored in a system of records, and 3. Accessed by personal identifier.	All agency records.

Privacy Act Record = Agency Record
Agency Record ≠ Privacy Act Record

Records Covered



5

Privacy Act Definitions

- Individual
- Record
- System of Records
- System of Records Notice

Privacy Act Definitions

Individual:
A citizen of the United States or a lawfully admitted permanent resident.

5 U.S.C. § 552a(a)(2)

Does not include:

- Organizations
- Deceased individuals

Privacy Act Definitions

Record:

"any item, collection, or grouping of information **about an individual** that is maintained by an agency…"

5 U.S.C. § 552a(a)(4)

Generally, "must both be 'about' an individual and include his name or other identifying particular."

Tobey v. NLRB, 40 F.3d 469, 471 (D.C. Cir. 1994)

Privacy Act Definitions

System of Records:

"a group of records under the control of any agency from which information is retrieved by [personal identifier]"

5 U.S.C. § 552a(a)(5)

The record must be locatable using a personal identifier and the agency must in fact access the records using a personal identifier.

OMB Guidelines, 40 Fed. Reg. 28,948 (July 9, 1975)

Privacy Act Definitions

System of Records Notice (SORN):

- Provides notice to the public about a system of records.
- Includes, among other items, the agency's purposes for collecting and routine uses of the information.
- If you have questions about whether disclosing records is appropriate, or whether a Privacy Act exemption applies, consult the SORN.

Privacy Act: General Rule

- Generally, agencies cannot disclose Privacy Act records without the prior written consent of the individual.

- Records may be disclosed without prior written consent under certain conditions.

Privacy Act Conditions of Disclosure

An agency can disclose Privacy Act records without prior written consent in the following circumstances:

(b)(1) Need to know within agency

(b)(2) If required under the FOIA

(b)(3) Routine use published in SORN

(b)(4) Census Bureau

(b)(5) Statistical research (if de-identified)

(b)(6) National Archives

Privacy Act Conditions of Disclosure

(b)(7) Law enforcement request

(b)(8) Compelling circumstances for the health and safety of an individual

(b)(9) Congress

(b)(10) Government Accountability Office

(b)(11) Court order

(b)(12) Pursuant to Debt Collection Act

Access under Privacy Act and FOIA

- Both the Privacy Act and FOIA provide rights of access to records.
- However, there are differences in the extent of access depending on the statute.

Who has a right of access?

Privacy Act

- U.S. Citizens
- Lawful Permanent Residents

Note: Certain non-U.S. persons may have access rights pursuant to the Judicial Redress Act of 2015.

FOIA

- U.S. Citizens
- LPRs
- Non-U.S. Citizens
- Organizations

ANYONE

First Party v. Third Party Requests

1st Party Request

- When an individual asks for records about him/herself.

3rd Party Request

- When someone seeks records about another individual.

Processing Requests

1st Party Requests

- Process first under the Privacy Act, then under the FOIA for the greatest disclosure.

3rd Party Requests

- Process only under FOIA

How to Process <u>First Party Requests</u>

1. Does a Privacy Act exemption apply?
   - If **no**, release.
   - If **yes**, continue to FOIA analysis.
2. Does a FOIA exemption apply?
   - If **no**, release.
   - If **yes**, withhold.

Information can only be withheld when <u>both</u> Privacy Act and FOIA exemptions apply.

How to Process Third Party Requests

- Process third party requests for Privacy Act records under the FOIA only.
- Release records if FOIA **requires** disclosure:
  - FOIA requires disclosure if no FOIA exemption applies.
- Agency generally needs a FOIA request in hand to release Privacy Act records.

Bartel v. FAA, 725 F.2d 1403 (D.C. Cir. 1984).

19

Privacy Act Exemptions

10 Exemptions

- One special
- Two general (apply to entire record)
- Seven specific (require segregation)

The exemptions apply to certain Privacy Act provisions, such as those concerning access and amendment.

One Special Exemption

Section 552a(d)(5) exempts from disclosure:

> **"Any information compiled in reasonable anticipation of a civil action or proceeding."**

Self-executing exemption.

FOIA Exemption: **5** (attorney work-product)

Two General Exemptions

(j)(1): **CIA systems of records.**

FOIA Exemption: **3**

(j)(2): Systems of records maintained by a **principal function** criminal law enforcement agency and the records were **compiled for criminal law enforcement purposes**.

FOIA Exemption: **7**

Seven Specific Exemptions

Agency may exempt a system of records if it contains:

(k)(1): **Classified information**

FOIA Exemption: **1**

Seven Specific Exemptions

(k)(2): Generally applies to **investigatory material** compiled for **law enforcement purposes, other than material within the scope of subsection (j)(2).**

FOIA Exemption: **7**

Seven Specific Exemptions

(k)(3): **U.S. Secret Service** information

(k)(4): required by statute to be maintained and used solely as **statistical records**.

Seven Specific Exemptions

(k)(5): **Source-identifying investigatory material** compiled solely for the purpose of determining suitability, eligibility, or **qualifications for Federal civilian employment**, military service, Federal contracts, or access to classified information.

FOIA Exemption: **7(C), 7(D)**

Seven Specific Exemptions

(k)(6): **Testing or examination material** used solely to determine individual **qualifications for appointment or promotion in the Federal service.**

(k)(7): **Evaluation material used to determine potential for promotion in the armed services**, but only to the extent it would reveal the identity of a confidential source who was granted an express promise of confidentiality.

FOIA and Privacy Act Exemptions

- FOIA and Privacy Act exemptions are not exact matches.
- Be clear about which statute to apply.

Third Party Information Within a Privacy Act Record

- There is no PA equivalent to FOIA Exemptions 6 or 7(C).
- Third parties may have a legitimate privacy interest in the information.

How have courts addressed this gap?

- Some courts hold that certain third party information is not part of the requesters "record."
  - FBI agents and phone numbers. (Nolan)
  - Non-government info where there is some potential for harassment or harm. (DePlanche)

Nolan v. DOJ, 1991 WL 36547, *9 (D. Colo. 1991), *aff'd* 973 F.2d 843.
DePlanche v. Califano, 549 F. Supp. 685, 693, 696-98 (W.D. Mich. 1982).

Summary

- Understand how to identify a Privacy Act record.
- Process records using one statute and one set of exemptions at a time.
- Seek guidance on the interface between Privacy Act and FOIA when needed.

Resources

Privacy Act

- OMB has primary responsibility for Privacy Act guidance
- Agency Privacy Officer
- Office of Privacy and Civil Liberties (DOJ Components)

FOIA

- Agency FOIA Officer
- DOJ Office of Information Policy

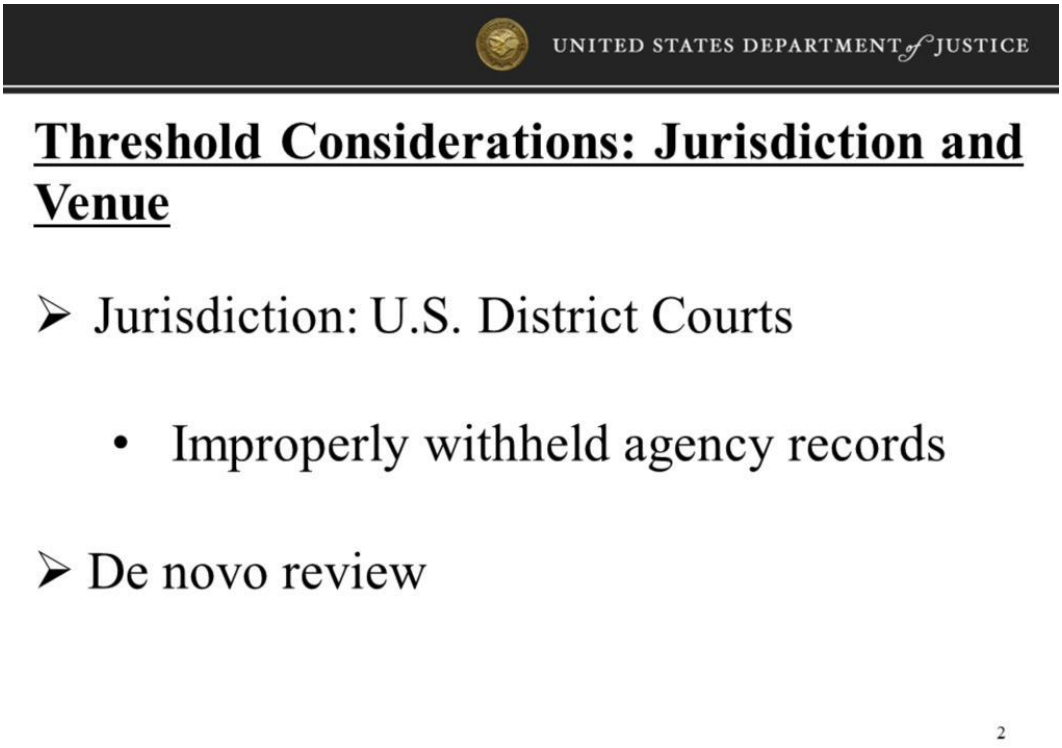
UNITED STATES DEPARTMENT of JUSTICE

Questions?

UNITED STATES DEPARTMENT of JUSTICE

Litigation Considerations

1

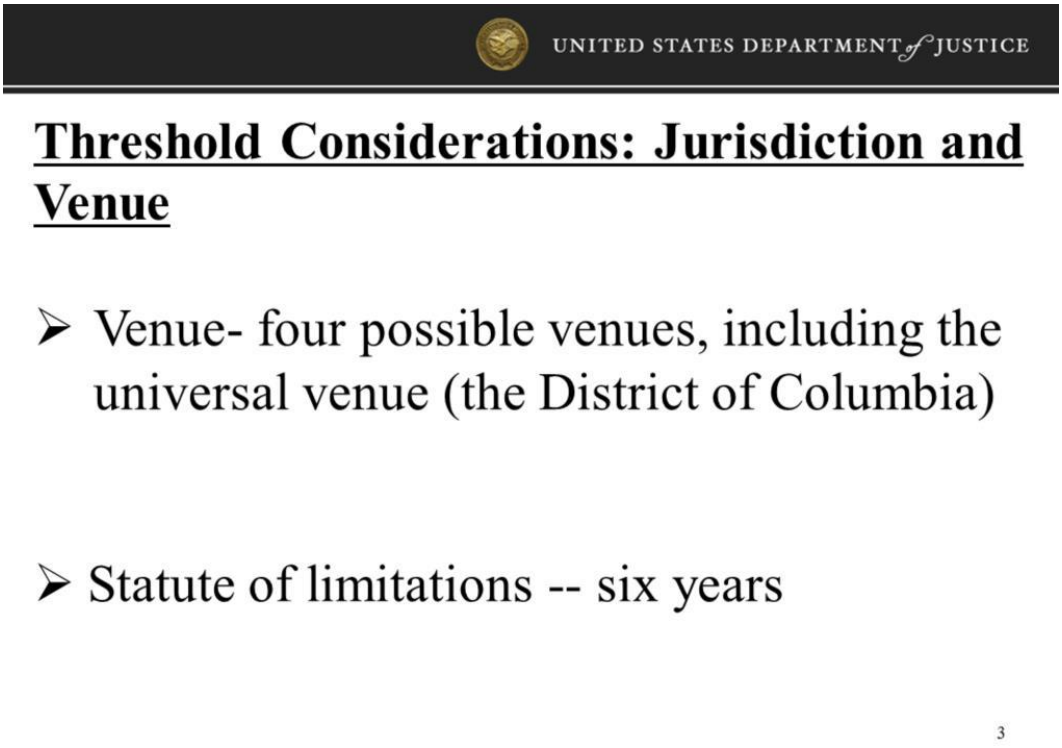


If a plaintiff fails to allege that an agency improperly withheld agency records, courts have dismissed such cases under two alternate grounds:

- 12(b)(1): lack of subject matter jurisdiction; and
- 12(b)(6): failure to state a claim upon which relief can be granted (even if all facts as pled are true, plaintiff not entitled to any FOIA relief).

Standard of review:

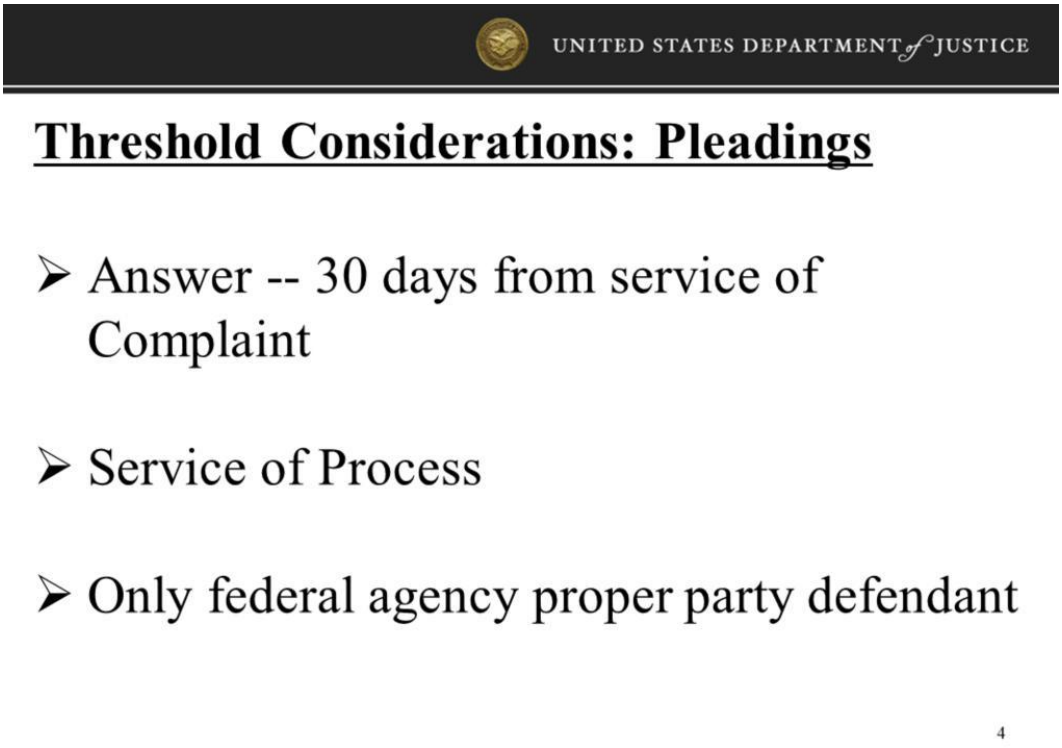
1) National Security Cases: Court use a highly deferential standard of review for classified documents in order to avoid compromising national security.
2) Fee Waiver Issues: Are reviewed De Novo, but the scope of the review is specifically limited by statute to the record before the agency.
3) Expedited Processing Issues: When denied under the statutorily based "compelling need" standard courts will review De novo. However, if additional methods for seeking expedited processing are found by regulation, court generally will give "judicial deference."
4) Reverse FOIA Lawsuits: Courts use the more deferential "arbitrary and capricious" standard under the APA.



Proper venue- The district of Columbia (always), where records are located, where plaintiff resides or has principal place of business. So, if you do not file in D.C., you must allege facts giving rise to venue in that court.

- Citizenship status is irrelevant- if R lives in U.S. district even if not a resident, he/she can bring suit in that forum.
- Forum non conveniens- While choice of P's forum gets significant weight, if there are strong reasons to transfer the case to another forum, the court can do so.
- Comity- if another case is pending on the same records or a very similar request, a court may stay its proceedings pending the ruling in the other court, or even dismiss the complaint or transfer the case to the other court.

Statute of limitations- six years from the date that plaintiff could have first filed suit. More on exhaustion below. Interesting question: What if an agency sits on a request for seven years?



Complaint-

- **Service**- Fed. R. Civ. Pro. Rule 4 states that to serve the United State Government a Plaintiff must: (1) deliver a copy of the summons and Complaint to the U.S. Attorney where the action is brought; (2) send a copy of each by registered mail or certified mail to the Attorney General of the United States at Washington, DC;

- **Proper Party Defendants**- Only federal agencies are proper party defendants in FOIA lawsuits. See 5 U.S.C. 552(a)(4)(B).

- **Proper Party Plaintiffs**- Generally, only the person who submitted a FOIA request at the administrative level can be the proper party plaintiff in any subsequent lawsuit.

Answer-

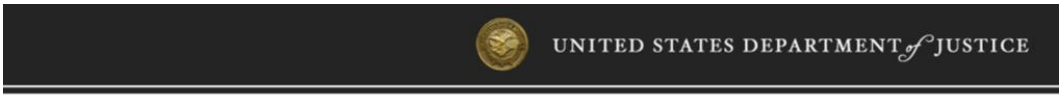
- Note that AUSA's inexperienced in FOIA can be tripped up by the 30 day limit. Normally federal agencies have 60 days to Answer complaints.
- The Answer should set forth all affirmative defenses or they could be lost. [provide

examples]

Threshold Considerations: Grounds for Dismissal

- Lack of subject-matter jurisdiction
- Lack of personal jurisdiction*
- Improper venue*
- Insufficient service of process*
- Failure to state a claim
- Res judicata/collateral estoppel

***waived if not raised in 1st responsive pleading**



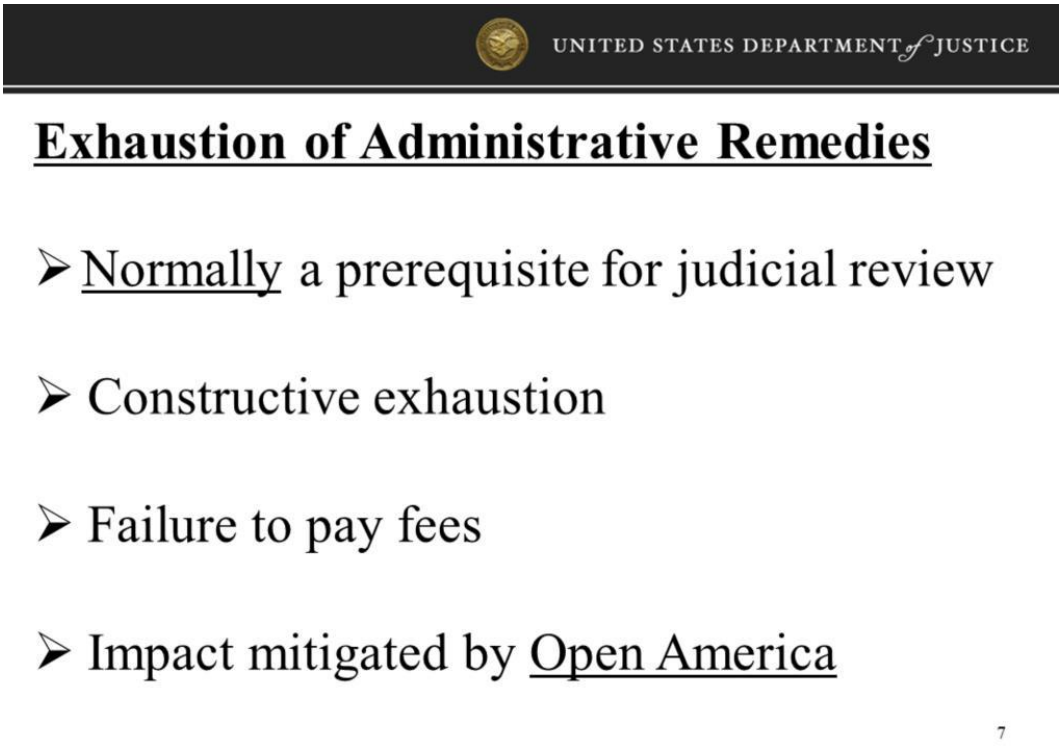
Standard of Review

- De novo
- National Security cases
- Fee waiver issues
- Expedited processing issues
- Reverse FOIA lawsuits

SEAN

Standard of review:

1) National Security Cases: Courts use a highly deferential standard of review for classified documents in order to avoid compromising national security.
2) Fee Waiver Issues: Are reviewed de novo, but the scope of the review is specifically limited by statute to the record before the agency.
3) Expedited Processing Issues: When denied under the statutorily based "compelling need" standard (imminent threat to life or safety; "urgency to inform") courts will review de novo. However, if additional methods for seeking expedited processing are created by regulation, court generally will give "judicial deference."
4) Reverse FOIA Lawsuits: Courts use the more deferential "arbitrary and capricious" standard under the APA.



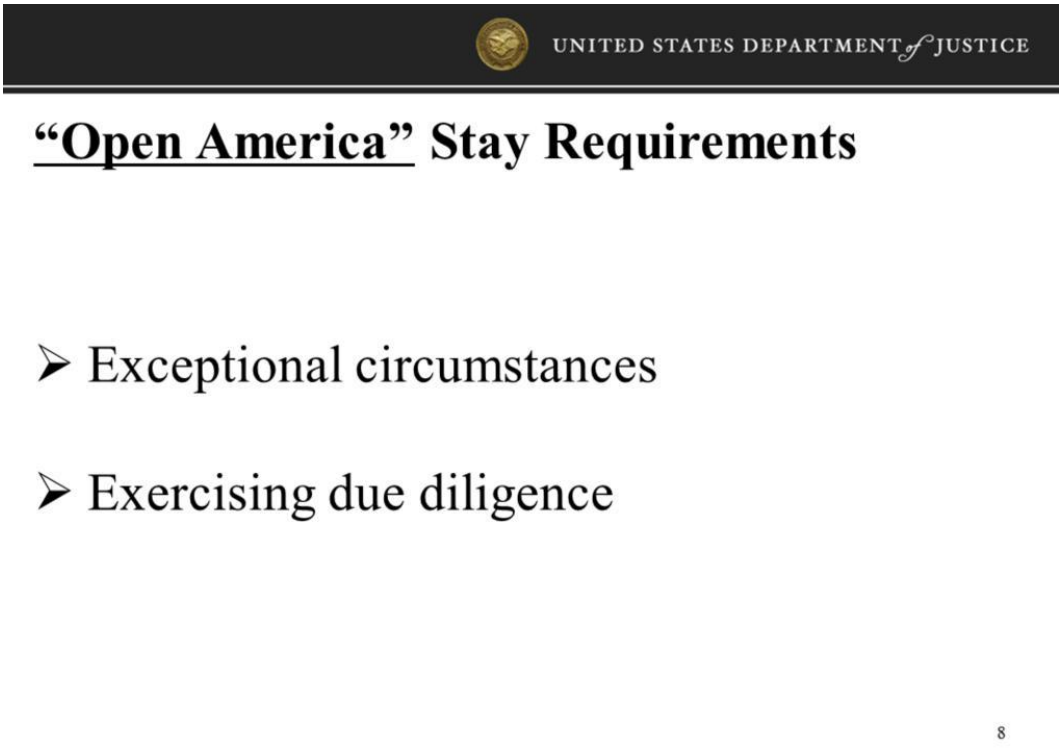
Exhaustion:

- Actual exhaustion happens where the agency responds, the requester appeals, and the appeal is adjudicated.

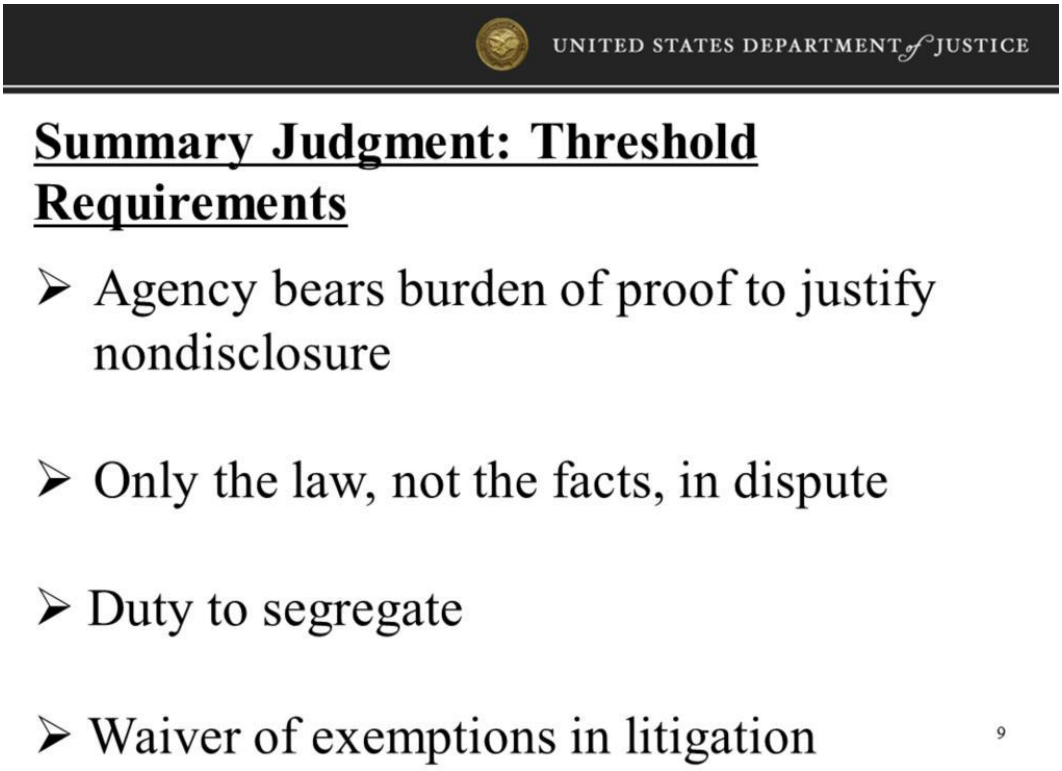
- Constructive exhaustion- since the FOIA does not prescribe a distinct SOL, the DC Cir. in Spannaus held that 28 USC 2401(a) applied to FOIA actions. Section 2401(a) provides, in pertinent part, that "every action commenced against the United States shall be barred unless the complaint is filed within six years after the right of action first accrues." Spannaus further held that the accrual date was when the plaintiff constructively exhausted his/her administrative remedies and not when all administrative appeals had been finally adjudicated. The accrual date is going to be either the date of complete exhaustion of administrative remedies (where there is no constructive exhaustion) or the date that the requester constructively exhausted his/her administrative remedies. Spannaus v. DOJ, 824 F.2d 52 (D.C. Cir. 1987). An interesting question- what if the agency waits seven years to respond to the request? Waivers of sovereign immunity are strictly construed by courts, so a court cannot equitably toll or ignore the six year limit.

- Exhaustion cannot occur until all assessed fees have been paid (unless a fee issue is itself at issue in the litigation).

- Open America- see next slide



- Open America- where R sued based on constructive exhaustion, and the court retains jurisdiction of the case while permitting the agency to continue adminstratively processing the request. Requirements for Open America stay:
    - 1) exceptional circumstances exist- Deluged with volume of requests not anticipated by Congress, with existing resources insufficient to deal with that volume. If the volume is predictable, agency must demonstrate reasonable progress in reducing the backlog. Other factors: efforts to reduce backlog; size and complexity of other pending requests; amount of classified material at issue, etc. Requester's refusal to reasonably modify scope of request can also be a factor. Yet another reason why negotiating/discussing requests with requesters is valuable.
    - 2) agency due diligence- it is processing requests on a FIFO basis (within the track system)

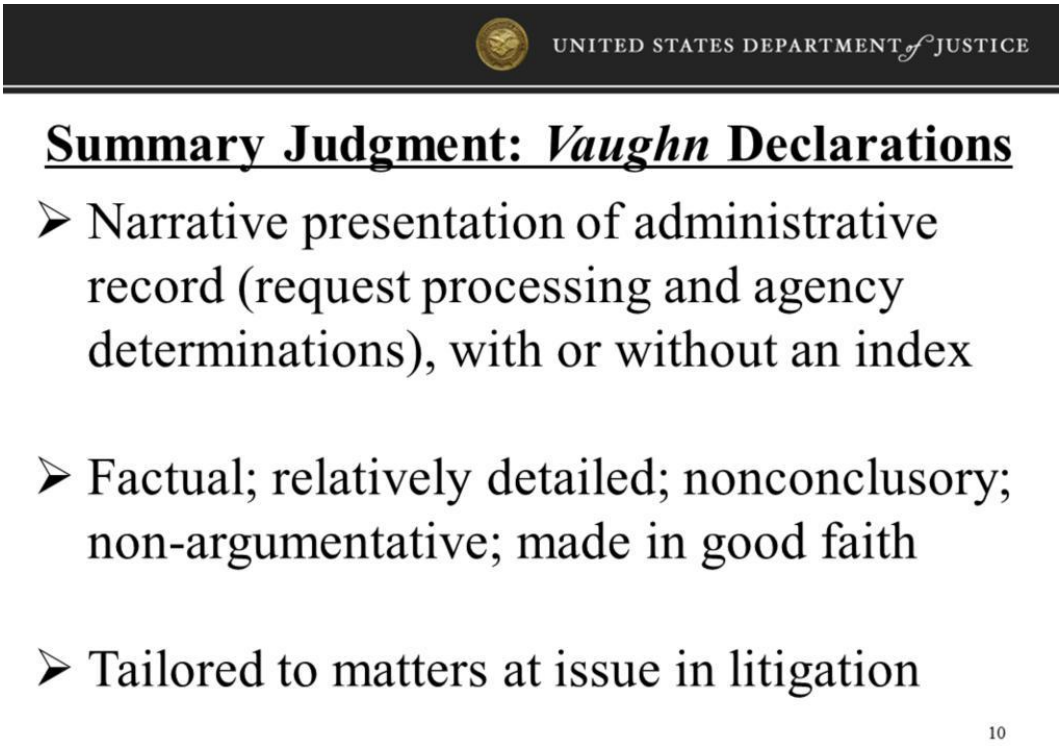


Summary judgment can be appropriate when the only disputes are legal, no factual disputes. **Almost all FOIA cases are decided on summary judgment.**

Agency meets its burden by filing Declarations and (if necessary) Vaughn index of withholdings.

Duty to segregate is essential- if the Declaration and brief do not address segregability, the court should not grant the government's MSJ, and it is grounds for reversal of an MSJ on appeal.

Waiver- if all applicable exemptions are not raised in the first dispositive motion, they could be waived. See Maydak. This can be particularly problematic in the 7A context.

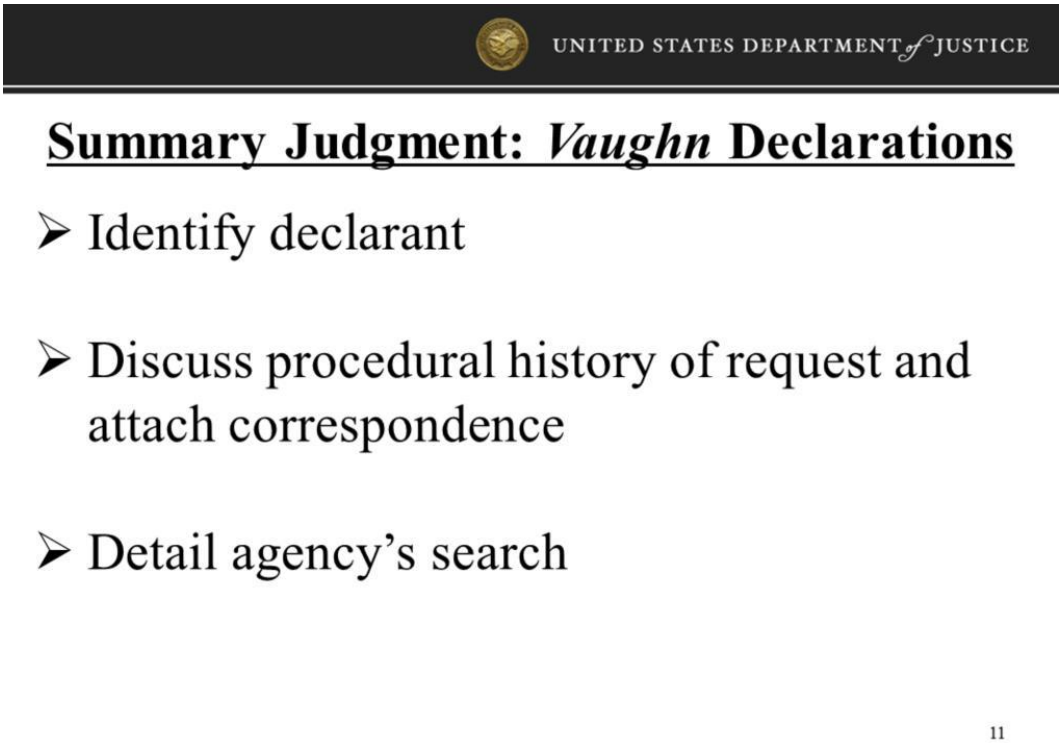


SEA

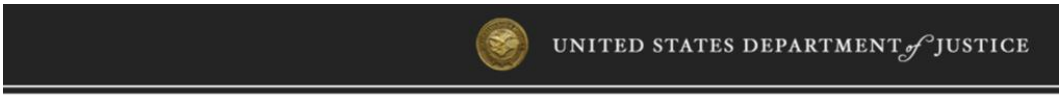
Dibacco v. U.S. Army, 795 F.3d 178, 191 (D.C. Cir. 2015) (holding that defendant's "burden was to show that its search efforts were reasonable and logically organized to uncover relevant documents; it need not knock down every single search design advanced by every requester"). "Adequacy not perfection is the standard that FOIA sets."

At the same time, focus on the word "nonconclusory." Your description of your search should be detailed, noting what databases were searched, what search terms were used, in such a way that the search will appear to the court to be logical and reasonable. Some of today's later lectures will talk more about this.

N


UNITED STATES DEPARTMENT of JUSTICE
Summary Judgment: *Vaughn* Declarations
➢ Identify declarant
➢ Discuss procedural history of request and attach correspondence
➢ Detail agency's search
11

SEAN

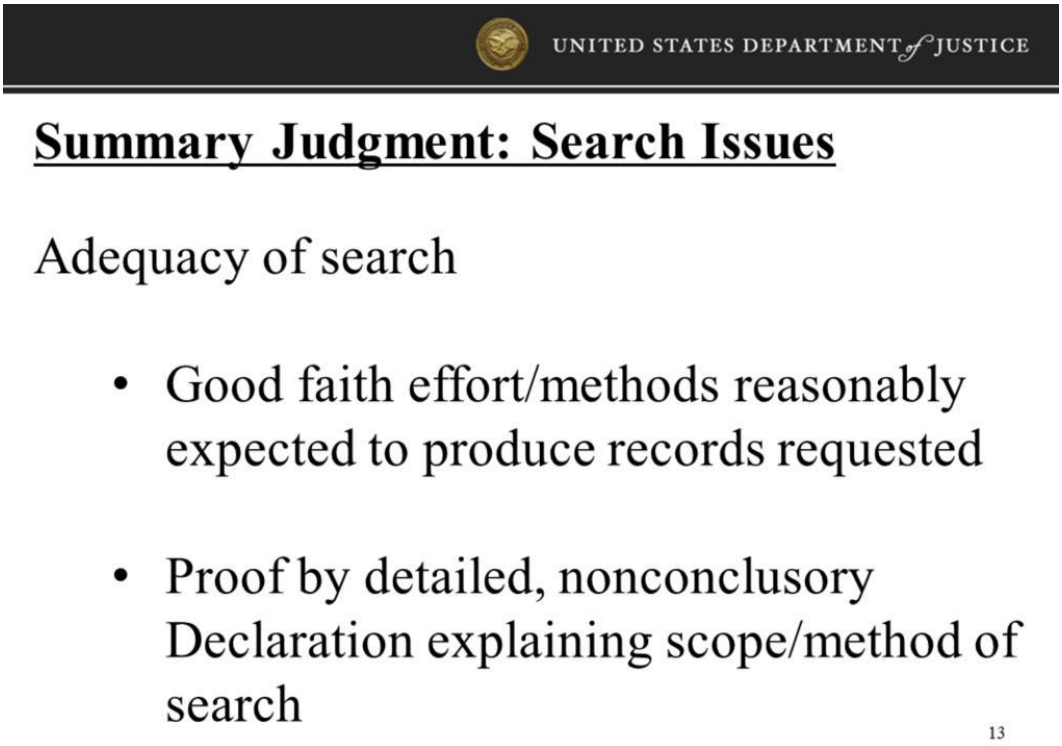


Summary Judgment: *Vaughn* Declarations

- Provide information about the records responsive to request
- Provide Vaughn Index -- either as part of declaration or as an attachment
- Explain that all reasonably segregable nonexempt information has been disclosed. **This must be done**

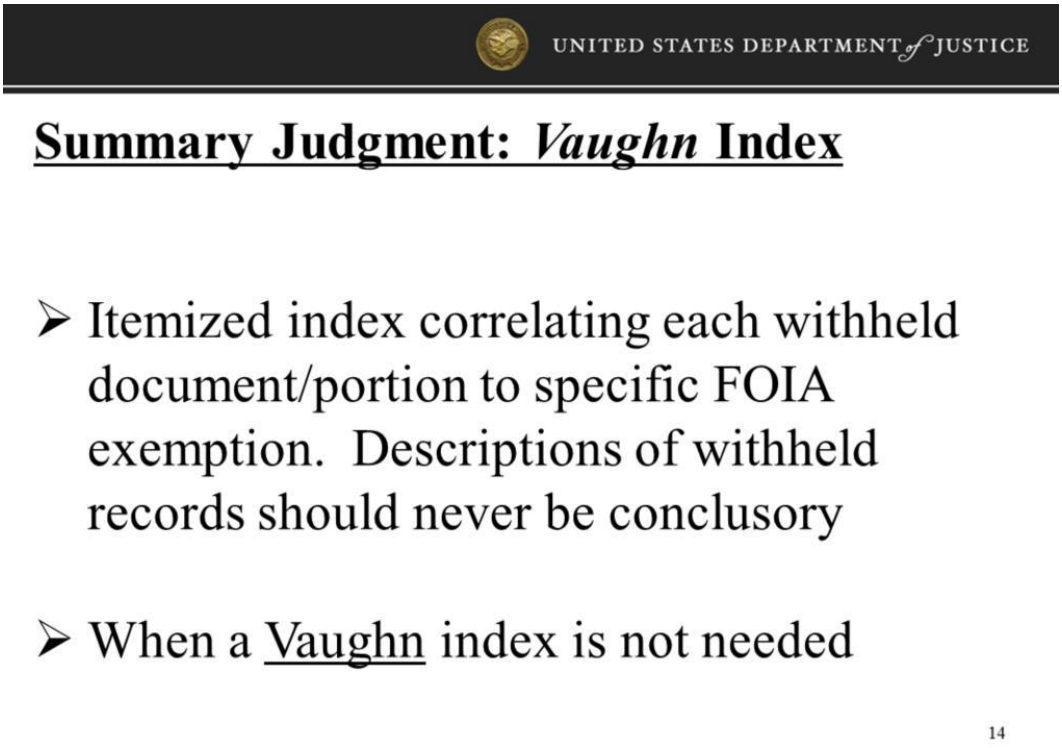
12

SEAN



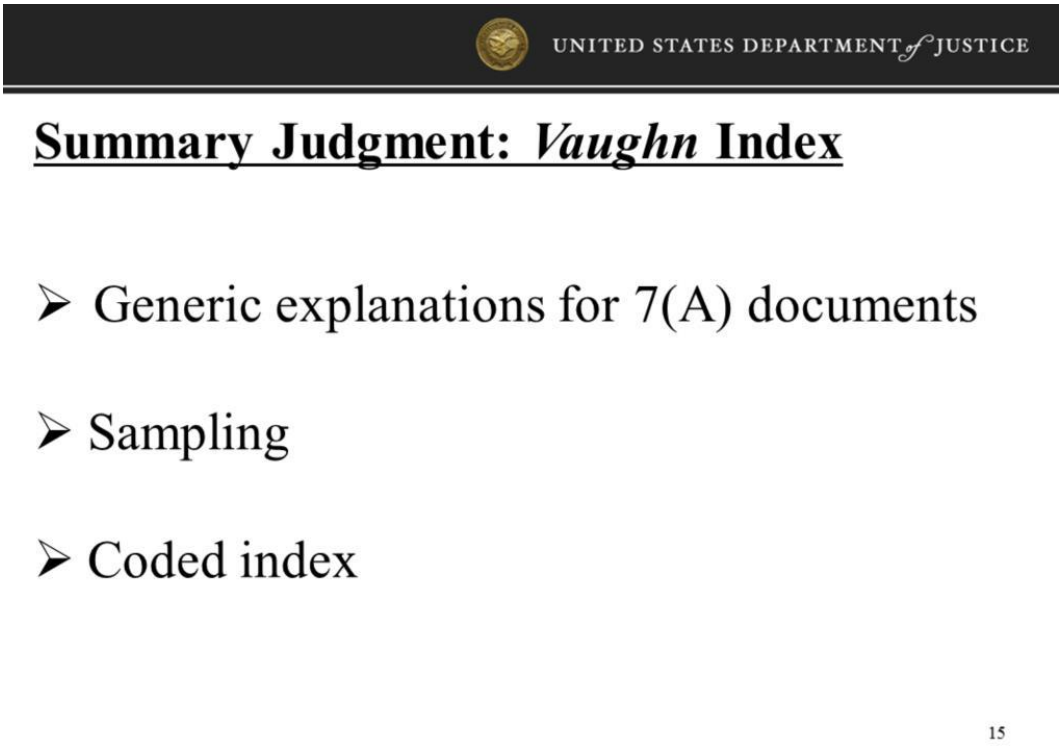
Dibacco v. U.S. Army, 795 F.3d 178, 191 (D.C. Cir. 2015) (holding that defendant's "burden was to show that its search efforts were reasonable and logically organized to uncover relevant documents; it need not knock down every single search design advanced by every requester"). "Adequacy not perfection is the standard that FOIA sets."

At the same time, focus on the word "nonconclusory." Your description of your search should be detailed, noting what databases were searched, what search terms were used, in such a way that the search will appear to the court to be logical and reasonable. Some of today's later lectures will talk more about this.



Just as with your description of the search adequacy, your description of the withholdings should be nonconclusory. When I read a court decision in which the government has lost on a withholding issue, it almost always is because the government simply asserted that the records were withholdable, and simply recited the statutory standard for withholding. A good description of the withholdings does not simply repeat the standard, but describes in as much detail as possible the withholdings in such a way as to demonstrate to the court that the statutory standard is satisfied. Again, more on this in later lectures.

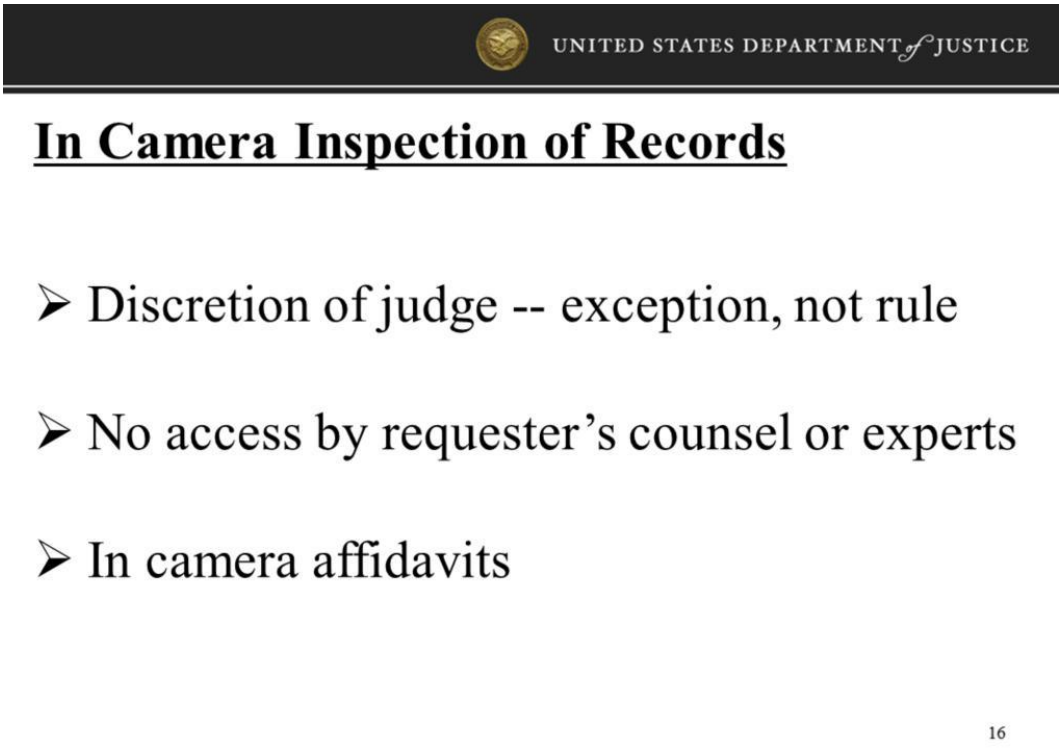
A Vaughn index is not always needed, such as when there are a small number of withholdings, or a large number of withholdings that are very similar and can be readily described in the Declaration itself.



- For Exemption 7(A), a detailed, itemized description of withholdings is often not required. Categorical treatment.

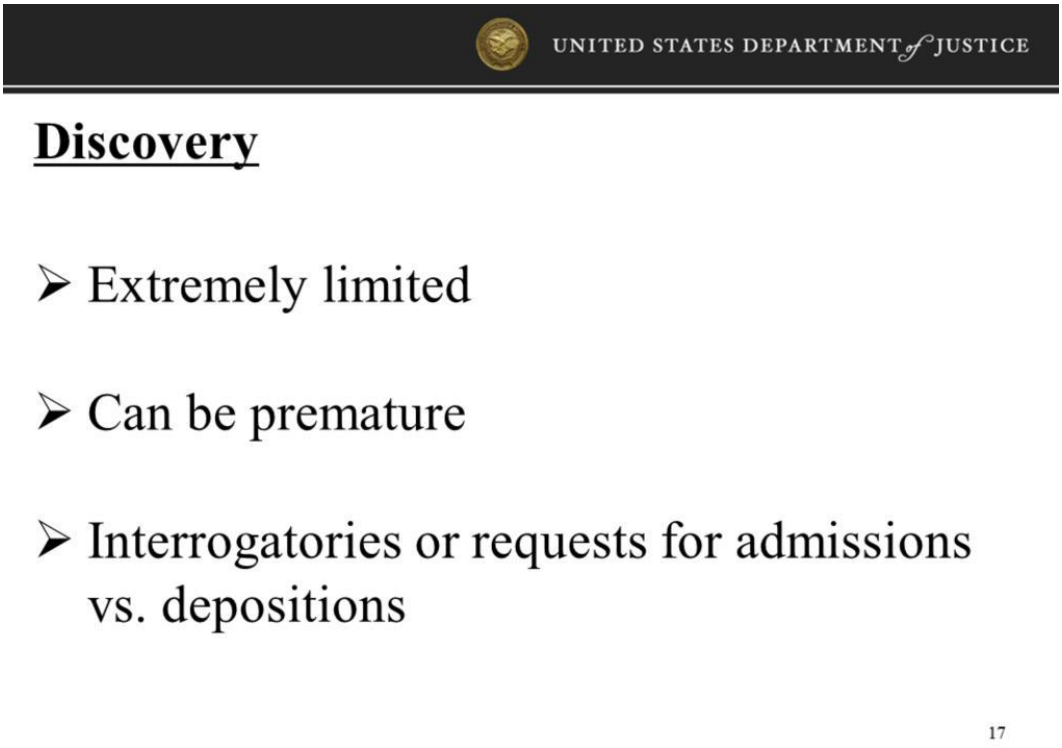
- Sampling- for large volumes of documents (thousands of pages), courts will normally accept a Vaughn index that describes only a sample of the documents. The size and composition of the sample will often be negotiated between the parties.

- Coded index- often used by the FBI, and most courts are OK with it. If the withholdings fall into general categories, you create a coded description of each category, and then insert the code rather than a full description of each withholding in the relevant entries of the Vaughn.

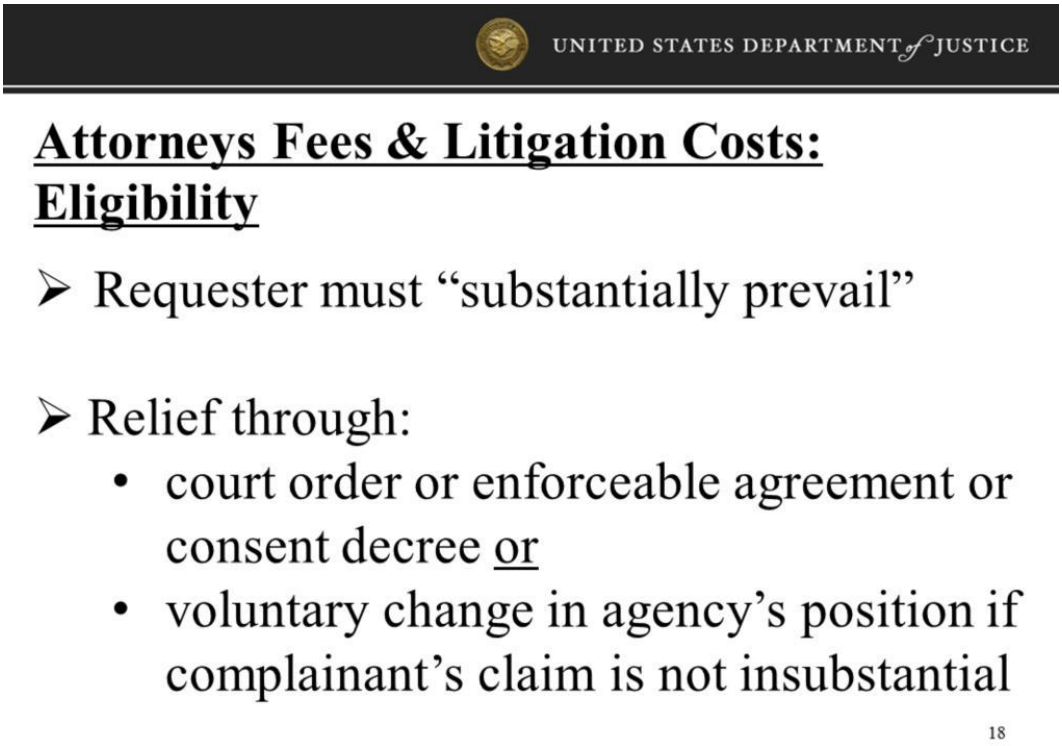


In camera inspection- sometimes used in national security cases where public declarations cannot sufficiently describe withholdings. Can also be used by a judge when he/she is not satisfied with the descriptions of withholdings made by the agency.

In camera affidavits- An alternative to in camera review, where the withholdings are too sensitive to describe on the public record.

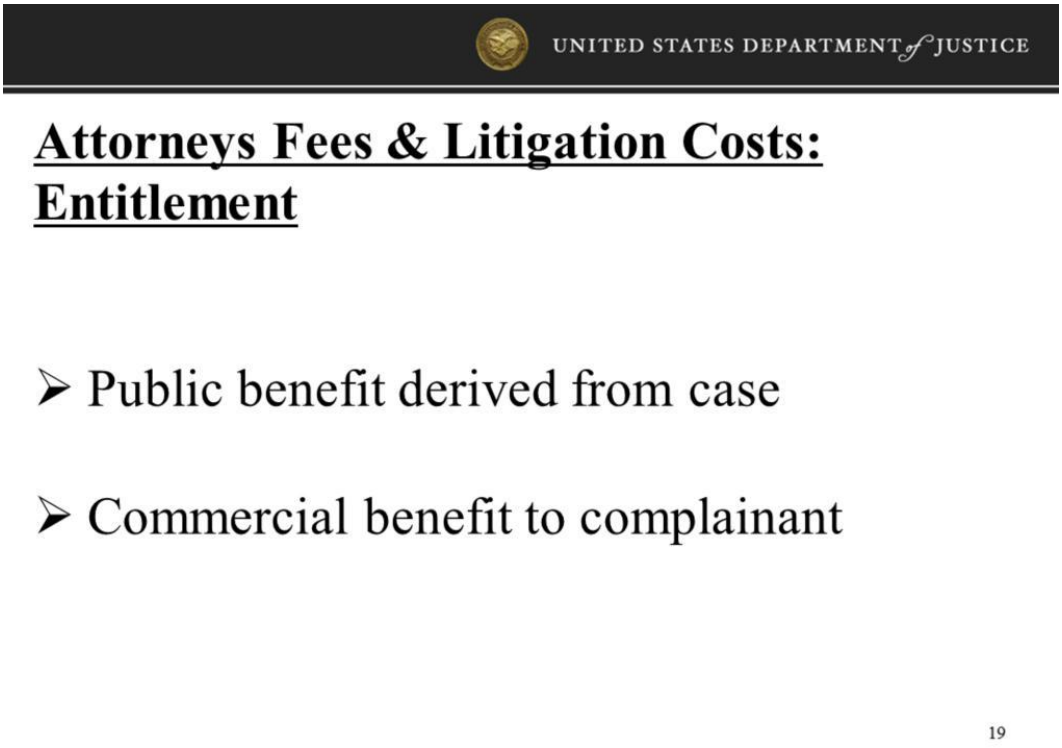


Discovery tends to happen more outside D.C., in courts that are less familiar with the FOIA, or where courts tend to be less deferential to the government. In DC, courts pretty consistently follow the principle that Declarations are presumed to be made in good faith, so discovery is rare.



The "voluntary change" in position standard for eligibility was reinstated by Congress through the 2007 FOIA amendments. Previously, a plaintiff could only get relief through a court ordered change in position.

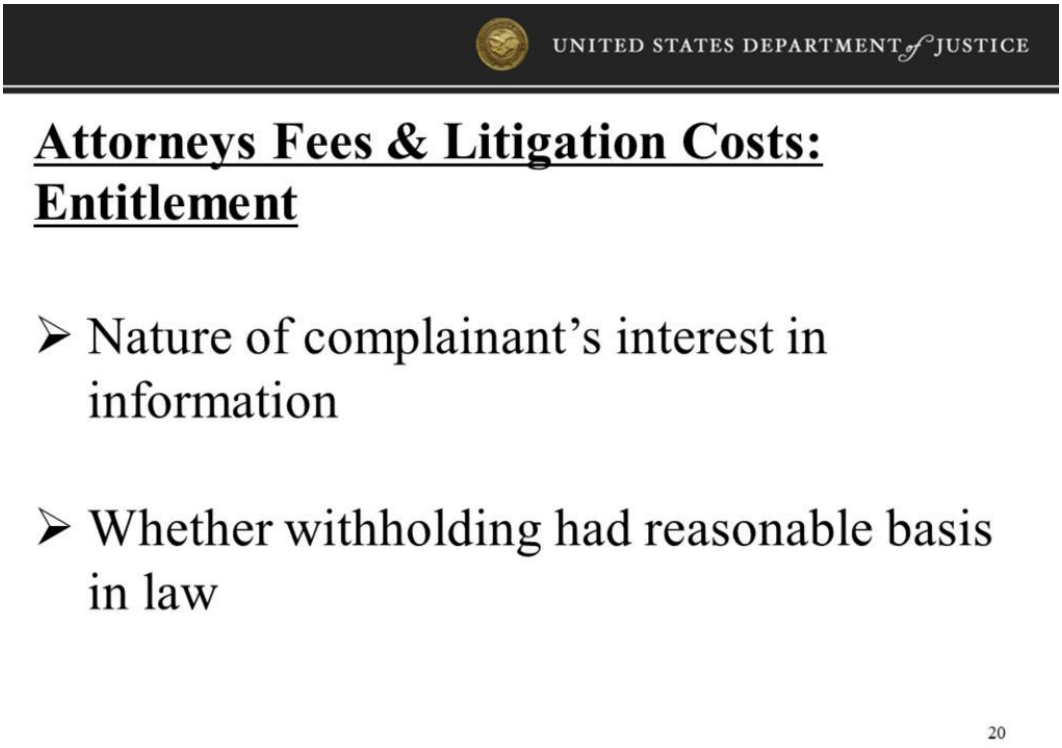
It is now relatively easy for plaintiff's to successfully argue that they are eligible for attorney fees, but remember that P's must show that they are both eligible AND entitled.



If possible, it is better to prevail on the "eligibility" prong of the attorney fee standard, because the four "entitlement" factors have no particular weight. A court can weigh them however it likes.

Public benefit- The records sought will add to the fund of information that citizens may use in making vital political choices. The likely extent of dissemination and the possible impact on the public are both relevant. **Per the 2016 D.C. Circuit case about the JFK assassination, this is based on the general topic, not on what is actually released.**

Commercial benefit- If plaintiff had an adequate private commercial incentive to litigate even in absence of attorney fees, that weighs against an award.



Nature of complainants interest in the records- similar to the second factor, and evaluated in tandem.

Whether withholding had reasonable basis in law- If there is supporting authority, likely the agency wins here. If there is no supporting authority, but no contradictory authority, the agency could still win. If there is contradictory authority and no supporting authority, the agency will lose on this factor If the agency's delay rather than an actual withholding is at issue, the court will look at whether the delay was reasonable.

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, March 8, 2018 1:17 PM
To:	Michelle Reed NOAA Federal
Subject:	Re: Please send me the slides ASAP
Attachments:	NOAA FOIA Litigation as of 03.9.18.docx; FOIA Privacy and DLP Overview Final.pptx

You bet

Here are the newly updated slides, along with the Litigation Summary.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Thu, Mar 8, 2018 at 1:11 PM, Michelle Reed NOAA Federal <michelle.reed@noaa.gov> wrote:

> Mark
> Please send the updated slides so I can send downtown asap.
> Thanks,
> Michelle
>
> Michelle Reed
> Chief of Staff
> Office of the Chief Information Officer
> Main Office: (301) 713 9600
> Direct: (301) 628 5725
> Mobile: (b)(6)

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

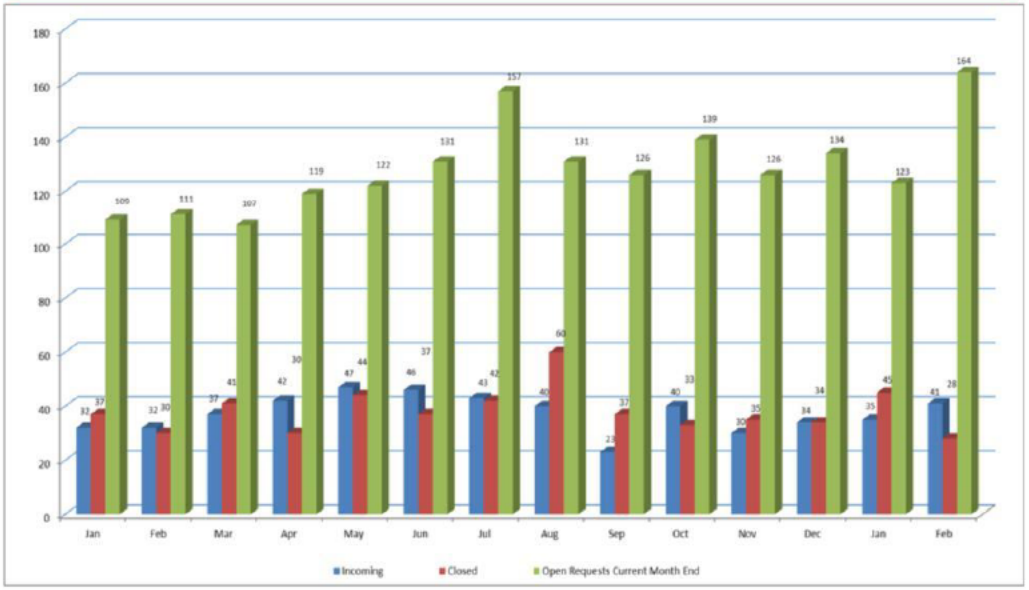
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

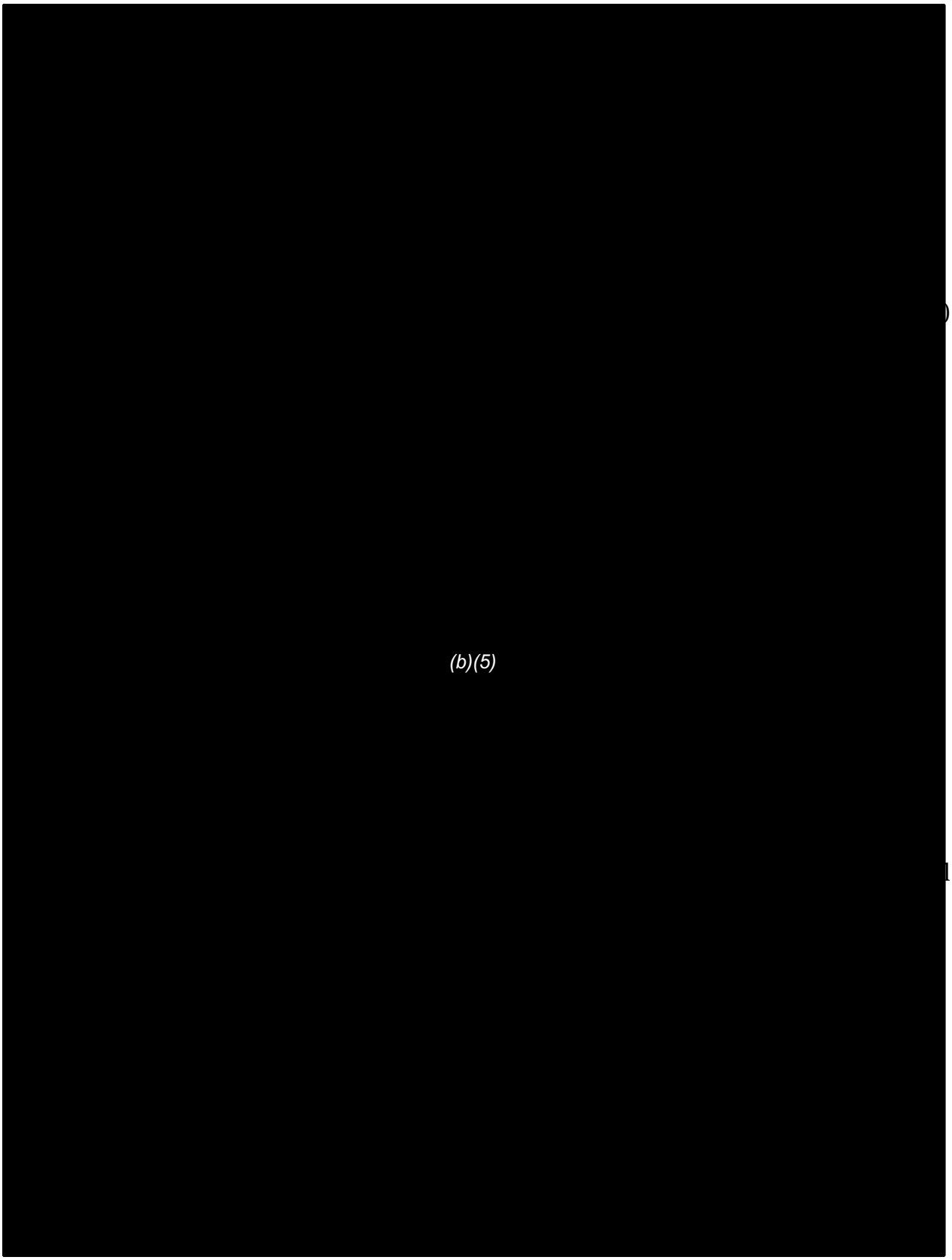
NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 9, 2018



Michelle Reed - NOAA Federal

From:	Michelle Reed NOAA Federal
Sent:	Thursday, March 8, 2018 2:38 PM
To:	Charles Powell NOAA Federal
Cc:	Pat A. Simms; Mark Graff NOAA Federal; Zachary Goldstein; Ann Madden NOAA Federal
Subject:	FOIA / Privacy / DLP Presentation for Dr. Jacobs 8:30 am 3/09/18
Attachments:	NOAA FOIA Litigation as of 03.9.18.docx; FOIA Privacy and DLP Overview Final.pptx

Charlie
Attached are the FOIA materials for Mark's presentation to Dr. Jacobs.
Please let us know if you have any questions.
Sincerely
Michelle

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

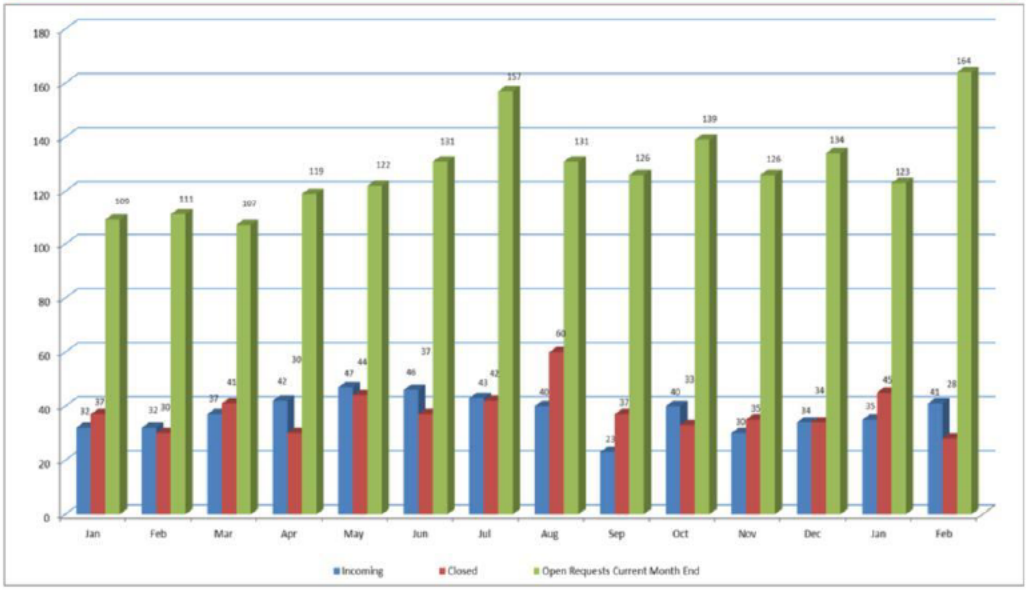
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

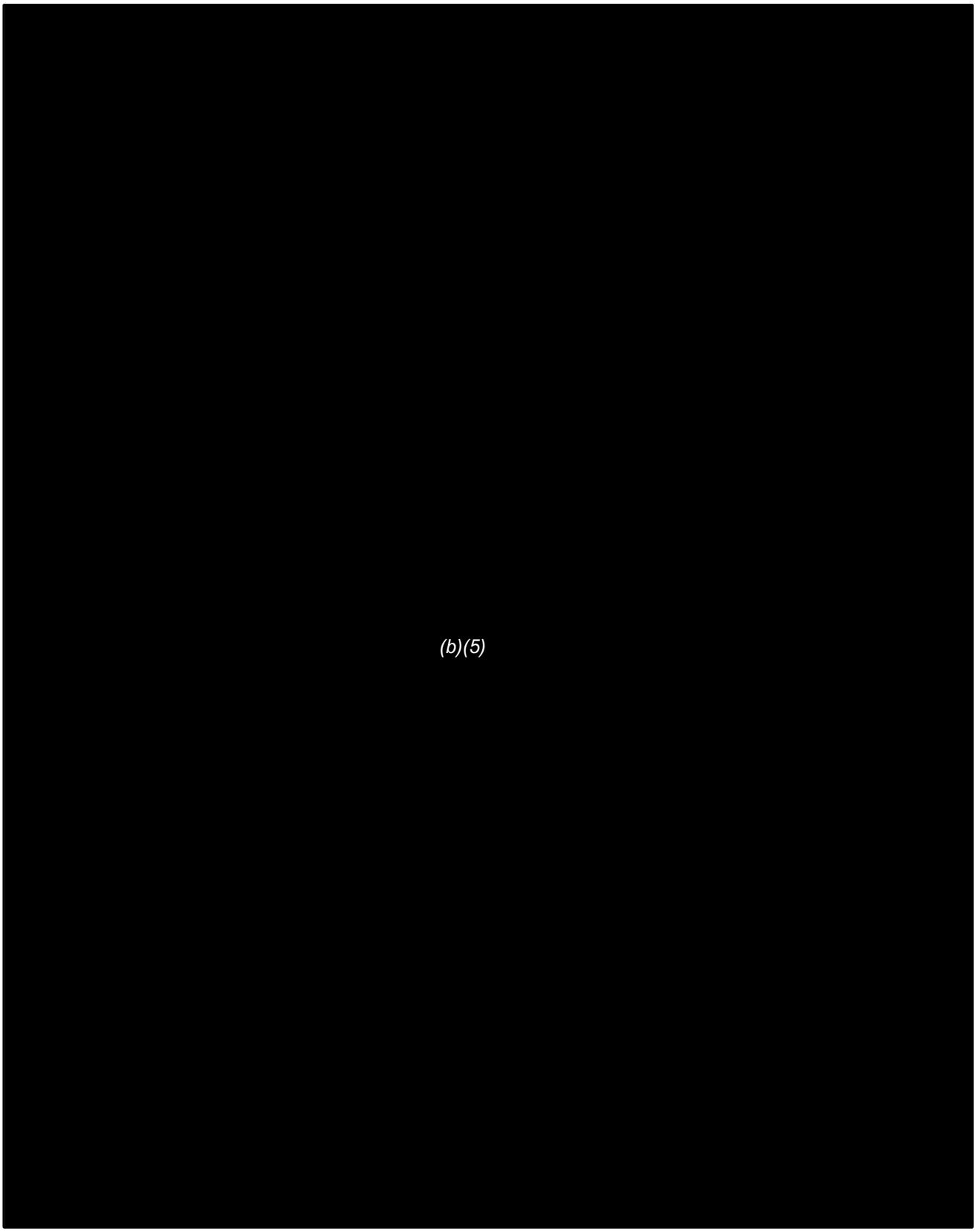
NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 9, 2018



Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, March 8, 2018 2:44 PM
To:	Robert Swisher NOAA Federal; Ed Kearns NOAA Federal; Dennis Morgan NOAA Federal
Cc:	Lola Stith NOAA Affiliate; Sarah Brabson NOAA Federal
Subject:	Fwd: FOIA / Privacy / DLP Presentation for Dr. Jacobs 8:30 am 3/09/18
Attachments:	NOAA FOIA Litigation as of 03.9.18.docx; FOIA Privacy and DLP Overview Final.pptx

FYI below these are the versions that are going to Dr. Jacobs for the briefing tomorrow morning. I'll let you guys know how it goes.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Forwarded message
From: **Michelle Reed - NOAA Federal** <michelle.reed@noaa.gov>
Date: Thu, Mar 8, 2018 at 2:38 PM
Subject: FOIA / Privacy / DLP Presentation for Dr. Jacobs 8:30 am 3/09/18
To: Charles Powell NOAA Federal <charles.powell@noaa.gov>
Cc: "Pat A. Simms" <Pat.A.Simms@noaa.gov>, Mark Graff NOAA Federal <mark.graff@noaa.gov>, Zachary Goldstein <zachary.goldstein@noaa.gov>, Ann Madden NOAA Federal <Ann.Madden@noaa.gov>

Charlie
Attached are the FOIA materials for Mark's presentation to Dr. Jacobs.
Please let us know if you have any questions.
Sincerely
Michelle

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

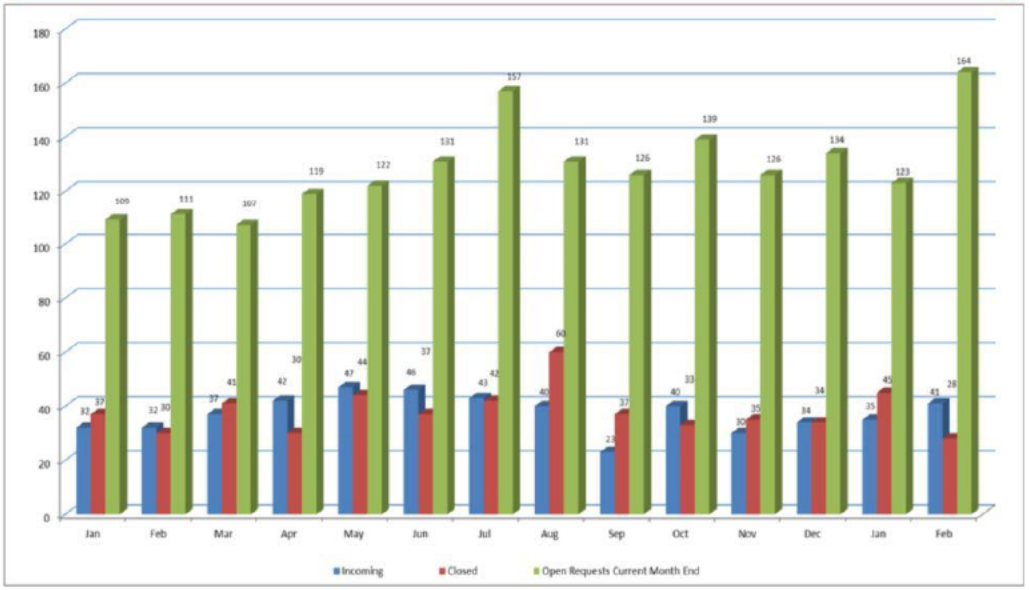
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

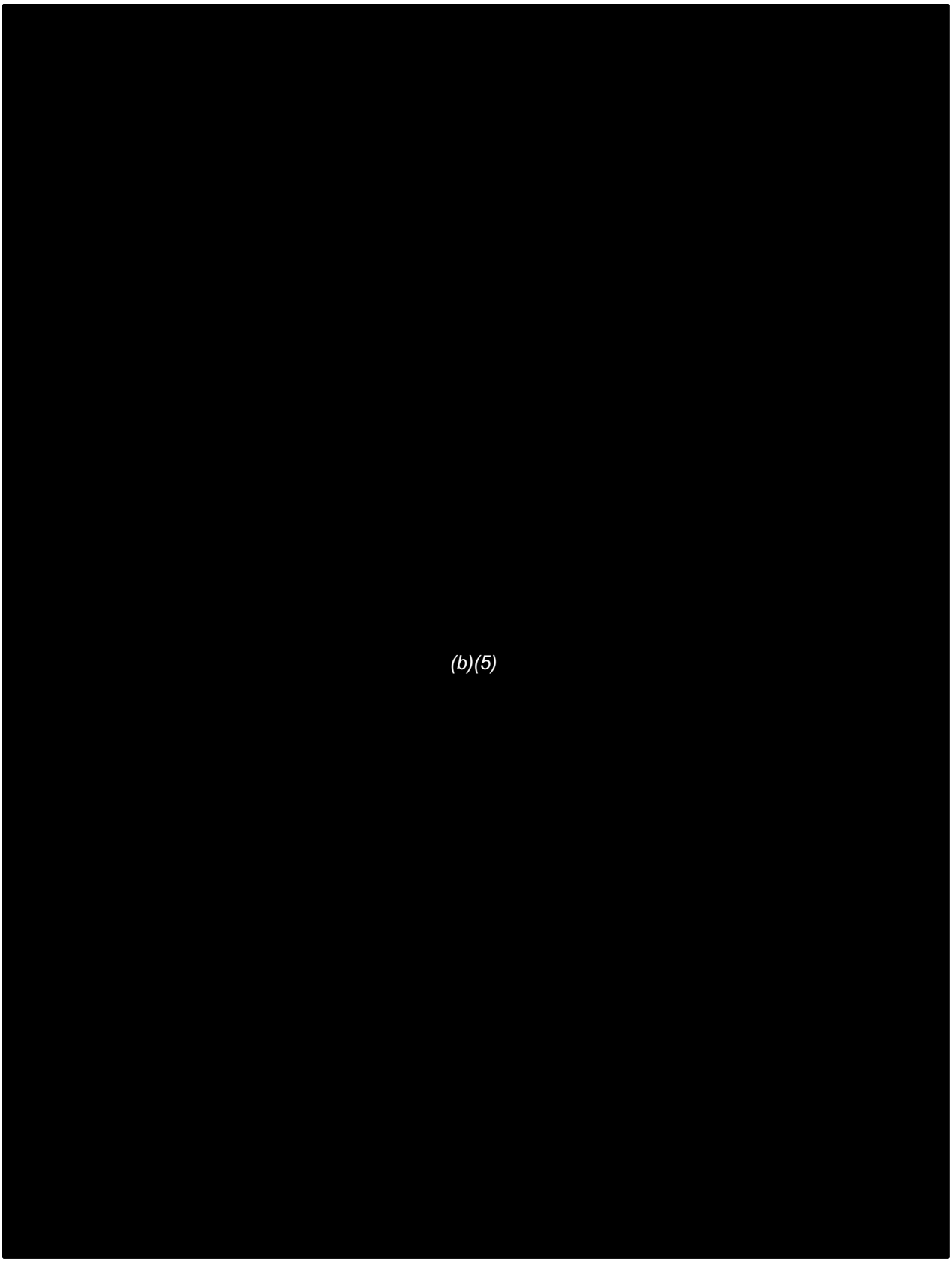
NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 9, 2018



Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, March 8, 2018 3:06 PM
To:	Samuel Dixon
Cc:	Steven Goodman NOAA Federal
Subject:	Re: Pending with NOAA FOIA
Attachments:	FOIA Privacy and DLP Overview Final.pptx; NOAA FOIA Litigation as of 03.9.18.docx

Still going through these

I might not complete all of them before COB, but I should be most of the way through. Some have quite a few records, so it's taking a bit. Thanks for the heads up.

Btw, I'm giving a briefing tomorrow to Dr. Jacobs, and it resulted in a pretty succinct summary of FOIA, Privacy, and DLP efforts I thought you guys might want to see, in case it helps your folks.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Thu, Mar 8, 2018 at 11:26 AM, Samuel Dixon <samuel.dixon@noaa.gov> wrote:

DOC NOAA 2018 000756	Final Review
DOC NOAA 2018 000387	Final Review
DOC NOAA 2016 000423	Interim Release Final Review
DOC NOAA 2018 000749	Final Review
DOC NOAA 2018 000716	Interim Release Final Review
DOC NOAA 2018 000463	Final Review
DOC NOAA 2017 001411	Interim Release Final Review
DOC NOAA 2017 002001	Final Review
DOC NOAA 2017 000304	Interim Release Initial Review
DOC NOAA 2018 000105	Final Review
DOC NOAA 2017 001431	Interim Release Final Review
DOC NOAA 2017 001198	Interim Release Final Review
DOC NOAA 2018 000740	Interim Release Final Review

Thanks,

Samuel Dixon
NMFS Assistant FOIA Liaison
Contractor - IBSS Corp

(301) 427-8739
samuel.dixon@noaa.gov

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

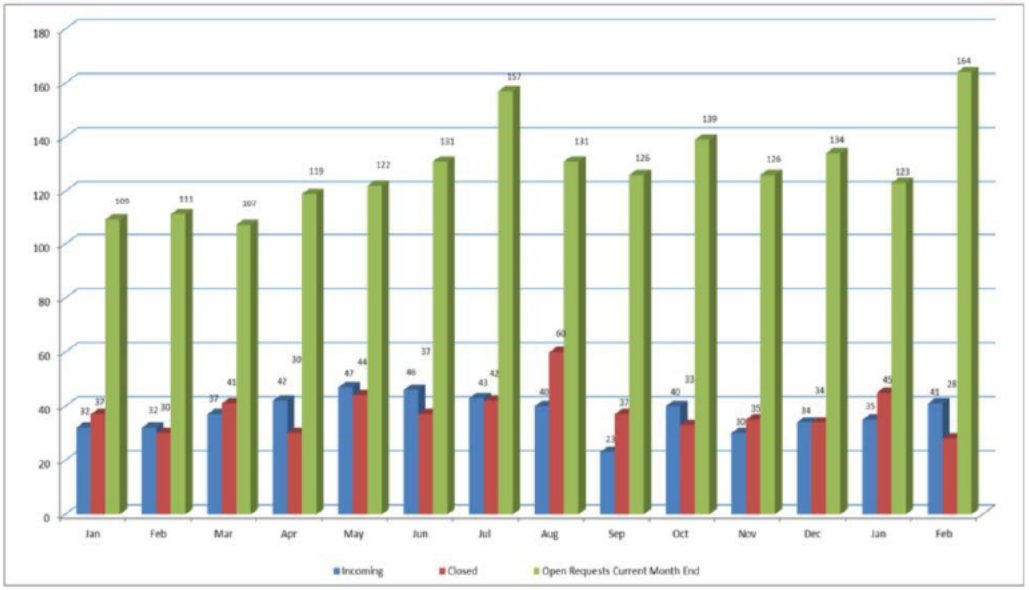
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

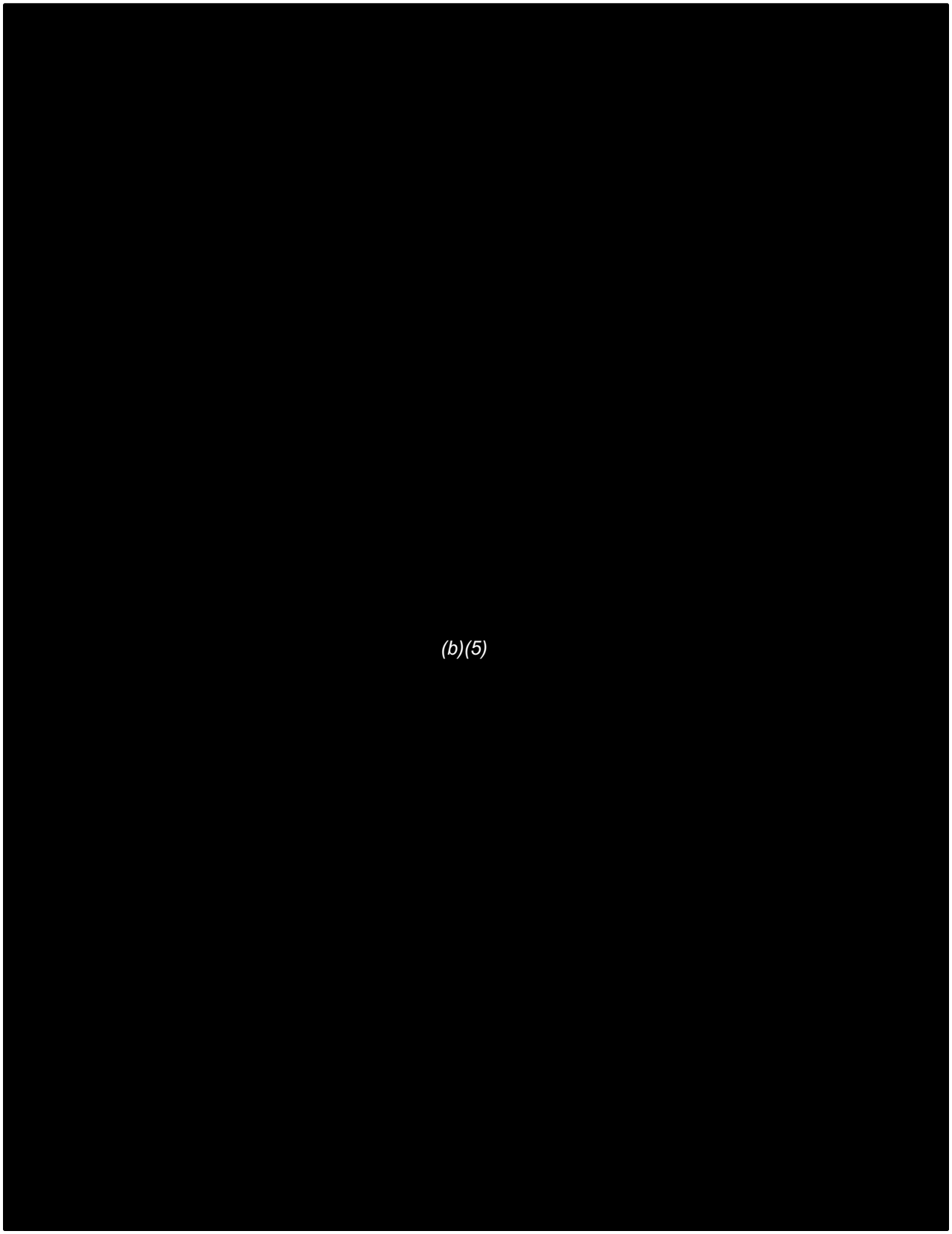
NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 9, 2018



Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 8, 2018 4:10 PM
To:	Mark Graff NOAA Federal
Cc:	Robert Swisher NOAA Federal; _OCIO GPD
Subject:	Re: Oral Arguments in Sierra Club FOIA lawsuit (view live)

Thanks, Mark! We'll be done with our NOAA1200 CRB by then and looking for some entertainment!

On Thu, Mar 8, 2018 at 3:58 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

> Hey Guys,
>
> In case you guys wanted to watch, Oral Arguments are scheduled in the Sierra Club litigation in the 9th Circuit on March 15 at 1:45 ET. It's not common to have oral arguments in a FOIA case, so thought you guys might want to watch. Bogo says you should be able to watch the arguments live at the second link below. The first link is the notice of the oral argument.
>
> https://www.ca9.uscourts.gov/calendar/view.php?caseno_17-16560
>
> **Sierra Club, Inc. v. U.S. Fish and Wildlife Serv.** - The U.S. Fish and Wildlife Service and National Marine Fisheries Service appeal the district court's judgment in a Freedom of Information Act action brought by the Sierra Club, Inc. seeking documents related to a proposed Clean Water Act regulation. [3:15-cv-05872-EDL]
>
> https://www.ca9.uscourts.gov/media/live_oral_arguments.php
>
> Mark H. Graff
> FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> National Oceanic and Atmospheric Administration
> (301) 628 5658 (O)
> (b)(6) (C)
>
> Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell (b)(6)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 8, 2018 4:11 PM
To:	Mark Graff NOAA Federal
Subject:	Re: Oral Arguments in Sierra Club FOIA lawsuit (view live)

And BOGO, not buy one get one free, what?

On Thu, Mar 8, 2018 at 4:10 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Thanks, Mark! We'll be done with our NOAA1200 CRB by then and looking for some entertainment!
>
> On Thu, Mar 8, 2018 at 3:58 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
>
> > Hey Guys,
> >
> > In case you guys wanted to watch, Oral Arguments are scheduled in the Sierra Club litigation in the 9th Circuit on March 15 at 1:45 ET. It's not common to have oral arguments in a FOIA case, so thought you guys might want to watch. Bogo says you should be able to watch the arguments live at the second link below. The first link is the notice of the oral argument.
> >
> > https://www.ca9.uscourts.gov/calendar/view.php?caseno_17-16560
> >
> > **Sierra Club, Inc. v. U.S. Fish and Wildlife Serv.** - The U.S. Fish and Wildlife Service and National Marine Fisheries Service appeal the district court's judgment in a Freedom of Information Act action brought by the Sierra Club, Inc. seeking documents related to a proposed Clean Water Act regulation. [3:15-cv-05872-EDL]
> >
> > https://www.ca9.uscourts.gov/media/live_oral_arguments.php
> >
> > Mark H. Graff
> > FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> > National Oceanic and Atmospheric Administration
> > (301) 628 5658 (O)
> > (b)(6) (C)
> >
> > Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell [redacted]

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, March 8, 2018 4:12 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Oral Arguments in Sierra Club FOIA lawsuit (view live)

Mike BOGOmolny. It's his last name. There are 2 Mike's we work with, and Bogo is way easier than a 4 syllable last name. Even he calls himself Bogo.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Thu, Mar 8, 2018 at 4:10 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> And BOGO, not buy one get one free, what?
>
> On Thu, Mar 8, 2018 at 4:10 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Thanks, Mark! We'll be done with our NOAA1200 CRB by then and looking for some entertainment!
> >
> > On Thu, Mar 8, 2018 at 3:58 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
> >
> > > Hey Guys,
> > >
> > > In case you guys wanted to watch, Oral Arguments are scheduled in the Sierra Club litigation in the 9th Circuit on March 15 at 1:45 ET. It's not common to have oral arguments in a FOIA case, so thought you guys might want to watch. Bogo says you should be able to watch the arguments live at the second link below. The first link is the notice of the oral argument.
> > >
> > > https://www.ca9.uscourts.gov/calendar/view.php?caseno_17-16560
> > >
> > > **Sierra Club, Inc. v. U.S. Fish and Wildlife Serv.** - The U.S. Fish and Wildlife Service and National Marine Fisheries Service appeal the district court's judgment in a Freedom of Information Act action brought by the Sierra Club, Inc. seeking documents related to a proposed Clean Water Act regulation. [3:15-cv-05872-EDL]
> > >
> > > https://www.ca9.uscourts.gov/media/live_oral_arguments.php
> > >
> > > Mark H. Graff
> > > FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> > > National Oceanic and Atmospheric Administration
> > > (301) 628 5658 (O)
> > > (b)(6) (C)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell (b)(6)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, March 8, 2018 4:12 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Oral Arguments in Sierra Club FOIA lawsuit (view live)

He's the Section Chief for GC Info Law at DOC.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Thu, Mar 8, 2018 at 4:10 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> And BOGO, not buy one get one free, what?
>
> On Thu, Mar 8, 2018 at 4:10 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Thanks, Mark! We'll be done with our NOAA1200 CRB by then and looking for some entertainment!
> >
> > On Thu, Mar 8, 2018 at 3:58 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
> >
> > > Hey Guys,
> > >
> > > In case you guys wanted to watch, Oral Arguments are scheduled in the Sierra Club litigation in the 9th Circuit on March 15 at 1:45 ET. It's not common to have oral arguments in a FOIA case, so thought you guys might want to watch. Bogo says you should be able to watch the arguments live at the second link below. The first link is the notice of the oral argument.
> > >
> > > https://www.ca9.uscourts.gov/calendar/view.php?caseno_17-16560
> > >
> > > **Sierra Club, Inc. v. U.S. Fish and Wildlife Serv.** - The U.S. Fish and Wildlife Service and National Marine Fisheries Service appeal the district court's judgment in a Freedom of Information Act action brought by the Sierra Club, Inc. seeking documents related to a proposed Clean Water Act regulation. [3:15-cv-05872-EDL]
> > >
> > > https://www.ca9.uscourts.gov/media/live_oral_arguments.php
> > >
> > > Mark H. Graff
> > > FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> > > National Oceanic and Atmospheric Administration
> > > (301) 628 5658 (O)
> > > (b)(6) (C)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell (b)(6)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 8, 2018 4:21 PM
To:	Mark Graff NOAA Federal
Subject:	Re: Oral Arguments in Sierra Club FOIA lawsuit (view live)

Yes, that's right, you were talking about him planning to read the riot act to those folks . . . .

On Thu, Mar 8, 2018 at 4:12 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

> He's the Section Chief for GC Info Law at DOC.
>
> Mark H. Graff
> FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> National Oceanic and Atmospheric Administration
> (301) 628 5658 (O)
> (b)(6) (C)
>
> Confidentiality Notice: This e mail message is intended only for the named recipients. It contains information that may be confidential, privileged, attorney work product, or otherwise exempt from disclosure under applicable law. If you have received this message in error, are not a named recipient, or are not the employee or agent responsible for delivering this message to a named recipient, be advised that any review, disclosure, use, dissemination, distribution, or reproduction of this message or its contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.
>
> On Thu, Mar 8, 2018 at 4:10 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > And BOGO, not buy one get one free, what?
> >
> > On Thu, Mar 8, 2018 at 4:10 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> >
> > > Thanks, Mark! We'll be done with our NOAA1200 CRB by then and looking for some entertainment!
> > >
> > > On Thu, Mar 8, 2018 at 3:58 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
> > >
> > > > Hey Guys,
> > > >
> > > > In case you guys wanted to watch, Oral Arguments are scheduled in the Sierra Club litigation in the 9th Circuit on March 15 at 1:45 ET. It's not common to have oral arguments in a FOIA case, so thought you guys might want to watch. Bogo says you should be able to watch the arguments live at the second link below. The first link is the notice of the oral argument.
> > > >
> > > > https://www.ca9.uscourts.gov/calendar/view.php?caseno_17-16560
> > > >
> > > > **Sierra Club, Inc. v. U.S. Fish and Wildlife Serv.** - The U.S. Fish and Wildlife Service and National Marine Fisheries Service appeal the district court's judgment in a Freedom of Information Act action brought by the Sierra Club, Inc. seeking documents related to a proposed Clean Water Act regulation. [3:15-cv-05872-EDL]
> > > >
> > > > https://www.ca9.uscourts.gov/media/live_oral_arguments.php
> > > >
> > > > Mark H. Graff
> > > > FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> > > > National Oceanic and Atmospheric Administration
> > > > (301) 628 5658 (O)
> > > > (b)(6)

[redacted] (C)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell [redacted]

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell [redacted]

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Cell [redacted]

James Cooperman - NOAA Affiliate

From:	James Cooperman NOAA Affiliate
Sent:	Friday, March 9, 2018 9:04 AM
To:	Sarah Brabson NOAA Federal; John D. Parker NOAA Federal; Jonathan Gordon NOAA Federal; Mark Graff NOAA Federal; Cheryl Marlin NOAA Federal
Subject:	Re: Status of signatures on NOAA6602 PIA and PTA? thx
Attachments:	NOAA6602 PIA_V4 03 08 2018 JC JA JP CLM.pdf; NOAA6602 PTA_V2 03 08 2018 JC JA JP CLM.pdf

Sarah

Attached please find the signed PDF and Signed PIA for Mark's review and approval.

Thank You

Jim Cooperman

James Cooperman CTR
Information System Security Office
Office of National Marine Sanctuaries
Desk 240-533-0680
Cell (b)(6)

On Thu, Mar 8, 2018 at 4:21 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> On Thu, Mar 8, 2018 at 1:18 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> How are you doing on signatures, Jim, and again, hope John signed. He can take the longest.
>
> On Thu, Mar 8, 2018 at 10:41 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> Did you send to John? Thx
>
> Sent from my iPhone
>
> On Mar 8, 2018, at 10:07 AM, James Cooperman NOAA Affiliate <james.cooperman@noaa.gov> wrote:

I've already sent the PIA and PTA to the AO and SO. I hope to have them signed by noon.

Jim

James Cooperman CTR
Information System Security Office
Office of National Marine Sanctuaries
Desk 240-533-0680
Cell (b)(6)

On Thu, Mar 8, 2018 at 10:02 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Thanks, John. I sent you and Jim the NOAA6602 PIA for signatures this am, and Jim already had the PIA to circulate for signatures. So I sincerely hope that we can get NOS signatures asap . .
>
> I also sent what i think is the last version of NOAA6702 to Russell this am.
>
> On Thu, Mar 8, 2018 at 9:59 AM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:
>
> > Hi Sarah,
> >
> > Our goal is to have the AO and Co AO sign the ATO memorandums by their current ATO expiration dates as stated in CSAM. NOAA6702 ATO approval will be after the current ATO expiration date due to delays in completing the independent assessment. NOAA6602 has completed independent assessment and awaiting PIA/PTA approval from NOAA and DOC before ATO approval.
> >
> > The ATO memos have been drafted by me and shared with the ISSOs for each system. They have been informed of the DOC Privacy Officer role in approving the PTA/PIA prior to the ATO approval.
> >
> > I hope this answers your question.
> > John
> >
> > --
> >
> > John D. Parker, CISSP, CISA <John.D.Parker@noaa.gov>
> > NOS IT Security Officer
> > DOC/NOAA/NOS IMO240-533-0832 (office (b)(6) (mobile)
> > Email NOS IT security inquires: NOS.ITSP@noaa.gov

On 3/5/2018 11:07 AM, Sarah Brabson NOAA Federal wrote:

> Okay. We need to have CRBs for these two systems, and get DOC approval, before the new ATOs are signed. I want to be able to tell DOC what exact dates we're looking at for the ATO signings. Sometimes the ATOs are signed a few days before the dates set in CSAM. If we can avoid any early signings, we'll have the "maximum" time for obtaining DOC approval.
>
> Capisce? thx Sarah
>
> On Mon, Mar 5, 2018 at 11:03 AM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:
>> Hi Sarah,
>>
>> I am not sure I understand your email below. Please clarify.
>>
>> Thanks,
>> John
>>
>> --
>>
>> John D. Parker, CISSP, CISA <John.D.Parker@noaa.gov>
>> NOS IT Security Officer
>> DOC/NOAA/NOS IMO240-533-0832 (office (b)(6) (mobile)
>> Email NOS IT security inquires: NOS.ITSP@noaa.gov
>>
>> On 3/5/2018 10:49 AM, Sarah Brabson NOAA Federal wrote:
>>
>>> And these are systems for which we should not do early signatures if at all avoidable. We will need every day possible.
>>>
>>> I let DOC know we'll have PIAs for them very shortly . . .
>>>
>>> thx Sarah
>>>
>>> Sarah D. Brabson
>>> IT Infrastructure Investment Program Manager
>>> PRA Clearance Officer
>>>
>>> Governance and Portfolio Division
>>> Office 301 628 5751
>>> Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, March 9, 2018 9:16 AM
To:	Mark Graff NOAA Federal
Subject:	NOAA6602 PIA and PTA for your signature!
Attachments:	NOAA6602 PIA_V4 03 08 2018 JC JA JP CLM.pdf; NOAA6602 PTA_V2 03 08 2018 JC JA JP CLM.pdf

Mark, if you have time today, could you sign these two docs? The PIA you had cleared for signatures and the PTA is based on and congruent with the PIA.

Forwarded message
From: **James Cooperman - NOAA Affiliate** <james.cooperman@noaa.gov>
Date: Fri, Mar 9, 2018 at 9:03 AM
Subject: Re: Status of signatures on NOAA6602 PIA and PTA? thx
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, "John D. Parker NOAA Federal" <john.d.parker@noaa.gov>, Jonathan Gordon NOAA Federal <Jonathan.Gordon@noaa.gov>, Mark Graff NOAA Federal <mark.graff@noaa.gov>, Cheryl Marlin NOAA Federal <cheryl.marlin@noaa.gov>

Sarah

Attached please find the signed PDF and Signed PIA for Mark's review and approval.

Thank You

Jim Cooperman

James Cooperman CTR
Information System Security Office
Office of National Marine Sanctuaries
Desk 240-533-0680
Cell (b)(6)

ires: NOS.ITSP@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Friday, March 9, 2018 9:42 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA6602 PIA and PTA for your signature!
Attachments:	NOAA6602 PIA_V4 03 08 2018 JC JA JP CLM mhg.pdf; NOAA6602 PTA_V2 03 08 2018 JC JA JP CLM mhg.pdf

Here you go

Out of curiosity, who is Marlin Lee (the 5th signator) on these docs? Is she the Co Authorizing official? Just wondering why more than the ITSO, ISSO, AO, and BCPO signatures are needed.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Fri, Mar 9, 2018 at 9:15 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, if you have time today, could you sign these two docs? The PIA you had cleared for signatures and the PTA is based on and congruent with the PIA.
>
> Forwarded message
> From: **James Cooperman - NOAA Affiliate** <james.cooperman@noaa.gov>
> Date: Fri, Mar 9, 2018 at 9:03 AM
> Subject: Re: Status of signatures on NOAA6602 PIA and PTA? thx
> To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, "John D. Parker NOAA Federal" <john.d.parker@noaa.gov>, Jonathan Gordon NOAA Federal <Jonathan.Gordon@noaa.gov>, Mark Graff NOAA Federal <mark.graff@noaa.gov>, Cheryl Marlin NOAA Federal <cheryl.marlin@noaa.gov>
>
> Sarah
>
> Attached please find the signed PDF and Signed PIA for Mark's review and approval.
>
> Thank You
>
> Jim Cooperman

James Cooperman CTR
Information System Security Office
Office of National Marine Sanctuaries
Desk 240-533-0680
Cell (b)(6)

ires: NOS.ITSP@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Impact Assessment
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose identified in Section 4

OSPREY

An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

e) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

FROM NOAA-12: The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.

FROM DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531 332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533 535; 44 U.S.C. 3101; Equal Employment Actof 1972; and all existing, applicable Department policies, and regulations.

FROM DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

FROM: OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

FROM OPM/GOVT-5: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

FROM DEPT-29: Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95. The system is also authorized by the U.S. Office of Management & Budget (OMB)

Circular A 130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq*. (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112 95); the American Fisheries Act, Title II, Public Law 105 277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101 5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951 961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq*. (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431 2444; the Marine Mammal Protection Act, 16 U.S.C. 1361; and the Debt Collection Improvement Act, 31 U.S.C. 7701.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

ONMS is a FIPS 199 Moderate Security risk.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS has developed a new permit application that collects non-sensitive PII; ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	

s. Other general personal data (specify):
The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work related data section.
The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			

i. Other work-related data (specify):
The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	

j. Other distinguishing features/biometrics (specify):
ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	

g. Other system administration/audit data (specify)
The NOAA6602 OSPREY application uses the NOAA LDAP to authenticate the permit coordinators. Only ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator

access is sent to NOAA ArcSight. ArcSight records User ID and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

2.3 Describe how the accuracy of the information in the system is ensured.

OSPREY

The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions

Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity.

For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport. HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0141, National Marine Sanctuary Permits
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

UAS Only Although the ONMS UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): ONMS Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics).			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking are stored temporarily during the hiring phase, including, standard HR information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number. The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS

ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

OSPREY

1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits fall into this category. This category also includes requests for authorizations of other agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

- The disposal of cremated human remains by a commercial operator in any national marine sanctuary
- The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
- The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
- The discharge and immediate recovery of objects related to special effects of motion pictures; and
- The continued presence of submarine cables beneath or on the seabed.

(d) Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

(e) Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

(f) Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

(g) Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

(h) Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish

to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research Only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

Collected from the public.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.

There is a potential for unauthorized access to the system, which would expose non-sensitive PII to an unauthorized user.

Old data is purged from the systems per retention schedule.

Users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the

PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Includes instances of security or privacy breach.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/management/permits/welcome.html

X	Yes, notice is provided by other means.	Specify how: **OSPREY: see above link to site with PAS.** **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR:** Applicants and employees: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of

their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information, **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information

		through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **Acquisition** Procurement information within NOAA6602 is not monitored or tracked. It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. **HR** Employee evaluations and potential employee resumes are not monitored, tracked, or recorded within NOAA6602. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONMS Permit application (OSPREY) is hosted on a data base. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution. Audit solution.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access controlled file cabinet.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants. DEPT-13, Investigative and Security Records. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-29, Unmanned Aircraft Systems; OPM/GOVT-1, General

	Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse

	effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: There is no sensitive data.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgrade the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the assessment. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: James Cooperman Office: National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:24:28 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: National Ocean Service Phone: 240-533-0832 Email: john.d.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:51 -05'00' Date signed:
Authorizing Official Name: John Armor Office: National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:22:31 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graph Office: NOAA Phone: 301-628-5751 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:39:27 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:48:42 05'00'

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS has developed a new permit application that collects non-sensitive PII; ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

OSPREY

In order to issue permits for research within our sanctuaries the ONMS Permit system (OSPREY) will collect minimal non-sensitive PII. This will include Name, Business or School Address, Email address and phone number. There is potential for an applicant to provide home address, home phone and personal email instead of business as requested.

HR Data

ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

UAS

The ONMS UAS has the potential to inadvertently capture PII.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc… alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, March 9, 2018 9:49 AM
To:	James Cooperman; John D. Parker; Jonathan M. Gordon
Cc:	Cheryl Marlin; Mark Graff NOAA Federal
Subject:	Fwd: NOAA6602 PIA and PTA for your signature!
Attachments:	NOAA6602 PIA_V4 03 08 2018 JC JA JP CLM mhg.pdf; NOAA6602 PTA_V2 03 08 2018 JC JA JP CLM mhg.pdf; PIA CRB Risk Analysis Guide.docx

I will now send these to DOC and see when they can squeeze this in for a Compliance Review (phone conference after they have completed their first review).

Jim, here's the Risk Analysis Guide from which DOC chooses one or more questions from one or more of the areas.

thx Sarah

Forwarded message
From: **Mark Graff - NOAA Federal** <mark.graff@noaa.gov>
Date: Fri, Mar 9, 2018 at 9:42 AM
Subject: Re: NOAA6602 PIA and PTA for your signature!
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>

Here you go

On Fri, Mar 9, 2018 at 9:15 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, if you have time today, could you sign these two docs? The PIA you had cleared for signatures and the PTA is based on and congruent with the PIA.
>
> Forwarded message
> From: **James Cooperman - NOAA Affiliate** <james.cooperman@noaa.gov>
> Date: Fri, Mar 9, 2018 at 9:03 AM
> Subject: Re: Status of signatures on NOAA6602 PIA and PTA? thx
> To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, "John D. Parker NOAA Federal" <john.d.parker@noaa.gov>, Jonathan Gordon NOAA Federal <Jonathan.Gordon@noaa.gov>, Mark Graff NOAA Federal <mark.graff@noaa.gov>, Cheryl Marlin NOAA Federal <cheryl.marlin@noaa.gov>

Sarah

Attached please find the signed PDF and Signed PIA for Mark's review and approval.

Thank You

Jim Cooperman

James Cooperman CTR
Information System Security Office
Office of National Marine Sanctuaries
Desk 240-533-0680
Cell (b)(6)

ires: NOS.ITSP@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Impact Assessment
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose identified in Section 4

OSPREY

An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

e) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

FROM NOAA-12: The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.

FROM DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531 332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533 535; 44 U.S.C. 3101; Equal Employment Actof 1972; and all existing, applicable Department policies, and regulations.

FROM DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

FROM: OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

FROM OPM/GOVT-5: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

FROM DEPT-29: Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95. The system is also authorized by the U.S. Office of Management & Budget (OMB)

Circular A 130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq*. (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112 95); the American Fisheries Act, Title II, Public Law 105 277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101 5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951 961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq*. (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431 2444; the Marine Mammal Protection Act, 16 U.S.C. 1361; and the Debt Collection Improvement Act, 31 U.S.C. 7701.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

ONMS is a FIPS 199 Moderate Security risk.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS has developed a new permit application that collects non-sensitive PII; ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	

s. Other general personal data (specify):
The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work related data section.
The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			

i. Other work-related data (specify):
The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	

j. Other distinguishing features/biometrics (specify):
ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	

g. Other system administration/audit data (specify)
The NOAA6602 OSPREY application uses the NOAA LDAP to authenticate the permit coordinators. Only ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator

access is sent to NOAA ArcSight. ArcSight records User ID and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

2.3 Describe how the accuracy of the information in the system is ensured.

OSPREY

The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions

Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity.

For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport. HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0141, National Marine Sanctuary Permits
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

UAS Only Although the ONMS UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): ONMS Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics).			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking are stored temporarily during the hiring phase, including, standard HR information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number. The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS

ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

OSPREY

1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits fall into this category. This category also includes requests for authorizations of other agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

- The disposal of cremated human remains by a commercial operator in any national marine sanctuary
- The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
- The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
- The discharge and immediate recovery of objects related to special effects of motion pictures; and
- The continued presence of submarine cables beneath or on the seabed.

(d) Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

(e) Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

(f) Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

(g) Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

(h) Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish

to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research Only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

Collected from the public.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.

There is a potential for unauthorized access to the system, which would expose non-sensitive PII to an unauthorized user.

Old data is purged from the systems per retention schedule.

Users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the

PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Includes instances of security or privacy breach.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/management/permits/welcome.html

X	Yes, notice is provided by other means.	Specify how: **OSPREY: see above link to site with PAS.** **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR:** Applicants and employees: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of

their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information, **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information

		through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **Acquisition** Procurement information within NOAA6602 is not monitored or tracked. It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. **HR** Employee evaluations and potential employee resumes are not monitored, tracked, or recorded within NOAA6602. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONMS Permit application (OSPREY) is hosted on a data base. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution. Audit solution.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access controlled file cabinet.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants. DEPT-13, Investigative and Security Records. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-29, Unmanned Aircraft Systems; OPM/GOVT-1, General

	Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse

	effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: There is no sensitive data.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgrade the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the assessment. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: James Cooperman Office: National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:24:28 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: National Ocean Service Phone: 240-533-0832 Email: john.d.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:51 -05'00' Date signed:
Authorizing Official Name: John Armor Office: National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:22:31 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graph Office: NOAA Phone: 301-628-5751 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:39:27 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:48:42 05'00'

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS has developed a new permit application that collects non-sensitive PII; ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

OSPREY

In order to issue permits for research within our sanctuaries the ONMS Permit system (OSPREY) will collect minimal non-sensitive PII. This will include Name, Business or School Address, Email address and phone number. There is potential for an applicant to provide home address, home phone and personal email instead of business as requested.

HR Data

ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

UAS

The ONMS UAS has the potential to inadvertently capture PII.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc… alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Privacy Impact Assessment Compliance Review Board
Risk Analysis Guide
(Date of Meeting)

Name of IT System:
Authorization to Operate (ATO) date:
ATO expiration date:

A Privacy Threshold Analysis (PTA) must be completed for a system processing PII/BII in order to determine if a Privacy Impact Assessment (PIA) is required. The purposes of a PIA are to ensure effective compliance with the Privacy Act for notice and disclosure and to confirm appropriate privacy protections are in place. The following critical areas will be discussed during this meeting:

- System/Data characterization
  - System location/Status
  - Type/Sources of information
  - Purpose/Use of information
  - Retention of information
  - Legal authority
  - FIPS 199 security impact category
  - Notice and consent
  - Records retrieval
  - System of records notice(s)
  - NIST SP 800-122 PII confidentiality impact level
- Information Sharing Practices
  - Access
  - Computer Matching Program
  - Connection with other IT systems
- Website/Mobile application processes
  - Website(s)
  - Website privacy policy/Privacy Act statement
  - Mobile application(s)
  - Tracking technologies
- Status of privacy controls
  - Plan of Action and Milestones
  - IT Security controls
- Risk Assessment Review
  - Threats and vulnerabilities
  - Summary risk

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, March 9, 2018 9:57 AM
To:	Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO; Toland, Michael
Cc:	Mark Graff NOAA Federal
Subject:	NOAA6602 PIA and PTA for review
Attachments:	NOAA6602 PTA_V2 03 08 2018 JC JA JP CLM mhg.pdf; NOAA6602 PIA_V4 03 08 2018 JC JA JP CLM mhg.pdf

Kathy, I sent you the Word PIA yesterday in case anyone had time to start review.

Mark and I had thought that the ATO date would be 3 30 18, but John Parker clarified a couple of days ago that it's the 16th. As often happens, it took longer than it should, for these documents to be in shape for signatures.

(b)(5)

So, we apologize for the very last minute submission!!

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Impact Assessment
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose identified in Section 4

OSPREY

An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

e) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

FROM NOAA-12: The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.

FROM DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531 332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533 535; 44 U.S.C. 3101; Equal Employment Actof 1972; and all existing, applicable Department policies, and regulations.

FROM DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

FROM: OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

FROM OPM/GOVT-5: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

FROM DEPT-29: Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95. The system is also authorized by the U.S. Office of Management & Budget (OMB)

Circular A 130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq*. (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112 95); the American Fisheries Act, Title II, Public Law 105 277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101 5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951 961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq*. (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431 2444; the Marine Mammal Protection Act, 16 U.S.C. 1361; and the Debt Collection Improvement Act, 31 U.S.C. 7701.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

ONMS is a FIPS 199 Moderate Security risk.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS has developed a new permit application that collects non-sensitive PII; ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	

s. Other general personal data (specify):
The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work related data section.
The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			

i. Other work-related data (specify):
The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	

j. Other distinguishing features/biometrics (specify):
ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	

g. Other system administration/audit data (specify)
The NOAA6602 OSPREY application uses the NOAA LDAP to authenticate the permit coordinators. Only ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator

access is sent to NOAA ArcSight. ArcSight records User ID and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

2.3 Describe how the accuracy of the information in the system is ensured.

OSPREY

The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions

Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity.

For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport. HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0141, National Marine Sanctuary Permits
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

UAS Only Although the ONMS UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): ONMS Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics).			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking are stored temporarily during the hiring phase, including, standard HR information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number. The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS

ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

OSPREY

1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits fall into this category. This category also includes requests for authorizations of other agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

- The disposal of cremated human remains by a commercial operator in any national marine sanctuary
- The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
- The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
- The discharge and immediate recovery of objects related to special effects of motion pictures; and
- The continued presence of submarine cables beneath or on the seabed.

(d) Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

(e) Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

(f) Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

(g) Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

(h) Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish

to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research Only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

Collected from the public.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.

There is a potential for unauthorized access to the system, which would expose non-sensitive PII to an unauthorized user.

Old data is purged from the systems per retention schedule.

Users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the

PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Includes instances of security or privacy breach.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/management/permits/welcome.html

X	Yes, notice is provided by other means.	Specify how: **OSPREY: see above link to site with PAS.** **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR:** Applicants and employees: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of

their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information, **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information

		through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **Acquisition** Procurement information within NOAA6602 is not monitored or tracked. It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. **HR** Employee evaluations and potential employee resumes are not monitored, tracked, or recorded within NOAA6602. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONMS Permit application (OSPREY) is hosted on a data base. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution. Audit solution.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access controlled file cabinet.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants. DEPT-13, Investigative and Security Records. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-29, Unmanned Aircraft Systems; OPM/GOVT-1, General

	Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse

	effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: There is no sensitive data.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgrade the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the assessment. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: James Cooperman Office: National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:24:28 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: National Ocean Service Phone: 240-533-0832 Email: john.d.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:51 -05'00' Date signed:
Authorizing Official Name: John Armor Office: National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:22:31 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graph Office: NOAA Phone: 301-628-5751 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:39:27 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:48:42 05'00'

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS has developed a new permit application that collects non-sensitive PII; ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

OSPREY

In order to issue permits for research within our sanctuaries the ONMS Permit system (OSPREY) will collect minimal non-sensitive PII. This will include Name, Business or School Address, Email address and phone number. There is potential for an applicant to provide home address, home phone and personal email instead of business as requested.

HR Data

ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

UAS

The ONMS UAS has the potential to inadvertently capture PII.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc… alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, March 9, 2018 1:42 PM
To:	Mark Graff NOAA Federal
Subject:	Fwd: RE NOAA8883 SAR and open POA&Ms
Attachments:	NOAA8883 PR PIA Annual Review Certification 20180305 for MHG signature.pdf; NOAA8883 PR PIA for 2018 certification_needs new signatures v2.docx; NOAA8883 PR PTA 20180307 for MHG signature.pdf

Here's Pete's response to my questions about high findings and cross walk to POA&Ms. The SAR is in the PIA folder (I was referencing Table 5.1)

Here are the PIA, PTA and certification for your signature. I couldn't put my review date into the certification the normal way, it's in a little text box.

Forwarded message
From: **Peter Thoenen - NOAA Federal** <peter.thoenen@noaa.gov>
Date: Tue, Mar 6, 2018 at 6:30 PM
Subject: RE: RE NOAA8883 SAR and open POA&Ms
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>

I found your table:

1 Closed

2 Still open, due in July. Will be changed to due in July 2018 do to unexpected vendor issues; already have this approved I'm just not going ot change it until July in case we can hit the deadline though unexpected

3 Closed

4 Closed

5 Closed

From: Sarah Brabson - NOAA Federal [mailto:sarah.brabson@noaa.gov]
Sent: Tuesday, March 6, 2018 7:14 AM
To: Peter Thoenen - NOAA Federal <peter.thoenen@noaa.gov>
Subject: Re: RE NOAA8883 SAR and open POA&Ms

O (b)(5) [redacted]

[redacted]? thx

On Tue, Mar 6, 2018 at 11:50 AM, Peter Thoenen NOAA Federal <peter.thoenen@noaa.gov> wrote:

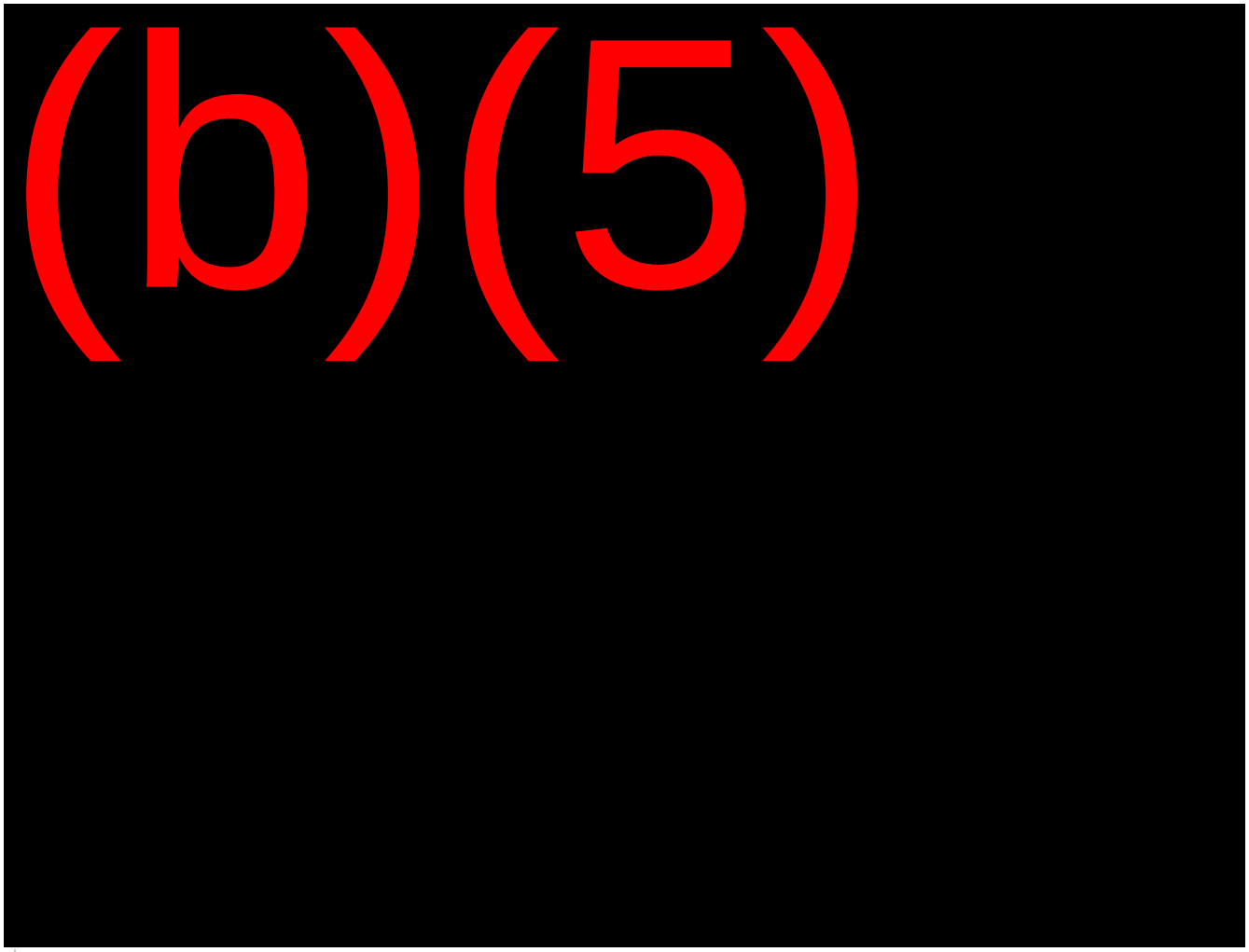
> (b)(5) [redacted] it

On Tue, Mar 6, 2018 at 6:00 AM 1000, "Sarah Brabson NOAA Federal" <sarah.brabson@noaa.gov> wrote:

> Pet (b)(5) [redacted]
>
> [redacted]
>
> [redacted]?
>
> Thanks, Sarah

On Mon, Mar 5, 2018 at 6:42 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> From your PIA: :Please select what best matches for these two questions:



On Mon, Mar 5, 2018 at 5:48 PM, Peter Thoenen NOAA Federal <peter.thoenen@noaa.gov> wrote:

> Attached, see comments inline.

> I don’t think whoever made this new PTA template understands how general support systems function TBH.

Sarah D. Brabson

IT Infrastructure Investment Program Manager

PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751

Ce (b)(6)

Sarah D. Brabson

IT Infrastructure Investment Program Manager

PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751

Ce (b)(6)

Sarah D. Brabson

IT Infrastructure Investment Program Manager

PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751

Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA:_Privacy Impact Assessment for the National Weather Service Pacific Region (NOAA8883)

FISMA Name/ID (if different):

_____

Name of IT System/ Program Owner: Derek Ching_____

Name of Information System Security Officer: Peter Thoenen___

Name of Authorizing Official(s): Ray Tanabe, Rich Varn__

Date of Last PIA Compliance Review Board (CRB): _3/21/2017_____
(This date must be within three (3) years.)

Date of PIA Review:_3/2/2018_____

Name of Reviewer:_Derek Ching_____

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: CHING.DEREK.KK.1232036318 Digitally signed by CHING.DEREK.KK.1232036318 Date: 2018.03.05 12:10:37 10'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _Sarah Brabson___

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Digitally signed by BRABSON.SARAH.1365710488 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BRABSON.SARAH.1365710488 Date: 2018.03.09 13:30:38 -05'00'

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO):_____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer:

_____

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Version Number: 01-2017

U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the
National Weather Service Pacific Region
(FISMA ID NOAA8883)

U.S. Department of Commerce Privacy Threshold Analysis

National Oceanic and Atmospheric Administration National Weather Service Pacific Region (FISMA ID NOAA8883)

Unique Project Identifier: 006-00035110400-48-02-00-02-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer.

Description of the information system and its purpose: The National Weather Service (NWS) Pacific Region (FIMSA ID: NOAA8883) information technology general support system is composed of various field and headquarter office[1] local area networks (LANs) and their directly connected information systems such as workstations, servers, printers, etc. which are linked together by a wide area network[2] (WAN) used to support weather forecasting throughout the Pacific Ocean. The system is primarily used to provide administrative support and supplemental operational services and specifically excludes from its accreditation boundary systems deemed as major applications or programs of records as well as various partner systems, though transit may be provided in some cases.

As a course of operations contact information is collected on local Federal employees to support emergency contact rosters. In addition, various amounts of work related information as well as basic personal information is collect on employee's to support day-to-day administrative efforts such as travel documents, performance plans, in and out processing of new and current employees, system user accounts, procurement records, etc. and are stored by the employees themselves and as well as various support staff such as supervisor or administrative assistants, in addition to automatic collection by IT staff and system logs as part of day-to-day operation and maintenance such as usernames, addresses, system and network activity logging, etc.

Various amount of PII to establish identity such as passport numbers, nationality, contact information, etc. are collected from foreign national visitors and guests on a transitory basis and

[1] RHQ Pacific Region (Honolulu, HI), WFO Honolulu (Honolulu, HI), WFO Guam (Barrigada, GU), WSO Pago Pago (Pago Pago, AS), DCO Lihue (Lihue, HI), and DCO Hilo (Hilo, HI)

[2] The NWS PR interconnects with NWS Enterprise Mission Enabling System for centralized user authentication, National Oceanic and Atmospheric Administration Corporate Services for audit collection of automated information technology records such as computer application security logs, and NWS Advanced Weather Interactive Processing, and NWS Weather and Climate Computing Infrastructure Services as its WAN provider.

transmitted to the applicable security office for building and installation access as well as for the purpose of protecting deemed exports and controlled technology.

Federal civil servants and private contractors under contract with the NWS working on behalf of the Pacific Region access parts of the system in support of its mission. Select PII is shared with Department of the Defense Joint Base Pearl Harbor-Hickam Pass and ID Office, the Department of Commerce Western Region Security Office, and various National Oceanic and Atmosphere Administration administrative offices such as Human Resources or Finance as applicable.

This system is classified as a moderate system under the Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X_ DOC employees
__X_ Contractors working on behalf of DOC
__X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a PIA must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the National Weather Service Pacific Region and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or Information System Owner:

CHING.DEREK.KK.1232036318

Digitally signed by CHING.DEREK.KK.1232036318
Date: 2018.03.08 08:22:32 10'00'

Information Technology Security Officer:

BROWNE.ANDREW.PATRICK.1472149349

Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.03.08 11:39:38 -05'00'

Authorizing Official:

TANABE.RAYMOND.M.1365894449

Digitally signed by TANABE.RAYMOND.M.1365894449
Date: 2018.03.08 08:56:19 10'00'

Bureau Chief Privacy Officer:

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Friday, March 9, 2018 5:32 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Re NOAA8883 the email I sent you earlier also has the three certification docs for your signature
Attachments:	NOAA8883 PR PIA Annual Review Certification 20180305 for MHG signature mhg.pdf; NOAA8883 PR PTA 20180307 for MHG signature mhg.pdf

Here is the certification form and the PTA. However, the PIA on your last email was in word format and didn't have the signatures of the ITSO, ISSO, and AO. Is the signed version on its way?

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Fri, Mar 9, 2018 at 4:33 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Should have changed the email subject.
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA:_Privacy Impact Assessment for the National Weather Service Pacific Region (NOAA8883)

FISMA Name/ID (if different):

_____

Name of IT System/ Program Owner: Derek Ching_____

Name of Information System Security Officer: Peter Thoenen___

Name of Authorizing Official(s): Ray Tanabe, Rich Varn__

Date of Last PIA Compliance Review Board (CRB): _3/21/2017_____
(This date must be within three (3) years.)

Date of PIA Review:_3/2/2018_____

Name of Reviewer:_Derek Ching_____

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: CHING.DEREK.KK.1232036318 Digitally signed by CHING.DEREK.KK.1232036318 Date: 2018.03.05 12:10:37 10'00'

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _Sarah Brabson___

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Digitally signed by BRABSON.SARAH.1365710488 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BRABSON.SARAH.1365710488 Date: 2018.03.09 13:30:38 -05'00'

Date of BCPO Review: 3/9/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer:

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.03.09 17:28:42 05'00'

Version Number: 01-2017

U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the
National Weather Service Pacific Region
(FISMA ID NOAA8883)

U.S. Department of Commerce Privacy Threshold Analysis

National Oceanic and Atmospheric Administration National Weather Service Pacific Region (FISMA ID NOAA8883)

Unique Project Identifier: 006-00035110400-48-02-00-02-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer.

Description of the information system and its purpose: The National Weather Service (NWS) Pacific Region (FIMSA ID: NOAA8883) information technology general support system is composed of various field and headquarter office[1] local area networks (LANs) and their directly connected information systems such as workstations, servers, printers, etc. which are linked together by a wide area network[2] (WAN) used to support weather forecasting throughout the Pacific Ocean. The system is primarily used to provide administrative support and supplemental operational services and specifically excludes from its accreditation boundary systems deemed as major applications or programs of records as well as various partner systems, though transit may be provided in some cases.

As a course of operations contact information is collected on local Federal employees to support emergency contact rosters. In addition, various amounts of work related information as well as basic personal information is collect on employee's to support day-to-day administrative efforts such as travel documents, performance plans, in and out processing of new and current employees, system user accounts, procurement records, etc. and are stored by the employees themselves and as well as various support staff such as supervisor or administrative assistants, in addition to automatic collection by IT staff and system logs as part of day-to-day operation and maintenance such as usernames, addresses, system and network activity logging, etc.

Various amount of PII to establish identity such as passport numbers, nationality, contact information, etc. are collected from foreign national visitors and guests on a transitory basis and

[1] RHQ Pacific Region (Honolulu, HI), WFO Honolulu (Honolulu, HI), WFO Guam (Barrigada, GU), WSO Pago Pago (Pago Pago, AS), DCO Lihue (Lihue, HI), and DCO Hilo (Hilo, HI)

[2] The NWS PR interconnects with NWS Enterprise Mission Enabling System for centralized user authentication, National Oceanic and Atmospheric Administration Corporate Services for audit collection of automated information technology records such as computer application security logs, and NWS Advanced Weather Interactive Processing, and NWS Weather and Climate Computing Infrastructure Services as its WAN provider.

transmitted to the applicable security office for building and installation access as well as for the purpose of protecting deemed exports and controlled technology.

Federal civil servants and private contractors under contract with the NWS working on behalf of the Pacific Region access parts of the system in support of its mission. Select PII is shared with Department of the Defense Joint Base Pearl Harbor-Hickam Pass and ID Office, the Department of Commerce Western Region Security Office, and various National Oceanic and Atmosphere Administration administrative offices such as Human Resources or Finance as applicable.

This system is classified as a moderate system under the Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X_ DOC employees
__X_ Contractors working on behalf of DOC
__X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a PIA must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the National Weather Service Pacific Region and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or Information System Owner:

CHING.DEREK.KK.1232036318

Digitally signed by CHING.DEREK.KK.1232036318
Date: 2018.03.08 08:22:32 10'00'

Information Technology Security Officer:

BROWNE.ANDREW.PATRICK.1472149349

Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.03.08 11:39:38 -05'00'

Authorizing Official:

TANABE.RAYMOND.M.1365894449

Digitally signed by TANABE.RAYMOND.M.1365894449
Date: 2018.03.08 08:56:19 10'00'

Bureau Chief Privacy Officer:

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.03.09 17:29:51 -05'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, March 12, 2018 12:42 PM
To:	Russell Worman
Cc:	John D. Parker; John Kaperick; Mark Graff NOAA Federal
Subject:	Re NOAA6702 I updated the PTA to match the PIA, pls see attached!
Attachments:	NOAA6702 PTA 031218 for signatures.docx

Russ, I started emailing you to check on signature status for the PIA.

But looking at the PTA, it needs to be redone to agree with the PIA. I've put it into the new template, if you can also circulate for signatures.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Purvis, Catrina (Federal)

Subject:	CRB NOAA6602
Location:	Open Office 52017 (SMC) Md Conf Rm dial in information is (b)(6) [redacted]
Start:	Thursday, March 15, 2018 9:00 AM
End:	Thursday, March 15, 2018 9:30 AM
Recurrence:	(none)
Meeting Status:	Not yet responsed
Organizer:	Purvis, Catrina (Federal)
Attachments:	NOAA6602 PTA_V2 03 08 2018 JC JA JP CLM mhg.pdf; NOAA6602 PIA_V4 03 08 2018 JC JA JP CLM mhg.pdf

Mark/Sarah

Please ensure all PIAs/PTAs are submitted to OCIO to obtain system security concurrence. Ensure all required attendees are present at this telecom (dial in information (b)(6) [redacted] meeting, such as the ITSO, System Owner, etc., and other attendees who are able to respond to questions related to the systems identified above.

Also, if any of the systems are classified, please provide a hard copy of the SARs and POA&Ms for each system identified above to Catrina Purvis 2 days prior to the meeting date.

Warm Regards,

Dorrie Ferguson,
Management and Program Analyst
Office of Privacy & Open Government
Error! Hyperlink reference not valid.
Office: (202) 482-8157

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Impact Assessment
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose identified in Section 4

OSPREY

An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

e) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

FROM NOAA-12: The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.

FROM DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531 332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533 535; 44 U.S.C. 3101; Equal Employment Actof 1972; and all existing, applicable Department policies, and regulations.

FROM DEPT-18: Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

FROM: OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

FROM OPM/GOVT-5: 5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

FROM DEPT-29: Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95. The system is also authorized by the U.S. Office of Management & Budget (OMB)

Circular A 130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq*. (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112 95); the American Fisheries Act, Title II, Public Law 105 277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101 5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951 961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq*. (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431 2444; the Marine Mammal Protection Act, 16 U.S.C. 1361; and the Debt Collection Improvement Act, 31 U.S.C. 7701.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

ONMS is a FIPS 199 Moderate Security risk.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS has developed a new permit application that collects non-sensitive PII; ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	

s. Other general personal data (specify):
The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work related data section.
The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			

i. Other work-related data (specify):
The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	

j. Other distinguishing features/biometrics (specify):
ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	

g. Other system administration/audit data (specify)
The NOAA6602 OSPREY application uses the NOAA LDAP to authenticate the permit coordinators. Only ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator

access is sent to NOAA ArcSight. ArcSight records User ID and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

2.3 Describe how the accuracy of the information in the system is ensured.

OSPREY

The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions

Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity.

For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport. HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0141, National Marine Sanctuary Permits
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

UAS Only Although the ONMS UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): ONMS Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics).			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking are stored temporarily during the hiring phase, including, standard HR information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number. The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS

ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

OSPREY

1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits fall into this category. This category also includes requests for authorizations of other agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

- The disposal of cremated human remains by a commercial operator in any national marine sanctuary
- The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
- The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
- The discharge and immediate recovery of objects related to special effects of motion pictures; and
- The continued presence of submarine cables beneath or on the seabed.

(d) Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

(e) Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

(f) Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

(g) Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

(h) Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish

to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research Only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

Collected from the public.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.

There is a potential for unauthorized access to the system, which would expose non-sensitive PII to an unauthorized user.

Old data is purged from the systems per retention schedule.

Users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the

PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Includes instances of security or privacy breach.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/management/permits/welcome.html

X	Yes, notice is provided by other means.	Specify how: **OSPREY: see above link to site with PAS.** **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR:** Applicants and employees: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of

their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information, **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information

		through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **Acquisition** Procurement information within NOAA6602 is not monitored or tracked. It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. **HR** Employee evaluations and potential employee resumes are not monitored, tracked, or recorded within NOAA6602. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONMS Permit application (OSPREY) is hosted on a data base. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution. Audit solution.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access controlled file cabinet.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants. DEPT-13, Investigative and Security Records. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-29, Unmanned Aircraft Systems; OPM/GOVT-1, General

	Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse

	effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: There is no sensitive data.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgrade the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the assessment. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: James Cooperman Office: National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:24:28 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: National Ocean Service Phone: 240-533-0832 Email: john.d.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:51 -05'00' Date signed:
Authorizing Official Name: John Armor Office: National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:22:31 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graph Office: NOAA Phone: 301-628-5751 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:39:27 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:48:42 05'00'

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS has developed a new permit application that collects non-sensitive PII; ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

OSPREY

In order to issue permits for research within our sanctuaries the ONMS Permit system (OSPREY) will collect minimal non-sensitive PII. This will include Name, Business or School Address, Email address and phone number. There is potential for an applicant to provide home address, home phone and personal email instead of business as requested.

HR Data

ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

UAS

The ONMS UAS has the potential to inadvertently capture PII.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc… alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 15, 2018 12:25 PM
To:	Martin, Lisa; Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO; Gitelman, Steve (Contractor); Toland, Michael
Cc:	John D. Parker; James Cooperman; John Dandy; Marie Murphy NOAA Affiliate; Mark Graff NOAA Federal
Subject:	NOAA6602 PIA and PTA revised per CRB, and responses to minutes also attached
Attachments:	NOAA6602 PTA_031518 per CRB.pdf; NOAA6602 PIA_3 15 2018 per CRB minutes.pdf; NOAA6602(3 15 18)Final_NOAA response.docx

Thanks, everyone!!

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Impact Assessment
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) **System location**: The sites that constitute the ONMS are the Silver Spring HQ, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose identified in Section 4

OSPREY

An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

e) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

- The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531 332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533 535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.
- 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
- 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
- 5 U.S.C. 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533
- Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95, U.S. Office of Management & Budget (OMB) Circular

A 130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq.* (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112 95); the American Fisheries Act, Title II, Public Law 105 277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101 5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951 961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq.* (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431 2444 and the Debt Collection Improvement Act, 31 U.S.C. 7701.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

ONMS is a FIPS 199 Moderate Security risk.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work related data section. The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance appraisals					

The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify)					

The NOAA6602 OSPREY application uses the NOAA LDAP to authenticate the permit coordinators. Only

ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator access is sent to NOAA ArcSight. ArcSight records User ID and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

2.3 Describe how the accuracy of the information in the system is ensured.

OSPREY

The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions

Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity.

For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport. HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0141, National Marine Sanctuary Permits
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): **UAS Only** Although the ONMS UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): ONMS Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. HR: ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking are stored temporarily during the hiring phase, including, standard HR information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number. Information sharing: NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics). Information shared is scientific data only.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees, including electronic copies of resumes and the processing of HR data about employees including hiring ranking are stored temporarily during the hiring phase, including, standard HR information such as travel authorization and vouchers, passports and international travel forms, information for transmitting the security badge request email which includes only an email address and possibly a phone number. The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS

ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

OSPREY

1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits fall into this category. This category also includes requests for authorizations of other agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

· The disposal of cremated human remains by a commercial operator in any national marine sanctuary
· The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
· The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
· The discharge and immediate recovery of objects related to special effects of motion pictures; and
· The continued presence of submarine cables beneath or on the seabed.

(d) Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

(e) Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

(f) Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

(g) Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

(h) Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or

slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research Only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

Collected from the public.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.

There is a potential for unauthorized access to the system, which would expose non-sensitive PII to an unauthorized user.

Old data is purged from the systems per retention schedule.

Users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the

PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Includes instances of security or privacy breach.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/management/permits/welcome.html

X	Yes, notice is provided by other means.	Specify how: **OSPREY: see above link to site with PAS.** **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR:** Applicants and employees: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information, **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants apply for positions through USA Jobs which allows the applicant to review and update information until the position closes. Contract employees initiate the change through their contracting company in person. Once an employee is hired, all changes and updates are made directly to the employee's HR representative.

		Acquisition The business works closely with the purchasing manager any updates are made directly to the purchasing manager, in writing.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **Acquisition data is monitored temporarily until a procurement is concluded.** It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. **Employee evaluations and potential employee resumes are monitored temporarily,** until transfer to the NOAA WFMO.. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONMS Permit application (OSPREY) is hosted on a data base. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution. Audit solution.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access controlled file cabinet.

All PII and BII are encrypted at rest.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants. COMMERCE/DEPT-13, Investigative and Security Records. COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-29, Unmanned Aircraft Systems; OPM/GOVT-1, General Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records

	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: Acquisition and performance ratings.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgraded the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the initial assessment. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: James Cooperman Office: National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:24:28 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: National Ocean Service Phone: 240-533-0832 Email: john.d.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:51 -05'00' Date signed:
Authorizing Official Name: John Armor Office: National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:22:31 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graph Office: NOAA Phone: 301-628-5751 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:39:27 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:48:42 05'00'

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily. The risk would be only if and when the UAS is in operation, which it is currently not.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

OSPREY

In order to issue permits for research within our sanctuaries the ONMS Permit system (OSPREY) will collect minimal non-sensitive PII. This will include Name, Business or School Address, Email address and phone number. There is potential for an applicant to provide home address, home phone and personal email instead of business as requested.

HR Data

ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

UAS

The ONMS UAS has the potential to inadvertently capture PII.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Privacy Impact Assessment (PIA) Compliance Review Board (CRB) Meeting Minutes
NOAA Office of National Marine Sanctuaries (NOAA6602)
March 15, 2018

Attendees:

Privacy Team
Kathy Gioffre
Lisa Martin
Steve Gitelman
Dorrie Ferguson
Eric Cline (OCIO)

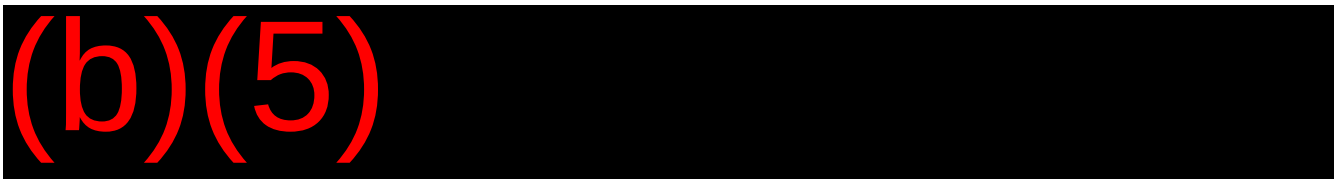
NOAA
Mark Graff
Sarah Brabson
John Dandy
James Cooperman
Marie Murphy

Results/Conclusion:

Upon review of NOAA Office of National Marine Sanctuaries (NOAA6602), Senior Agency Official for Privacy (SAOP) approval is pending additional review of the System of Record Notice (SORN) prior to providing concurrence for renewal of the Authorization to Operate (ATO). The Office of the Chief Information Officer (OCIO) has provided concurrence on the NIST 853 Appendix J privacy controls.

Action Items:

NOAA:


(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 15, 2018 2:17 PM
To:	Martin, Lisa; CPO
Cc:	Mark Graff NOAA Federal
Subject:	Re revised NOAA6602 PIA and PTA
Attachments:	NOAA6602 PIA_03152018 per CRB v2.pdf; NOAA6602 PTA_031518 per CRB v2.pdf

Here you go, Lisa, hope this is it . . .thx again

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Impact Assessment
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) **System location**: The sites that constitute the ONMS are the Silver Spring HQ, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose identified in Section 4

OSPREY

An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

e) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

- The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531 332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533 535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.
- E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
- 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
- 5 U.S.C. 3109, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533
- Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95, U.S. Office of Management & Budget (OMB) Circular A 130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq.* (Magnuson-Stevens Act); High Seas Fishing Compliance Act

of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112 95); the American Fisheries Act, Title II, Public Law 105 277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101 5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951 961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq.* (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431 2444 and the Debt Collection Improvement Act, 31 U.S.C. 7701.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

ONMS is a FIPS 199 Moderate Security risk.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	

b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work related data section. The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance appraisals					

The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify)					

The NOAA6602 OSPREY application uses the NOAA LDAP to authenticate the permit coordinators. Only ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator access is sent to NOAA ArcSight. ArcSight records User ID and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

2.3 Describe how the accuracy of the information in the system is ensured.

OSPREY

The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions

Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity.

For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport.

HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0141, National Marine Sanctuary Permits
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): **UAS Only** Although the ONMS UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): ONMS Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. HR: ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees. This includes electronic copies of resumes stored temporarily during the hiring phase. Also stored temporarily are standard HR information such as travel authorization and vouchers, passports and international travel forms, and information for transmitting the security badge request email, which includes only an email address and possibly a phone number. Information sharing: NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics). Information shared is scientific data only.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees. This includes electronic copies of resumes stored temporarily during the hiring phase. Also stored temporarily are standard HR information such as travel authorization and vouchers, passports and international travel forms, and information for transmitting the security badge request email, which includes only an email address and possibly a phone number.

The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

OSPREY
1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits fall into this category. This category also includes requests for authorizations of other agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

· The disposal of cremated human remains by a commercial operator in any national marine sanctuary
· The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
· The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
· The discharge and immediate recovery of objects related to special effects of motion pictures; and
· The continued presence of submarine cables beneath or on the seabed.

(d) Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

(e) Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

(f) Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

(g) Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

(h) Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or

slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research Only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

Collected from the public.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.

Old data is purged from the systems per retention schedule.

Users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Includes instances of security or privacy breach.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/management/permits/welcome.html	
X	Yes, notice is provided by other means.	Specify how:

		OSPREY: see above link to site with PAS. **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR:** Applicants and employees: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants apply for positions through USA Jobs which allows the applicant to review and update information until the position closes. Contract employees initiate the change through their contracting company in person. Once an employee is hired, all changes and updates are made directly to the employee's HR representative.

		Acquisition The business works closely with the purchasing manager and any updates are made directly to the purchasing manager, in writing.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **Acquisition data is monitored and tracked temporarily until a procurement is concluded.** It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. **Employee evaluations and potential employee resumes are monitored and tracked temporarily,** until transfer to the NOAA WFMO..They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONMS Permit application (OSPREY) is hosted on a data base. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution. Audit solution.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access controlled file cabinet.

All PII and BII are encrypted at rest.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants. COMMERCE/DEPT-13, Investigative and Security Records. COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-29, Unmanned Aircraft

	Systems; OPM/GOVT-1, General Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: Acquisition and performance ratings.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgraded the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the initial assessment. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: James Cooperman Office: National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:24:28 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: National Ocean Service Phone: 240-533-0832 Email: john.d.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:51 -05'00' Date signed:
Authorizing Official Name: John Armor Office: National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:22:31 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graph Office: NOAA Phone: 301-628-5751 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:39:27 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:48:42 05'00'

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Silver Spring Headquarters, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily. The risk would be only if and when the UAS is in operation, which it is currently not.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

UAS

The ONMS UAS has the potential to inadvertently capture PII, when in operation.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 15, 2018 2:20 PM
To:	James Cooperman; John D. Parker
Cc:	Mark Graff NOAA Federal
Subject:	Additional minor revisions to NOAA6602
Attachments:	NOAA6602 PTA_031518 per CRB v2.pdf; NOAA6602 PIA_03152018 per CRB v2.docx

Here's the Word version of the PIA for your records. I'll send you the signed pdf as soon as it's signed. It was mostly punctuation errors.

And here the slightly revised PTA. I removed permits and HR from Question 2.

Both PIA and PTA re sent to Lisa.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Silver Spring Headquarters, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily. The risk would be only if and when the UAS is in operation, which it is currently not.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

UAS

The ONMS UAS has the potential to inadvertently capture PII, when in operation.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Martin, Lisa (Federal)

From:	Martin, Lisa (Federal)
Sent:	Thursday, March 15, 2018 3:49 PM
To:	Graff, Mark (Federal); Brabson, Sarah (Federal)
Cc:	Gioffre, Kathy (Federal); Murphy, Tahira (Federal); Purvis, Catrina (Federal); CPO
Subject:	NOAA6602 SAOP Approved PIA
Attachments:	NOAA6602 PIA SAOP Approved.pdf; NOAA6602 PTA_031518 per CRB v2.pdf

Mark/Sarah,

The PIA for the Office of National Marine Sanctuaries (NOAA6602) has been approved by me, the Acting SAOP/CPO. Tahira Murphy within the Office of Privacy and Open Government will post the PTA and PIA (attached) to the DOC Privacy website within three work days.

Thanks,
Lisa

Lisa J. Martin

Lisa J. Martin
Deputy Director of Departmental Privacy Operations
U.S. Department of Commerce
Office of Privacy and Open Government
Office: (202) 482-2459
Email: LMartin1@doc.gov

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Impact Assessment
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

LISA MARTIN

Digitally signed by LISA MARTIN
DN c=US, o=U S Government, ou=Department of Commerce, ou=Office of the Secretary, cn=LISA MARTIN, 0 9 2342 19200300 100 1 1=13001000105292
Date 2018 03 15 15 42 59 04 00'

03/15/18

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) **System location**: The sites that constitute the ONMS are the Silver Spring HQ, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose identified in Section 4

OSPREY

An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

e) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

- The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531 332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533 535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.
- E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
- 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
- 5 U.S.C. 3109, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533
- Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95, U.S. Office of Management & Budget (OMB) Circular A 130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq.* (Magnuson-Stevens Act); High Seas Fishing Compliance Act

of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112 95); the American Fisheries Act, Title II, Public Law 105 277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101 5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951 961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq.* (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431 2444 and the Debt Collection Improvement Act, 31 U.S.C. 7701.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

ONMS is a FIPS 199 Moderate Security risk.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	

b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work related data section. The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance appraisals					

The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify)					

The NOAA6602 OSPREY application uses the NOAA LDAP to authenticate the permit coordinators. Only ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator access is sent to NOAA ArcSight. ArcSight records User ID and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

2.3 Describe how the accuracy of the information in the system is ensured.

OSPREY

The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions

Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity.

For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport.

HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0141, National Marine Sanctuary Permits
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): **UAS Only** Although the ONMS UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): ONMS Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. HR: ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees. This includes electronic copies of resumes stored temporarily during the hiring phase. Also stored temporarily are standard HR information such as travel authorization and vouchers, passports and international travel forms, and information for transmitting the security badge request email, which includes only an email address and possibly a phone number. Information sharing: NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics). Information shared is scientific data only.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees. This includes electronic copies of resumes stored temporarily during the hiring phase. Also stored temporarily are standard HR information such as travel authorization and vouchers, passports and international travel forms, and information for transmitting the security badge request email, which includes only an email address and possibly a phone number.

The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

OSPREY
1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits fall into this category. This category also includes requests for authorizations of other agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

· The disposal of cremated human remains by a commercial operator in any national marine sanctuary
· The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
· The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
· The discharge and immediate recovery of objects related to special effects of motion pictures; and
· The continued presence of submarine cables beneath or on the seabed.

(d) Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

(e) Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

(f) Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

(g) Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

(h) Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or

slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research Only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

Collected from the public.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.

Old data is purged from the systems per retention schedule.

Users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Includes instances of security or privacy breach.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/management/permits/welcome.html	
X	Yes, notice is provided by other means.	Specify how:

		OSPREY: see above link to site with PAS. **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR:** Applicants and employees: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants apply for positions through USA Jobs which allows the applicant to review and update information until the position closes. Contract employees initiate the change through their contracting company in person. Once an employee is hired, all changes and updates are made directly to the employee's HR representative.

		Acquisition The business works closely with the purchasing manager and any updates are made directly to the purchasing manager, in writing.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **Acquisition data is monitored and tracked temporarily until a procurement is concluded.** It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. **Employee evaluations and potential employee resumes are monitored and tracked temporarily,** until transfer to the NOAA WFMO. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONMS Permit application (OSPREY) is hosted on a data base. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution. Audit solution.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access controlled file cabinet.

All PII and BII are encrypted at rest.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants. COMMERCE/DEPT-13, Investigative and Security Records. COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-29, Unmanned Aircraft

	Systems; OPM/GOVT-1, General Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: Acquisition and performance ratings.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgraded the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the initial assessment. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: James Cooperman Office: National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:24:28 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: National Ocean Service Phone: 240-533-0832 Email: john.d.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:51 -05'00' Date signed:
Authorizing Official Name: John Armor Office: National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:22:31 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graph Office: NOAA Phone: 301-628-5751 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:39:27 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:48:42 05'00'

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Silver Spring Headquarters, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily. The risk would be only if and when the UAS is in operation, which it is currently not.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

UAS

The ONMS UAS has the potential to inadvertently capture PII, when in operation.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, March 15, 2018 3:50 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Go ahead and sign NOAA8881 PTA
Attachments:	NOAA8881_PTA_2018 AB mhg.pdf

Got it. Ok, here it is signed.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Thu, Mar 15, 2018 at 3:37 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> I sent Adam the cert info and explained our normal process for review etc.
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NWS Central Region WAN/LAN (NOAA8881)

U.S. Department of Commerce Privacy Threshold Analysis

NWS Central Region WAN/LAN (NOAA8881)

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The NWS Central Region (CR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees, contractors, volunteers, and other individuals who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of tracking job vacancies, developing statistical reports, and performing other related administrative tasks. Weather Forecast Office (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers who provide weather reports to them.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

The statutory authority covering the collection of this data is 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce].

This is a moderate level system.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X_ DOC employees
____ Contractors working on behalf of DOC
_X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NWS Central Region WAN/LAN and as a consequence of this applicability. I will perform and document a PIA for this IT system. The current PIA was approved by DOC on 6/29/2017.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Adam Van Meter

Signature of ISSO: VAN METER.ADAM.L.1365874057 Digitally signed by VAN METER.ADAM.L.1365874057 Date: 2018.03.15 10:16:05 -05'00'

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.03.15 12:50:18 -04'00'

Name of Authorizing Official (AO): Christopher Strager

Signature of AO: STRAGER.CHRISTOPHER.S.1040261962 Digitally signed by STRAGER.CHRISTOPHER.S.1040261962 Date: 2018.03.15 10:23:41 05'00'

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.15 15:48:47 04'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 15, 2018 3:52 PM
To:	James Cooperman; John D. Parker; John Dandy; Marie Murphy NOAA Affiliate
Cc:	Mark Graff NOAA Federal
Subject:	Fwd: NOAA6602 SAOP Approved PIA
Attachments:	NOAA6602 PIA SAOP Approved.pdf; NOAA6602 PTA_031518 per CRB v2.pdf

Forwarded message
From: **Martin, Lisa (Federal)** <LMartin1@doc.gov>
Date: Thu, Mar 15, 2018 at 3:48 PM
Subject: NOAA6602 SAOP Approved PIA
To: "Graff, Mark (Federal)" <Mark.Graff@noaa.gov>, "Brabson, Sarah (Federal)" <Sarah.Brabson@noaa.gov>
Cc: "Gioffre, Kathy (Federal)" <KGioffre@doc.gov>, "Murphy, Tahira (Federal)" <TMurphy2@doc.gov>, "Purvis, Catrina (Federal)" <CPurvis@doc.gov>, CPO <CPO@doc.gov>

Mark/Sarah,

The PIA for the Office of National Marine Sanctuaries (NOAA6602) has been approved by me, the Acting SAOP/CPO. Tahira Murphy within the Office of Privacy and Open Government will post the PTA and PIA (attached) to the DOC Privacy website within three work days.

Thanks,

Lisa

Lisa J. Martin

Lisa J. Martin

Deputy Director of Departmental Privacy Operations

U.S. Department of Commerce

Office of Privacy and Open Government

Office: (202) 482 2459

Email: LMartin1@doc.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Impact Assessment
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

LISA MARTIN

Digitally signed by LISA MARTIN
DN c=US, o=U S Government, ou=Department of Commerce, ou=Office of the Secretary, cn=LISA MARTIN, 0 9 2342 19200300 100 1 1=13001000105292
Date 2018 03 15 15 42 59 04 00'

03/15/18

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of National Marine Sanctuaries (ONMS)
NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

Provide a description of the system that addresses the following elements:

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) **System location**: The sites that constitute the ONMS are the Silver Spring HQ, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The way the system operates to achieve the purpose identified in Section 4

OSPREY

An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. **However, it is currently not in operation.**

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

e) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY
Permit data is only used internally by ONMS and entered or retrieved from the permit application using encryption for data in transit.

UAS
Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation. **However, it is currently not in operation.**

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

f) How information is transmitted to and from the system

OSPREY
All communication, by the permit coordinators, to and from the OSPREY application is using encryption for data in transit.

UAS
The UAS is hand carried from UAS to Scientific workstation.

HR
HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data
Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network.

g) Any information sharing conducted by the system

OSPREY
NOAA6602 only shares scientific data. Permit data is used internally. Any permit data shared does not include PII.

UAS data is processed then shared internally only. **However, it is currently not in operation.**

Acquisition data is not shared.

Employee information is shared internally and also with DOC and federal agencies in case of breach.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

OSPREY The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

- The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531 332; 15 U.S.C. 1501 *et seq.*; 28 U.S.C. 533 535; 44 U.S.C. 3101; Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.
- E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
- 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.
- 5 U.S.C. 3109, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533
- Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015); National Marine Sanctuaries Act, 16 U.S.C. 1431 *et seq.*; Marine Debris Act, 33 U.S.C. 1951 *et seq.;* Coast and Geodetic Survey Act, 33 U.S.C. 883a *et seq.*; Coastal Zone Management Act, 16 U.S.C. 1451 *et seq.*; Coral Reef Conservation Act, 16 U.S.C. 6401 *et seq.*; National Historic Preservation Act, 16 U.S.C. 470 *et seq.*; Ocean Pollution Act, 33 U.S.C. 2701 *et seq.*; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9601 *et seq.*; Clean Water Act, 33 U.S.C. 1251; 47 CFR parts 80, 87, and 95, U.S. Office of Management & Budget (OMB) Circular A 130; the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 *et seq.* (Magnuson-Stevens Act); High Seas Fishing Compliance Act

of 1995, 16 U.S.C. 5501 *et seq.*; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the FAA Modernization and Reform Act of 2012 (Pub. L. 112 95); the American Fisheries Act, Title II, Public Law 105 277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101 5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951 961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C. Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 *et seq.* (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431 2444 and the Debt Collection Improvement Act, 31 U.S.C. 7701.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

ONMS is a FIPS 199 Moderate Security risk.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	

b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

The above information is only collected to assist employees with making travel arrangements. Paper copies are temporarily stored in a locked file cabinet and destroyed when no longer needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

The **OSPREY** application collects the Applicant's name Business or Institution Mailing Address, Business or Institution Phone Number and Business or Institution email address. The potential exists for an applicant to provide personal information and is being included in this section as well as the work related data section. The applicant must provide the following information: (1) the names, addresses, and telephone numbers of owner, captain, and applicant; (2) vessel name and home port; (3) USCG documentation number, state license, or boat registration number; (4) Length of vessel and primary propulsion type (i.e., motor or sail); (5) Number of divers aboard; and (6) Requested effective date and duration of permit.

The **UAS** does not collect any of the above data types.

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance appraisals					

The OSPREY application collects the above checked data types.
The UAS does not collect any of the above data types. It is also not in operation.
HR related data is stored in the NOAA HR system. but is temporarily stored locally in an access controlled file share prior to being moved to the NOAA HR system..

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

ONMS does not collect any of the above data types.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify)					

The NOAA6602 OSPREY application uses the NOAA LDAP to authenticate the permit coordinators. Only ONMS permit coordinators have access to the OSPREY application Auditing of ONMS permit coordinator access is sent to NOAA ArcSight. ArcSight records User ID and date and time of access to the OSPREY system.

Other Information (specify)
UAS Currently the UAS is not authorized to operate. No data has been collected or stored on or with the device. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): Procurement data is provided in proposals and other procurement documents					

2.3 Describe how the accuracy of the information in the system is ensured.

OSPREY

The completion of ONMS permits is an interactive task completed by the applicant and the ONMS permit coordinator. The permit process is accomplished over multiple weeks and requires interaction between the applicant and permit coordinator. During this process the permit coordinator contacts the applicant via Email and phone calls and verifies information provided.

Acquisitions

Acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

HR data is validated at the time of receipt by the HR representative. The HR representative compares picture ID and other information to validate the applicant's identity.

For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport.

HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648-0141, National Marine Sanctuary Permits
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):ONMS recently purchased a UAS. The UAS has the potential to temporarily contain PII. **However, it is currently not in operation,**			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): **UAS Only** Although the ONMS UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is also only operated in remote locations to avoid the potential to capture PII. **However, it is currently not in operation.**			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): ONMS Both the National Marine Sanctuaries Act and ONMS regulations prescribe procedures by which certain activities that would otherwise be prohibited may be conducted through the issuance of a permit. Any person proposing to conduct an activity prohibited by ONMS regulations must apply for and receive a permit prior to conducting that activity. There are nine types of permits, including those for research, education, and special use activities. HR: ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees. This includes electronic copies of resumes stored temporarily during the hiring phase. Also stored temporarily are standard HR information such as travel authorization and vouchers, passports and international travel forms, and information for transmitting the security badge request email, which includes only an email address and possibly a phone number. Information sharing: NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer experience. The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics). Information shared is scientific data only.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package. *Collected from the public.*

ONMS stores PII on an ad-hoc basis as part of the application and hiring of employees. This includes electronic copies of resumes stored temporarily during the hiring phase. Also stored temporarily are standard HR information such as travel authorization and vouchers, passports and international travel forms, and information for transmitting the security badge request email, which includes only an email address and possibly a phone number.

The travel information collected is kept in both hard and soft forms. The hard copies are kept in a locked file cabinet and the soft copies are kept on the shared drive in a folder accessible only to travel admins. The travel documents contain only the traveler's name, home address, and a truncated vendor number associated to the traveler's name. There are no social security numbers or dates of birth. *Collected from the public, federal employees and contractors.*

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does not intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for performing the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted. **However, it is currently not in use.**

OSPREY
1. The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries. A brief description of some permits are as follows:

(a) General Permits

Scope of this category. This category includes all permits not specifically addressed in subsections (b) through (j) below; typically, permit applications for scientific research, education, management, and salvage (excluding activities aimed at historical resources) activities permits fall into this category. This category also includes requests for authorizations of other agency permits processed pursuant to 15 CFR §922.49.

(b) Baitfish Permits

Scope of this category. This category includes applications for permits to collect baitfish in certain Sanctuary Preservation Areas (SPAs) of the Florida Keys National Marine Sanctuary that are otherwise closed to fishing. There are two types of baitfish permits that may be issued depending on the gear used (castnet or hairhook).

(c) Special Use Permits

Scope of this category. This category includes all permit applications processed under section 310 of the NMSA (16 U.S.C. §1441). Activities must be noticed in the Federal Register before NOAA can issue special use permits for those activities. Presently, these activities are as follows:

· The disposal of cremated human remains by a commercial operator in any national marine sanctuary
· The operation of aircraft below the minimum altitude in restricted zones of national marine sanctuaries for commercial purposes
· The placement and subsequent recovery of objects associated with public events on non-living substrate of the seabed
· The discharge and immediate recovery of objects related to special effects of motion pictures; and
· The continued presence of submarine cables beneath or on the seabed.

(d) Historical Resource Permits

Scope of this category. This category includes all permit applications for activities aimed at historical, cultural, and/or maritime heritage resources of sanctuaries.

(e) Certification

Scope of this category. This category includes all requests for the ONMS to certify activities that are being conducted pursuant to a valid government authorization prior to a sanctuary being designated (commonly known as "grandfathered" activities).

(f) Voluntary Registry

Scope of this category. This category is for researchers who are conducting activities that are not otherwise prohibited. The registry allows them to register their activity, which adds to the database of research activities within a sanctuary.

(g) Tortugas Access Permits

Scope of this category. In 2001, NOAA established the Tortugas Ecological Reserve in the Florida Keys National Marine Sanctuary. Regulations implementing the reserve include controlling access to the reserve through the granting of "access permits" (15 CFR §922.167). Applicants give their information and receive their permit orally, via phone or VHF radio, prior to entering the reserve.

(h) Lionfish Permits

Scope of this category. Florida Keys National Marine Sanctuary encourages the safe removal of invasive lionfish from its waters and issues lionfish removal permits to divers for the collection of lionfish from Sanctuary Preservation Areas (SPAs). The permit allows lionfish to be removed from the SPAs, which are otherwise no-fishing, no-take zones, with hand nets or

slurp guns only. Spear guns or pole spears may not be used. This permit does not allow lionfish removal from the Ecological Reserves or the four Special-use Research Only Areas.

2. When designating each sanctuary, NOAA consulted with the relevant states and Federal agencies regarding their permitting requirements and procedures. Where appropriate, agreements were put in place to use a coordinated permit process. Post-designation, the ONMS continuously works with other state and Federal agencies to identify and eliminate duplication of permit requirements or conditions and, when appropriate, coordinate reviews of applications. In addition, the ONMS routinely accepts information developed for other purposes (e.g., a report on an activity developed for another agency) as part of an ONMS permit application or to meet requirements of an ONMS permit condition.

Collected from the public.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system, there is a chance that privacy data will be viewed if the document is left in plain sight.

Old data is purged from the systems per retention schedule.

Users take privacy training at least annually in the required annual security awareness course.

Users sign rules of behavior to ensure they understand their responsibilities.

UAS
The UAS is currently grounded but **if operational** has the potential to collect PII if it inadvertently flies over an individual.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Includes instances of security or privacy breach.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. The UAS comes with its own remote control. The communication is encrypted digital transmission. All data recorded by the UAS is stored internally on the UAS encrypted SD Card and is not transmitted to the controlling device.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **OSPREY** The PII is only accessed by ONMS employees.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://sanctuaries.noaa.gov/management/permits/welcome.html	
X	Yes, notice is provided by other means.	Specify how:

		OSPREY: see above link to site with PAS. **UAS** The ONMS UAS is operated remotely and does not have the ability to provide notice or consent. **However, currently not in operation.** **COOP** information is provided in hard copy form only to the users performing roles in the COOP function (ACIO, deputy ACIO, ISSO and CTO). Any employee data for the COOP is gathered from the employee on a voluntary basis when they agree to take the position. **HR:** Applicants and employees: all federal forms provide notice, including Privacy Act Statements. Acquisition: Notice is given through solicitations.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **OSPREY** If individuals do not want to provide the PII, they will not submit a permit application. **UAS** The UAS does not have the ability to provide notice and consent. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Federal employees may decline in writing to provide PII to their supervisors, but this may affect their employment. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR). Information is provided on a voluntary basis through individuals who provide their business cards. If they do not want to be placed in the database, they do not provide their business cards.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **OSPREY** There is only one use, the generation of the permit. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants for positions who have applied through the USAJobs system are able to consent to the use of their information in the system. Applicants for positions through contractor companies consent to the use of their information through their companies. For ongoing employee business, such as travel, the user consents to the use of their information by submitting travel requests to their admins. **Acquisition** Businesses provide information related to procurement activities on a voluntary basis through proposals. All information received from businesses is handled in the manner dictated by the federal acquisition regulations (FAR).
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **OSPREY** Individuals may provide their permit coordinators with updated information. **UAS** The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.** **HR** Applicants apply for positions through USA Jobs which allows the applicant to review and update information until the position closes. Contract employees initiate the change through their contracting company in person. Once an employee is hired, all changes and updates are made directly to the employee's HR representative.

		Acquisition The business works closely with the purchasing manager and any updates are made directly to the purchasing manager, in writing.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **Acquisition data is monitored and tracked temporarily until a procurement is concluded.** It is kept on shared drives, access to which is restricted by access control lists (ACLs). Laptop tops are configured with full disk encryption. If PII is kept on a laptop, the data is encrypted. NOAA6602 restricts access to shared folders by ACL. PII is not centralized in a database, and it cannot be easily monitored for access. However, as stated above, the access to the shared folders is restricted by ACL. **Employee evaluations and potential employee resumes are monitored and tracked temporarily,** until transfer to the NOAA WFMO. They are kept on shared drives, access to which is restricted by ACL. NOAA policy requires users not to keep data on their local drives. Policy indicates that they should save it on their own ACL-restricted folders on the shared drive. Policy also requires users to remove all PII from their file share when no longer needed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 03/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.

	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

OSPREY
The ONMS Permit application (OSPREY) is hosted on a data base. All communication with the application is using encryption for data in transit. Only approved Permit coordinators are allowed access to the OSPREY system. User access to the OSPREY database is controlled by NOAA enterprise directory. All access audit trails are uploaded to the NOAA enterprise audit logging solution. Audit solution.

UAS
The UAS system stores data on an encrypted SD card. All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**

HR
Digital HR data may be temporarily stored on ACL protected network file share accessible only by HR personnel. HR related data is permanently stored in the NOAA HR system. Paper copies of HR related material is stored in access controlled file cabinets.

Acquisition
Digital Acquisition data is stored on an ACL controlled networks file share accessible only by contract specialists. Paper copies of acquisition materials are stored in an access controlled file cabinet.

All PII and BII are encrypted at rest.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants. COMMERCE/DEPT-13, Investigative and Security Records. COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-29, Unmanned Aircraft

	Systems; OPM/GOVT-1, General Personnel Records; OPM/GOVT-5, Recruiting, Examining, and Placement Records
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules Chapter 1609 Marine Sanctuaries **UAS** All data is over written or the SD card is destroyed once the data is removed from the SD card. Any PII collection is incidental and unintentional and not retained. See DEPT-29, Section 9.1. **However, currently not in operation.**
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified by the provision of their contact information
X	Quantity of PII	Provide explanation: There is a small quantity of PII.
X	Data Field Sensitivity	Provide explanation: Acquisition and performance ratings.
X	Context of Use	Provide explanation: **OSPREY** permit data is used to generate permits for activity conducted within one of the ONMS sanctuary. **UAS** Data is used to produce coastal and wildlife maps. **However, currently not in operation.** **Acquisition** People or organizations provided their information voluntarily.
X	Obligation to Protect Confidentiality	Provide explanation: **Acquisition** Per the FAR, Procurement Integrity Act, and Economic Espionage Act
X	Access to and Location of PII	Provide explanation: **OSPREY** Data is stored in a database with restricted access to the database. Permit coordinators are granted access to the database after review by the IT manager, OSPREY manager and ISSO. **UAS** The UAS data is only transferred by a UAS pilot and can only be transferred to a ONMS scientific workstation. **However, currently not in operation.**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

OSPREY was recently migrated to the new application. The old OSPREY application has been deactivated. ONMS re-evaluated the system impact level (FIPS-199) and upgraded the FISMA system impact level to Moderate. Many of the privacy controls, although in place, were not properly documented at the time of the initial assessment. The data fields that are implemented were reviewed on multiple occasions to ensure that only the necessary data is collected, especially PII. The ONMS ISSO is included in all development meeting with the database administrator, application programmer and IT manager. The ONMS ISSO is also included in OSPREY permit coordinators meetings and training. **UAS** The UAS has a low risk of threat to privacy since it is operated only in remote locations and is not authorized above buildings or people. **However, currently not in operation.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: James Cooperman Office: National Marine Sanctuaries Phone: 240 533-0680 Email: James.Cooperman@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:24:28 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: National Ocean Service Phone: 240-533-0832 Email: john.d.parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:51 -05'00' Date signed:
Authorizing Official Name: John Armor Office: National Marine Sanctuaries Phone: 240-533-0681 Email: john.armor@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:22:31 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graph Office: NOAA Phone: 301-628-5751 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:39:27 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:48:42 05'00'

Version Number: 01-2018

U.S. Department of Commerce
National Ocean Service

Privacy Threshold Analysis
for the
Office of National Marine Sanctuaries (ONMS)
NOAA6602

U.S. Department of Commerce Privacy Threshold Analysis

Office of National Marine Sanctuaries (ONMS) NOAA6602

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

Provide a general description of the information system in a way that a non-technical person can understand.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system.

NOAA6602 is an information technology (IT) general support system (GSS) that services all fourteen ONMS sites nationwide. NOAA6602 is a GSS and stores PII on an ad-hoc basis if and when employees receive documentation as part of the application and hiring of employees, and the processing of HR data about employees. Electronic copies of resumes and hiring ranking are stored temporarily during the hiring phase; in addition, the system temporarily stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

b) System location

The sites that constitute the ONMS are the Silver Spring Headquarters, Channel Islands, Cordell Bank, Fagatele Bay, Florida Keys, Flower Garden Banks, Gray's Reef, Gulf of the Farallones, Hawaiian Islands Humpback Whale, Monitor, Monterey Bay, Olympic Coast, Stellwagen Bank, and Thunder Bay national marine sanctuaries and the Papahānaumokuākea Marine National Monument. Each site maintains a file server for storage of scientific data and research. All sensitive data is stored on an ACL controlled file share.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA6602 does not interconnect with other systems.

d) The purpose that the system is designed to serve

The purpose of the Office of National Marine Sanctuaries (ONMS) is to serve as the trustee for the nation's system of marine protected areas, i.e., to conserve, protect, and enhance their biodiversity, ecological integrity, and cultural legacy.

Unmanned Aviation System (UAS)
The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data. Currently the UAS is not operational.

The ONMS Permit System (OSPREY)
The Office of National Marine Sanctuaries administers the National Marine Sanctuaries Act, Executive Order 13158, Marine Protected Areas, and other authorities pertaining to designation and management of national marine sanctuaries and marine national monuments.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. This information is used to award contracts that are in support of the ONMS mission.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. Travel data is used to assist ONMS employees in the performance of their duties. Hiring data is used by ONMS to hire qualified personnel to meet the ONMS job requirements.

e) The way the system operates to achieve the purpose identified in Section 4
OSPREY
An applicant for a research permit downloads the permit application from the ONMS website. Once completed the application is sent by US postal Service or delivered in person to an ONMS facility. Permit Coordinators at each site enter the completed permit into the OSPREY applications secure web interface. Permit coordinators at each ONMS site work with the applicant to complete the application and verify the accuracy of the data submitted.

UAS
ONMS recently acquired a Unmanned Aviation System (UAS). The UAS is used to capture photogrammetry (eg. living marine resources and coastal mapping) and meteorological data.

Tier 2 Web
NOAA6602 has multiple websites using Tier 2 multi-session cookies that are not collecting PII. The web admin uses the cookies for analytics and for improving the customer

experience. The home website for NOAA6602 is http://sanctuaries.noaa.gov and the privacy policy for ONMS is https://sanctuaries.noaa.gov/about/privacy.html.

The use of Tier 2 multi-session cookies that are not collecting PII is a requirement by the Federal CIO (https:// policy.cio.gov/web-policy/analytics), which states:

- All agencies must participate in the General Service Administration's (GSA) Digital Analytics Program DAP and deploy the DAP tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management. Participation in the DAP does not preclude agencies from using other analytics programs." And

- Agency use of web measurement and customization technologies must comply with OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies".

- The Federal CIO provides the mandate to use tier-2 multi-session cookies and/or other technologies for tracking analytics.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation. All digital PII received is stored temporarily in Access Controlled files shares used by the HR department. All paper copies of PII is stored within access controlled locked file cabinets. All HR data is stored temporarily and destroyed when no longer needed.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Geographic Information Systems (GIS) are used to process bathymetric and other cartographic data to generate maps that provide a great deal of information about marine sanctuaries.

Acquisition
ONMS collects and stores limited BII on an ad-hoc basis from businesses or other entities that are providing proprietary information in support of federal acquisition actions. Occasionally there is financial information included with the acquisition package.

UAS
ONMS recently acquired a UAS for use in mapping photogrammetry living marine resources and coastal mapping and meteorological data. ONMS does intend to keep the UAS within its boundary and is currently in discussion with another NOAA line office to take possession of the device in return for preforming the required mapping. ONMS use of the UAS is covered by the DOC SORN and the NOAA Policy. The UAS would be exclusively operated in remote areas and is not authorized to operate above people or structures. Any privacy data that is inadvertently collected will be immediately deleted.

OSPREY
The ONMS permit system, OSPREY, is used to generate permits for multiple types of activities within the ONMS Sanctuaries.

HR Data
ONMS temporarily maintains PII data during the hiring process or to assist employees with travel preparation.

g) Identify individuals who have access to information on the system
NOAA6602 maintains scientific data that is freely available to the general public.

OSPREY
NOAA6602 also maintains permit data. OSPREY data is only accessible by ONMS permit coordinators. All permit coordinators must be approved by the ONMS IT Manager, ONMS ISSO and the Osprey system manager.

UAS
Currently the UAS is not operational and had not data that to access. Currently ONMS is trying to transfer the UAS to another NOAA system that has the capability to operate the UAS.

Acquisitions
Contract information is only accessible by the ONMS contracting officer and the IT manager. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

HR Data
ONMS HR data is only accessible by the ONMS HR representative and the ONMS deputy Director. Only employees designated by the ONMS director to fill these roles are allowed access to acquisitions data.

h) How information in the system is retrieved by the user

Scientific data that is collected is published on NOAA6602 websites and in scientific journals.

OSPREY

Permit data is only used internally by ONMS and entered or retrieved from the permit application over the HTTPS protocol.

UAS

Data on the UAS is captured on an encrypted SD card and transferred to the scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Access to the data is restricted to the purchasing manager and the IT manager.

i) How information is transmitted to and from the system

OSPREY

All communication, by the permit coordinators, to and from the OSPREY application is VIA HTTPS protocol.

UAS

The UAS is hand carried from UAS to Scientific workstation.

HR

HR data is stored on the NOAA HR system. Administrators access the data over the NOAA secure portal. Data is transmitted to and from the system over HTTPS.

Acquisition data

Acquisition data is stored on an ACL controlled network share and access over the secured NOS network. Data transmission occurs of the NOS secure network

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): ONMS purchased a UAS that will only be in the system temporarily. The risk would be only if and when the UAS is in operation, which it is currently not.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

UAS

The ONMS UAS has the potential to inadvertently capture PII, when in operation.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities.
ONMS collects and stores limited BII from businesses or other entities that are providing proprietary information in support of a grant application or federal acquisition actions. Occasionally financial information is included with the acquisition package.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA6602 ONMS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA6602 ONMS and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

James Cooperman ISSO_____

Signature of ISSO or SO: COOPERMAN.JAMES.EDWARD.1454108970 Digitally signed by COOPERMAN.JAMES.EDWARD.1454108970 Date: 2018.03.08 09:39:16 -05'00' Date: _____

John D Parker (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.08 15:01:04 05'00' Date: _____

John Armor (AO): _____

Signature of AO: ARMOR.JOHN.ALEXANDER.1365819404 Digitally signed by ARMOR.JOHN.ALEXANDER.1365819404 Date: 2018.03.08 14:23:20 -05'00' Date: _____

Mark Graph (BCPO): GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.09 09:40:32 -05'00'

Signature of BCPO: _____ Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.09 07:43:57 -05'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, March 16, 2018 10:14 AM
To:	Mark Graff NOAA Federal
Cc:	Chris Ortiz
Subject:	NOA8861 PTA for signature
Attachments:	NOAA8861 PTA for MHG signature.pdf

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, March 19, 2018 1:26 PM
To:	Mark Graff NOAA Federal
Cc:	Jean Apedo NOAA Federal; Hadona Diep; Amit Sharma NOAA Affiliate
Subject:	Fwd: FW: Signature for PTA
Attachments:	NOAA1300_PTA_FY18 AO signed.pdf

Mark, for your signature in anticipation of the PIA to be written.

Forwarded message
From: **Douglas Perry - NOAA Federal** <douglas.a.perry@noaa.gov>
Date: Mon, Mar 19, 2018 at 1:24 PM
Subject: Re: FW: Signature for PTA
To: Jean Apedo NOAA Federal <jean.apedo@noaa.gov>
Cc: Patrice Coleman NOAA Federal <patrice.coleman@noaa.gov>, Amit Sharma NOAA Affiliate <amit.sharma@noaa.gov>, Sarah Brabson <Sarah.Brabson@noaa.gov>

See signed PTA.

On Wed, Mar 14, 2018 at 10:37 AM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:

> Doug,
>
> Attached is NOAA1300 PTA for your review. The document is being submitted due to the annual review requirement. Currently, NSDesk does not collect any sensitive data, but they will be doing so in the next few months. When that comes, we will be updating the PTA and generating a new PIA.
>
> Thank you.
>
> **From:** Sarah Brabson - NOAA Federal [mailto:sarah.brabson@noaa.gov]
> **Sent:** Friday, March 09, 2018 2:11 PM
> **To:** Jean Apedo - NOAA Federal
> **Cc:** Amit Sharma - NOAA Affiliate
> **Subject:** Re: Signature for PTA
>
> I did already, sorry, Jean! No comments!
>
> On Fri, Mar 9, 2018 at 1:49 PM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:

Doug

~~~~~~

Douglas A. Perry

Deputy Chief Information Officer
National Oceanic and Atmospheric Administration

Office: (301) 713-9600

www.noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)
~~~~~~

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, March 16, 2018 12:35 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA5044 certification docs for your review and signature
Attachments:	NOAA5044_PIA_Feb2018_BL_ND_VG for MHG signature.pdf; NOAA5044_PTA_Feb2018_BL_ND_VG for MHG signature.pdf; NOAA5044 Annual Review Certification Form for MHG signature.pdf

Mark, all is correct. But they actually redid the PIA in the new template, which I sure did not ask them to do.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA/NSOF Administrative LAN (NSOF Admin LAN) (NOAA5044)

FISMA Name/ID (if different): NSOF Administrative LAN (NSOF Admin LAN) / NOAA5044

Name of IT System/ Program Owner: Andre' Hammond

Name of Information System Security Officer: Brian Little

Name of Authorizing Official(s): Vanessa Griffin

Date of Last PIA Compliance Review Board (CRB): 11/02/2017

(This date must be within three (3) years.)

Date of PIA Review: 2/20/2018

Name of Reviewer: Brian Little

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 Date: 2018.02.20 11:34:29 -05'00'

Date of Privacy Act (PA) Review: 3/16/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 03 16 12 23 09 04'00'

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: _____

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, March 19, 2018 7:58 AM
To:	Sarah Brabson NOAA Federal
Cc:	Chris Ortiz
Subject:	Re: NOA8861 PTA for signature
Attachments:	NOAA8861 PTA for MHG signature mhg.pdf

Signed and attached thanks

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Fri, Mar 16, 2018 at 10:14 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Version Number: 01-2017

U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the
Aviation Weather Center
NOAA8861

U.S. Department of Commerce Privacy Threshold Analysis
National Oceanic and Atmospheric Administration
National Weather Service/Aviation Weather Center (NOAA8861)

Unique Project Identifier: NOAA8861

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
The Aviation Weather Center (AWC), located in Kansas City, MO, enhances aviation safety by issuing accurate warnings, forecasts and analyses of hazardous weather for aviation interests. The Center identifies existing or imminent weather hazards to aircraft in flight and creates warnings for transmission to the aviation community. The Center also originates operational forecasts of weather conditions predicted to affect domestic and international aviation interests during the next 24 hours. The AWC collaborates with universities, governmental research laboratories, Federal Aviation Administration facilities, international meteorological watch offices and other National Weather Service components to maintain a leading edge in aviation meteorology hazards training, operations and forecast technique development.

Warnings of flight hazards, such as turbulence, icing, low clouds and reduced visibility remain most critical for the protection of life and property over the United States from the earth's surface up to Flight Level (FL) 240. Above FL 240, the AWC provides warnings of dangerous wind shear, thunderstorms, turbulence, icing, and volcanic ash for the Northern Hemisphere from the middle of the Pacific Ocean eastward to the middle of the Atlantic Ocean. Additionally, above FL 240, the AWC forecasts jet stream cores, thunderstorms, turbulence and fronts for the Northern Hemisphere from the east coast of Asia eastward to the west coast of Europe and Africa. Through international agreement, the AWC also has responsibility to back up other World Area Forecast Centers with aviation products distributed through the World Area Forecast System.

The AWC supports requirements for products and services established by national and international agreements. The Center coordinates closely with the aviation community to identify new standards in support of Federal Aviation Administration (FAA) national requirements and International Civil Aviation Organization (ICAO) international requirements.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

__X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies

____ Other business entities
__X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
__X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA8861 Aviation Weather Center and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA8861 Aviation Weather Center and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Christopher John Ortiz (AWC ISSO)

Signature of ISSO or SO: ORTIZ.CHRISTOPHER.J.1154749175 Digitally signed by ORTIZ CHRISTOPHER J 1154749175 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn ORTIZ CHRISTOPHER J 1154749175 Date 2018 03 15 10 35 21 06'00' Date: 3/15/18

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.03.15 12:49:18 -04'00' Date: 3/15/18

Name of Authorizing Official (AO): Dr. William Lapenta

Signature of AO: LAPENTA.WILLIAM.M.1370194030 Digitally signed by LAPENTA.WILLIAM.M.1370194030 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=LAPENTA.WILLIAM.M.1370194030 Date: 2018.03.15 14:32:32 -04'00' Date: 3/15/18

Name of Bureau Chief Privacy Officer (BCPO): Mark H. Graff (NOAA)

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.19 07:57:30 -04'00' Date:

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, March 19, 2018 3:59 PM
To:	Mark Graff NOAA Federal
Subject:	Re NOAA5009 certification
Attachments:	NOAA5009_PTA_March 2018 v2.pdf; NOAA5009 certification 2018 for MHG signature.pdf; NOAA5009_PIA2018 for MHG signature.pdf

Mark, attached are the PIA, PTA and Certification for your signature.

(b)(5)

SAR and POA&Ms are in PIA folder.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: National Climatic Data Center Local Area Network

FISMA Name/ID (if different): NOAA5009

Name of IT System/ Program Owner: Juanita Sandidge

Name of Information System Security Officer: Jason Symonds

Name of Authorizing Official(s): Mary Wohlgemuth, Irene Parker

Date of Last PIA Compliance Review Board (CRB): 6/22/17

(This date must be within three (3) years.)

Date of PIA Review: 2/28/2018

Name of Reviewer: Jason Symonds

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: SYMONDS.JASON.T.1366777411 Digitally signed by SYMONDS.JASON.T.1366777411 Date: 2018.03.05 12:36:08 -05'00'

Date of Privacy Act (PA) Review: 3/19/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 03 19 13 00 23 04'00'

Date of BCPO Review: _____

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): _____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: _____

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Tuesday, March 20, 2018 4:16 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Stuff you owe me
Attachments:	NOAA5044_PIA_Feb2018_BL_ND_VG for MHG signature mhg.pdf; NOAA5044_PTA_Feb2018_BL_ND_VG for MHG signature mhg.pdf; NOAA5044 Annual Review Certification Form for MHG signature mhg.pdf

Here is NOAA5044. The question I've got, thoug (b)(5) (b)(5) .

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Tue, Mar 20, 2018 at 3:34 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> NOAA0013 PTA
>
> NOAA5009 certification
>
> NOAA5044 certification
>
> NOAA6702 PIA and PTA signatures
>
> Let me know if you want any of these re sent!
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751

Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA/NSOF Administrative LAN (NSOF Admin LAN) (NOAA5044)

FISMA Name/ID (if different): NSOF Administrative LAN (NSOF Admin LAN) / NOAA5044

Name of IT System/ Program Owner: Andre' Hammond

Name of Information System Security Officer: Brian Little

Name of Authorizing Official(s): Vanessa Griffin

Date of Last PIA Compliance Review Board (CRB): 11/02/2017

(This date must be within three (3) years.)

Date of PIA Review: 2/20/2018

Name of Reviewer: Brian Little

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 Date: 2018.02.20 11:34:29 -05'00'

Date of Privacy Act (PA) Review: 3/16/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 03 16 12 23 09 04'00'

Date of BCPO Review: 3.20.18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 03 20 16 02 25 04'00'

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA5044
NOAA Satellite Operations Facility (NSOF) Administrative LAN

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
[NESDIS/NOAA5044]

Unique Project Identifier: 006-000351101 00-00-02-00-02-00

Introduction: System Description

General Description NSOF Admin LAN (NOAA5044) is a FIPS 199 moderate designated general support system that is physically located in the NOAA building at 4231 Suitland Road, Suitland, Maryland, a suburb of Washington, D.C. The building is owned by NOAA and managed and secured by the General Services Administration. The NSOF Admin LAN provides standard office automation for all NESDIS employees located within the NSOF. It also provides access to the Internet. The LAN provides end-to-end connectivity and network access to all LAN Federal employee and contract users, to increase productivity through the use of applications, data resources, or other electronic office automation tools.

The two types of applications supported by the NSOF Admin LAN -- server applications and client applications -- are considered minor applications in that they are accredited as a GSS rather than separately. There are no major applications (as defined by OMB A-130) in the NSOF Admin LAN environment.
There are five user communities located in the NSOF: the Office of Satellite Ground Systems (OSGS), the Office of Satellite and Product Operations (OSPO), the General Services Administration (GSA), the National Ice Center (NIC) and the Defense Meteorological Satellite Program (DMSP). These user communities have dedicated workstations connected to the NSOF Admin LAN. NOAA5044 provides access to automated programs and systems supporting administrative programs such as budget and financial management, personnel management, procurement, building operation and management, interagency programs, IT planning, and IT security. The system also supports access to the Internet. There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking. Version Number: 01-2015

DOC and DOD performance evaluation are also compiled and maintained in the system. The appropriate forms are completed on the NOAA5044 Manager's secure home directory. They are then printed, hand-carried for signature, and then transferred via the agency-specific secure electronic transfer procedure.
There is also ESPC account management, collecting contact information, such as name, work phone number and work email address from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored in restricted areas of the NSOF Admin LAN shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an

ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.
In addition, the NOAA5044 collects PII of NSOF LAN personnel on a voluntary basis for purposes of Continuity of Operations Planning (COOP). This data is stored on a LAN shared drive only accessible by authorized personnel.
The PII/BII information collected by NOAA5044 is shared with other agencies or parties on a case-by-case basis, as described below. If any of the data is sensitive or For Official Use Only (FOUO), then the data is restricted by drives and folders to only NSOF Admin LAN personnel authorized to access the information.

NSOF Admin LAN currently has interconnections with 6 other NOAA systems. NOAA5044 is connected to NOAA0100 via network using SSL Protection transmitting and receiving unclassified information. NOAA5044 is connected to NOAA0200 via network using SSL protection to send but not receive unclassified data. NOAA5044 is connected to NOAA5006 via network using a site to site VPN to transmit and receive unclassified data. NOAA5044 is connected to NOAA5008 via network using a site to site VPN to send unclassified data. NOAA5044 is connected to NOAA5032 via network using a site to site VPN to send unclassified data. NOAA5044 is connected to NOAA5040 via network using SSL Protection transmitting and receiving unclassified information.

Transfers - The system collects PII of DOC (NOAA employees only) and DOD civilian and military personnel to the extent necessary for preparation of performance, promotion, and awards for these personnel. The NSOF Admin LAN contains personally assigned network shares (H:\), which are accessible only by the person assigned the shared drive.
DOC electronic personnel related forms (NOAA employees only) may be transferred to DOC Bureau HR personnel in bulk or on a case-by-case basis via DOC Accellion (for DOC records only) or via tracked United Parcel Service (UPS) package.

Authority - Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1512 (Powers and Duties of the Department of Commerce)
- 5 USC 2101 to 10210 (Government Organizations and Employees, Part III, Employees)
- 5 USC 301 (Departmental Regulations)
- 10 USC 8010 to 9448 (Armed Forces - Air Force - Organization, Personnel, and Training)
- 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
- E.O. 9397; E.O. 12931; 40 U.S.C. Sec. 501 502.

- 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended

by 13478, 9830, and 12107.

- 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107 347, Sec. 203), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105 277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD 12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
- Sections 1104, 3321, 4305, and 5405 of Title 5, U.S. Code, and Executive Order 12107.
- Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c); FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989)
- E-Government Act of 2002 (Pub. L. 107 347) Section 204; Davis-Bacon and Related Acts: 40 U.S.C. 3141 3148 40 U.S.C. 276a; 29 CFR parts 1, 3, 5, 6 and 7; Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113 101.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
- Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016)

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	X
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	X
c. Employer ID		g. Passport	X	k. Financial Transaction	X
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:
Performance and award forms require the individual's SSN. The Navy requires SSN in its performance evaluation guidance (document provided with PIA).

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
Offeror responses to RFIs and RFPs, confidential/proprietary

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The accuracy of the information is ensured by the information owner. The PII/BII information owner has the responsibility to review the content before dissemination.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	X
Video surveillance		Electronic purchase transactions	X
Other (specify):			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in

reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

1) There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking. The documents are usually completed by the individual or preparer (administrative person that prepares the document for an individual employee). The files are sent to an HR system via DOC Accellion or via tracked United Parcel Service (UPS) package, but copies are stored on the NSOF Admin LAN. This information is not shared with anyone beyond those that are required to process it within the respective bureau.
2) For contractual and budgetary purposes, the NSOF admin LAN stores procurement and contract information, purchase requests, and accounting information which is stored locally or in restricted areas of the shared drive accessible only by authorized personnel.
3) The system's audit logs collect User ID, IP Address, Date/Time of Access, Queries Run, and ID Files accessed on the network and stored locally or into restricted areas of the server that are only accessible by authorized personnel. The NOAA Directory collects PII in the form of name, email and contact number for Continuity Of Operations Plan (COOP). This information is stored on the NSOF Admin LAN and is accessible by authorized personnel.
4) Environmental Satellite Processing Center (ESPC), NOAA5045, account management processes collects name, work phone number, and work email address from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored into restricted areas of the NSOF Admin LAN shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.
5) Performance awards that contain full Social Security Numbers for military and civilians assigned to the Naval Ice Center are stored on the NSOF Admin LAN. Access to the folder is restricted to those that have a need to know.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example:

mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

NOAA5044 utilizes NOAA's annual mandatory IT security training which addresses the proper handling of sensitive information.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA WFMO Recruitment Analysis Data System (RADS). NOAA5044 uploads data in specified formats to RADS. NSOF LAN has media protection controls in place as well as user procedures on how to protect this information.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.ospo.noaa.gov/Organization/About/access.html. The COOP form with PAS was enclosed in the cover email. It is not posted on the Web but kept in a shared drive.	
X	Yes, notice is provided by other means.	Specify how: a. Written notice is included on all personnel forms that employees complete. b. For DOC and DOD performance/award documents, employees are informed by their supervisors that the evaluations are in process. Employees have access to view the official documents. c. For NSOF LAN COOP or emergency recall in the NOAA directory, employees are notified in writing when collecting the applicable information. d. For ESPC, information is voluntarily submitted when a user completes the account request form. e. For responses to solicitations, notice is given on the request for information (RFI) or request for proposal (RFP).
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: a. An individual may decline to provide PII when applying for a position, by not completing all required forms, but his or her employment status may be affected. b. For DOD and DOC personnel data, employees may opt not to provide PII – at the time of the request, and in writing to the personnel administration representative who is assisting them - but this information is needed for processing awards. Performance information is part of the official personnel record for DOD and DOC employees and information is added to the eOPF in conjunction with the employee mid-year and annual reviews. The performance record/information is required in order to conduct performance evaluations. c. For NSOF LAN COOP or emergency recall in the NOAA directory, employees are asked permission in writing by their supervisors when collecting the

		applicable information, and may decline at that time. This information is not required. d. For ESPC, information is voluntarily submitted through email and is stored on the NSOF Admin LAN shared drive, with access controls permitting access to only those with a need to know. An individual may choose not to provide the information, by not answering the questions, but then will not have access to requested information. e. Responses to RFPs/RFIs are voluntary, based on the offeror's decision to respond.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: a. There is only one use for information provided during employee onboarding. b. Consent is included on all personnel forms that employees complete, and consent to the uses explained on the forms is implied by completion of the forms. c. For DOD and DOC personnel data, employees may opt not to provide PII – at the time of the request, and in writing to the personnel administration representative who is assisting them, but this information is needed for processing awards. Performance information is part of the official personnel record for DOD and DOC employees and information is added to the eOPF in conjunction with conduct performance evaluations. This is the only use. d. For NSOF LAN COOP or emergency recall, there is only one use, and consent to that use is implied by the voluntary provision of the information for that intended use. e. For ESPC, the only use is to provide information as requested. f. For contract offerers, there is only one use of the BII information provided and acceptance of that use is implied by proposal submission. the employee mid-year and annual reviews. The performance record/information is required in order to
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to	Specify how: a. An employee may update information on personnel

	them.	forms at any time by contacting their HR representative This is explained during employee orientation. b. For DOD personnel data, employees may update their PII– by contacting their HR representative, as explained during orientation. Employees review information in the eOPF and notify HR of errors. c. b. For Emergency and COOP information, the employee may not review the information, because it contains other staff's PII unless there is need-to-know, but may request updates from the assigned administrative staff, as explained by that staff when requesting the information. d. For ESPC, information can be updated by contacting the ESPC help desk. – as stated on the Web page. e. Offerors will contact the office with updated BII information.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 12/15/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): As stated in the NSOF Admin LAN System Security Plan (SSP), all employees and contractors undergo a national agency check with inquiries (NACI) security check when employed or contracted. This involves a check of Federal and local law enforcement records to help ensure the trustworthiness of the employee. The user (internal or external) signs the NSOF LAN Rules of Behavior (ROB) indicating that they have

	read and understand the ROB. To protect mobile information, all NSOF Admin LAN laptops are fully encrypted using the NOAA enterprise supplied encryption software.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

PII/BII is protected through a combination of measures, including operational safeguards, privacy specific safeguards, and security controls. Policies and awareness training are provided annually. The minimum amount of PII necessary to meet the mission is collected. Security controls are in place, such as access controls limiting access to PII/BII. This information has restricted access limited to authorized NOAA staff. Further, if someone that doesn't have access attempts to access to a folder containing PII/BII, then a failed access log is created. The NSOF Admin LAN has a dedicated drive with user access restrictions for those that store PII/BII. The NSOF Admin LAN has NIST 800-53 Rev 4 security controls in place, including, but not limited to: the Access Control family, limiting access to allow only the necessary functions for users to operate within the NSOF Admin LAN. Account privileges are tied directly to job function and designed to enable the user to accomplish only what the job requires and no more. The Audit and Accountability family utilizes tools such as Tripwire to record, store and manage logs for auditable events. For the Identification and Authentication family, NOAA5044 utilizes two factor to identify and authenticate users. The Media Protection family to monitor access to stored data and the approved sanitation methods for all media. NOAA5044 uses approved DOD sanitization software to ensure no data remains on NOAA5044 media. NOAA5044 is monitored using various tools including Solarwinds, Nessus, McAfee, and Cisco IPS. Also, NOAA5044 has enterprise monitoring tools, such as FireEye. FireEye is managed by NOAA and provides real time monitoring of potential threats to the system and data.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: DEPT-13, *Investigative and Security Records* DEPT-18, *Employees Information Not Covered by Records of Other Agencies.* NOAA-11, *Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission*; OPM/GOVT-1, *General Personnel Records*, OPM/GOVT-2, *Employees Performance File Records*, GSA-GOVT-6, *GSA SmartPay*

	Purchase Charge Card Program, GSA-GOVT -7, *Federal Personal Identity Verification Identity Management System (PIV IDMS)*, GSA-GOVT-9, *System for Award Management*, GSA-GOVT-10, *Federal Acquisition Regulation (FAR) Data Collection System*
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Chapter 100 – General, Chapter 200 – Administrative and Housekeeping Records, and Chapter 300 – Personnel.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified based
X	Quantity of PII	Provide explanation: There is a large amount of PII in the system.
X	Data Field Sensitivity	Provide explanation: There are several types of PII/BII collected
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access to PII is restricted to need to know. If someone that doesn't have access attempted to access a folder containing PII/BII, then a failed access log is created. We also employ security monitoring tools that can detect PII in unauthorized locations. We also employ security monitoring tools that can detect PII in unauthorized locations
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

NOAA5044 has no additional potential threats for the PII/BII information collected or collected from. NOAA5044 provides additional layers of security by having access controls on the PII/BII folders, therefore limiting who has access to the data. Within FY18, NOAA5044 will migrate all PII/BII data to Headquarters LAN, NOAA5006.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: We have recommended to the business process owner responsible for processing DoD awards and performance evaluations that the collection of SSN is not necessary for this activity.

	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: NOAA5044 has increased its privacy controls.
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner	**Information Technology Security Officer**
Name: Brian Little Office: DOC\NOAA\OSPO Phone: (301) 817-3899 Email: Brian.Little@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 Date: 2018.03.13 14:00:35 -04'00' Date signed:	Name: Nancy DeFrancesco Office: DOC\NOAA\NESDIS Phone: (301) 713-1312 Email: Nancy.DeFrancesco@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.13 15:23:20 -04'00' Date signed: 03/13/2018
Authorizing Official	**Bureau Chief Privacy Officer**
Name: Vanessa L. Griffin Office: DOC\NOAA\NESDIS\OSPO Phone: (301) 817-4607 Email: Vanessa.L.Griffin@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.15 16:36:00 -04'00' Date signed:	Name: Mark Graff Office: DOC\NOAA\CPO Phone: (301) 628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 16:04:41 04'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA5044
NOAA Satellite Operations Facility (NSOF) Administrative LAN

U.S. Department of Commerce Privacy Threshold Analysis

NOAA5044

NOAA Satellite Operations Facility (NSOF) Administrative LAN

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

General Description NSOF Admin LAN (NOAA5044) is a FIPS 199 moderate designated general support system that is physically located in the NOAA building at 4231 Suitland Road, Suitland, Maryland, a suburb of Washington, D.C. The building is owned by NOAA and managed and secured by the General Services Administration. The NSOF Admin LAN provides standard office automation for all NESDIS employees located within the NSOF. It also provides access to the Internet. The LAN provides end-to-end connectivity and network access to all LAN Federal employee and contract users, to increase productivity through the use of applications, data resources, or other electronic office automation tools.

The two types of applications supported by the NSOF Admin LAN -- server applications and client applications -- are considered minor applications in that they are accredited as a GSS rather than separately. There are no major applications (as defined by OMB A-130) in the NSOF Admin LAN environment.
There are five user communities located in the NSOF: the Office of Satellite Ground Systems (OSGS), the Office of Satellite and Product Operations (OSPO), the General Services Administration (GSA), the National Ice Center (NIC) and the Defense Meteorological Satellite Program (DMSP). These user communities have dedicated workstations connected to the NSOF Admin LAN. NOAA5044 provides access to automated programs and systems supporting administrative programs such as budget and financial management, personnel management, procurement, building operation and management, interagency programs, IT planning, and IT security. The system also supports access to the Internet. There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone

Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking. Version Number: 01-2015

DOC and DOD performance evaluation are also compiled and maintained in the system. The appropriate forms are completed on the NOAA5044 Manager's secure home directory. They are then printed, hand-carried for signature, and then transferred via the agency-specific secure electronic transfer procedure.
There is also ESPC account management, collecting contact information, such as name, work phone number and work email address from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored in restricted areas of the NSOF Admin LAN shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.
In addition, the NOAA5044 collects PII of NSOF LAN personnel on a voluntary basis for purposes of Continuity of Operations Planning (COOP). This data is stored on a LAN shared drive only accessible by authorized personnel.
The PII/BII information collected by NOAA5044 is shared with other agencies or parties on a case-by-case basis, as described below. If any of the data is sensitive or For Official Use Only (FOUO), then the data is restricted by drives and folders to only NSOF Admin LAN personnel authorized to access the information.

NSOF Admin LAN currently has interconnections with 6 other NOAA systems. NOAA5044 is connected to NOAA0100 via network using SSL Protection transmitting and receiving unclassified information. NOAA5044 is connected to NOAA0200 via network using SSL protection to send but not receive unclassified data. NOAA5044 is connected to NOAA5006 via network using a site to site VPN to transmit and receive unclassified data. NOAA5044 is connected to NOAA5008 via network using a site to site VPN to send unclassified data. NOAA5044 is connected to NOAA5032 via network using a site to site VPN to send unclassified data. NOAA5044 is connected to NOAA5040 via network using SSL Protection transmitting and receiving unclassified information.

Transfers - The system collects PII of DOC (NOAA employees only) and DOD civilian and military personnel to the extent necessary for preparation of performance, promotion, and awards for these personnel. The NSOF Admin LAN contains personally assigned network shares (H:\), which are accessible only by the person assigned the shared drive.
DOC electronic personnel related forms (NOAA employees only) may be transferred to DOC Bureau HR personnel in bulk or on a case-by-case basis via DOC Accellion (for DOC records only) or via tracked United Parcel Service (UPS) package.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_X_ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

_X_ Companies
_X_ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X_ DOC employees
_X_ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA5044 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA5044 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Brian Little, NOAA5044 ISSO

Signature of ISSO or SO: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 Date: 2018.03.13 15:03:02 04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Nancy A. DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.13 15:21:20 04'00' Date: 03/13/2018

Name of Authorizing Official (AO): Vanessa L. Griffin

Signature of AO: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.15 16:34:59 04'00' Date: 03/15/2018

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 16:06:22 -04'00' Date: 3/20/18

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Tuesday, March 20, 2018 4:47 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Stuff you owe me
Attachments:	NOAA5009_PIA2018 for MHG signature mhg.pdf; NOAA5009_PTA_March 2018 v2 mhg.pdf; NOAA5009 certification 2018 for MHG signature mhg.pdf

Here is NOAA5009. It looks like it has the same problem a (b)(5) [redacted].

Otherwise good to go for all three docs.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Tue, Mar 20, 2018 at 3:34 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> NOAA0013 PTA
>
> NOAA5009 certification
>
> NOAA6702 PIA and PTA signatures
>
> Let me know if you want any of these re sent!
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> Governance and Portfolio Division
> Office 301 628 5751
> (b)(6)

Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: National Climatic Data Center Local Area Network

FISMA Name/ID (if different): NOAA5009

Name of IT System/ Program Owner: Juanita Sandidge

Name of Information System Security Officer: Jason Symonds

Name of Authorizing Official(s): Mary Wohlgemuth, Irene Parker

Date of Last PIA Compliance Review Board (CRB): 6/22/17

(This date must be within three (3) years.)

Date of PIA Review: 2/28/2018

Name of Reviewer: Jason Symonds

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: SYMONDS.JASON.T.1366777411 Digitally signed by SYMONDS.JASON.T.1366777411 Date: 2018.03.05 12:36:08 -05'00'

Date of Privacy Act (PA) Review: 3/19/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 03 19 13 00 23 04'00'

Date of BCPO Review: 3/20/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 03 20 16 42 10 04'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Climatic Data Center Local Area Network (NOAA5009)

Reviewed by: _____Mark Graff_____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/National Climatic Data Center Local Area Network

Unique Project Identifier: 006-48-00-00-01-3209-00-108-023

Introduction: System Description

(a) NOAA's National Centers for Environmental Information (NCEI)-NC, a general support system, maintains the world's largest climate data archive and provides climatological services and data to every sector of the U.S. economy and to users worldwide. Records in the archive range from paleoclimate data to centuries-old journals to data less than an hour old. The Center's mission is to preserve these data and make them available to the public, business, industry, government, and researchers.

NCEI-NC develops national and global datasets, which maximize the use of our climatic and natural resources while also minimizing the risks caused by climate variability and weather extremes. NCEI has a statutory mission to describe the climate of the United States and it acts as the "Nation's Scorekeeper" regarding the trends and anomalies of weather and climate. NCEI-NC's climate data have been used in a variety of applications including agriculture, air quality, construction, education, energy, engineering, forestry, health, insurance, landscape design, livestock management, manufacturing, national security, recreation and tourism, retail, transportation, and water resources management.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI-NC coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service. NCEI-NC manages and contributes to a variety of climate service partnerships including the Regional Climate Services Directors, Regional Climate Centers, State Climatologists, and Cooperative Institute for Climate and Satellites North Carolina. To facilitate a global data and information exchange, the Center also operates two World Data Centers one for meteorology and one for paleoclimatology and plays an active role in professional societies and user engagement activities. *Data available through these partnerships does not require access accounts.*

NCEI-NC has approximately 310 users that connect within NCEI-NC's security boundary. The NCEI-NC user environment consists mainly of web developers, scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, graphic designers, order fulfillers, and computer operators.

(b) A typical transaction conducted on the system, where PII is collected, includes public access to data products via an ordering mechanism for customized order fulfillment.

(c) Information sharing is conducted by the system. As it relates to PII, NCEI-NC will share usernames with other NOAA entities in support of NOAA Incident Response (the system does not share this information directly with DOC). In addition, NCEI sends, to a FEDRAMP authorized cloud service (SalesForce at The Landmark @ One Market Suite 300 San Francisco, CA 94105), public customer name/address info that was collected during order placement. NCEI is trying to get meaningful information such as which products are important to a particular group of users or what particular variables within products customers from various sectors are asking for (ex. temperature, precipitation, irradiance). We are also interested in seeing how those requests change over time so that we can make sure NCEI is not under- or over-investing in any particular product or portfolio. If possible, we would also like to capture benefits that users derive from the data. Without some individual identifier, we could not determine how customer needs change, we would only be able to see the mass movement of users as a whole or an entire sector.

(d) The legal authority for collection of information addressed in this PIA is: 5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records; additional authorities: 44 U.S.C. 3101, Records Management by Agency Heads; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; Government Paperwork Elimination Act (Pub. L. 105 277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD 12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

(e) NOAA5009 is categorized as a FIPS 199 moderate system.

NCEI-NC has various requirements to collect PII from its employees. These include employee contact information for contingency planning, information related to performance plans, photographs for internal use, and biometric information used to authenticate certain employees to restricted areas. The following information is collected and maintained:

A. Employee's Name
B. Personal email address
C. Personal phone number
D. Photograph for internal use (voluntary posting to intranet for face recognition)
E. Dates for the period of performance
F. Title, Series, and Grade of the position

G. Employee's Division
H. Information about the employee's work and work performance, constituting the plan or appraisal
I. Photograph (copied from government issued PIV card)
J. Fingerprint template file (copied from government issued PIV card)

NCEI-NC offers data to the public through its website. In order for the data to be shipped to the customer, the customer must provide their name and mailing address. It is optional for the customer to leave their phone number and email address as another way of communication. NCEI-NC website utilizes a third party for submitting and authorizing credit cards for data product purchase that require payment. Those credit card numbers are entered directly into the Pay.gov system. The credit card numbers are not stored at NCEI-NC. The information collected is as follows:

A. Name
B. Address
C. Email address (optional)
D. Phone number (optional)

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

___ This is an existing information system in which changes do no create new privacy risks and for which there is an SAOP-approved PIA.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance information					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X*	d. Photographs	X**	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

*From the CAC, to generate the building registration card.

** From the CAC, and for internal use after signed consent.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics*	X
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

*A physical access control system (PACS) is in place to authorize employees who require access to the computer room. This system requires the employee to present their government issued PIV card and their fingerprint to register; once registered, the CAC only is required. The PACS system stores the PIV information on a database in a restricted network where only IT Security personnel have access.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

- Entry points into the computer room and within the computer room are under video surveillance, with warning signs posted. The cameras record on motion and the video files stored on an air gapped system. Access to that system is restricted to the computer operators (staff and contractors) and the IT Security team.

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Continuity of Operations (COOP); Physical Access Control Authorization; Cybersecurity Incident Response			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

NCEI-NC has various requirements to collect PII from its employees. These include employee contact information for contingency planning, information related to performance plans, photographs for internal use, and biometric information used to authenticate certain employees to restricted areas. The following information is collected and maintained:

A. Employee's Name
B. Personal email address
C. Personal phone number
D. Photograph for internal use (voluntarily posted to the intranet for face recognition)
E. Dates for the period of performance
F. Title, Series, and Grade of the position
G. Employee's Division
H. Information about the employee's work and work performance, constituting the plan or appraisal
I. Photograph (copied from government issued PIV card) for computer room access
J. Fingerprint template file (copied from government issued PIV card) for computer room access

Information is not shared outside the bureau unless there is a breach notification.

NCEI-NC offers data to the public through its website. If data delivery is not feasible online, then an alternative method is direct shipment to the customer. In order for the data to be shipped, the customer must provide their name and mailing address. It is optional for the customer to leave their phone number and email address as another way of communication. The NCEI-NC website utilizes a third party for submitting and authorizing credit cards for data product purchase that require payment. Those credit card numbers are entered directly into the Pay.gov system. The credit card numbers are not stored at NCEI-NC. The information collected is as follows:

A. Name
B. Address
C. Email address (optional)
D. Phone number (optional)

This information is not shared outside the bureau except with Salesforce, for data analytics.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			

Private sector		X	
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: National Geophysical Data Center (NGDC)/NOAA5011, National Oceanographic Data Center (NGDC)/NOAA5010. HR info may be shared because the support services division has employees from each FISMA system who may need to access information on employees in another NCEI system. DOC authorized cloud service (SalesForce): NCEI sends public customer name/address info that was collected during order placement, for generation of analytic reports to understand representation by sector of those entities ordering data. Physical and logical access to PII/BII is restricted to authorized personnel only. Encryption is used for PII/BII in transit. Media is sanitized prior to disposal or reuse.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. A Privacy Act Statement is available at the NCDC customer order page and a form for PACs permission with a PAS is included at the end of this PIA, as it is a paper form. The NCEI Privacy Policy is also located on the customer order page of the online store. Link: https://www.ncei.noaa.gov/privacy.	
X	Yes, notice is provided by other means.	Specify how: Before an employee's/contractor's photograph can be used for internal use, notice is provided by means of the DOC written consent form requesting permission and obtaining the

		employee's signature. A Privacy Notice is posted at the registration station to those employees who require unescorted access to restricted areas. The notice reads, "As part of the registration process for the system granting access to the restricted area, the photo and fingerprint template will be collected from the CAC. This information is protected under the Privacy Act. Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent access to the restricted area." The authentication system requires the collection of the information stored on their government issued PIV card (photograph and fingerprint template.)
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: When ordering public data, the customer can choose not to enter their personal email address and phone number and still receive the data they ordered. Additionally, they can choose not to provide name and address but if so, they will be unable to receive the requested data. In the following circumstance individuals are provided instruction on the forms that they may decline to provide the information, but the related services could then not be provided: Employees must provide the General Personal Data and Social Security number (in hardcopy form) in order to receive an identification card once they have accepted employment. Employees/contractors may decline the use of their photographs for internal use by not granting permission via consent form. Employees who require unescorted access to restricted areas may also decline to provide a copy of the data on their PIV card (photograph, fingerprint template) (both the Privacy Act Statement and the sign state that the collection is voluntary) but this will affect their unescorted access.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Customers are provided a link to the Privacy Act Statement on the customer order page for data. The NOAA Web site privacy policy states "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose. When users click the "Submit" button on any of the Web forms found on our site, they are indicating voluntary consent to use of the information they submit for the stated purpose."

		Employee and contractor General Personal Data information is required for ID and emergency notifications. Employees are informed in writing (OF 306) of the use of their data at the time the information is collected when they are onboarding. This form is not stored in NOAA5009. Employees who require unescorted access to the restricted areas provide verbal consent to the collection of the information stored on their government issued PIV card (photograph and fingerprint template). Written consent is required before using employee photographs.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Customers ordering data can change their PII information under their account settings. Employees review and discuss performance plans with supervisors during annual performance plan meetings. Any updates will be made at this time. The NCEI-NC Contingency Plans are updated annually. Employees are requested to update their personal information. When employees who require access to restricted areas are issued new PIV (CAC) credentials. Their previous PIV information (photograph and fingerprint template) is deleted and replaced with the updated information on the PIV card.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: PII/BII on the system is located in access restricted folders. Access or attempted access to these folders is recorded in system logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/6/2017

	☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Physical and logical access to PII/BII is restricted to authorized personnel only.

All NOAA5009 monitors and printers are operated within NOAA5009 controlled spaces. Server consoles are located in the multi-factor access controlled computer room. NOAA5009 positions monitors away from windows whenever possible. Cubicle configuration within the financial branch are completely enclosed and designed with high partition walls.

Encryption is used for PII/BII in transit.
Backup tapes are encrypted and transported in locked containers.
Media is sanitized prior to disposal or reuse.
Shredders are available to NCEI personnel.

The physical access system database containing fingerprints and photos is encrypted at rest.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: NOAA-11, Contact Information for Members of Public Requesting or Providing Information Related to NOAA's Mission, COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies, COMMERCE/DEPT-25, Access Control and Identity Management System, GSA/Govt-7, Federal Personal Identity Verification Identity Management System.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 1: Civilian Personnel Records, GRS 20, item 3: Electronic Records That Replace Temporary Hard Copy Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: NOAA5009 maintains very little sensitive PII. The potential adverse effects of the PII collected (name, address, phone number) is limited.
X	Quantity of PII	Provide explanation: If NOAA5009 had a breach of PII, the number of employees affected would be less than 300.

X	Data Field Sensitivity	Provide explanation: NOAA5009 does not maintain sensitive PII on the information system.
X	Context of Use	Provide explanation: Cybersecurity Incident Response and employee performance information are part of the context.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Physical and logical access controls are in place.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Yes, creation of form with PAS, for PACS.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Yes, creation of form with PAS, for PACS.
	No, the conduct of this PIA does not result in any required technology changes.

PACS Consent Form

As part of the registration process for the system granting access to the restricted area, the photo and fingerprint template will be collected from the CAC. This information is protected under the Privacy Act of 1974 (5 U.S.C. Section 552a).

Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations and 15 U.S.C. 1512, Powers and duties of Department.

Purpose: Authentication for access to restricted areas.

Routine Uses: Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among Department staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-25 (http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html), Access Control and Identity Management System.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent access to the restricted area.

By signing this document I consent to providing the information stored on my CAC (name, photograph, and fingerprint) for use in gaining access to the computer room.

_____

Print Name

_____

Signature

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Jason Symonds, ISSO Office: NOAA/NESDIS/NCEI Phone: 828-271-4733 Email: Jason.Symonds@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: SYMONDS.JASON.T.1366777411 Digitally signed by SYMONDS.JASON.T.1366777411 Date: 2018.03.09 07:52:04 -05'00' Date signed:	**Information Technology Security Officer** Name: Nancy A. DeFrancesco Office: NOAA/NESDIS/ACIO-S Phone: 301-713-1312 Email: Nancy.DeFrancesco@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.06 07:42:18 -05'00' Date signed: 03/06/2018
Authorizing Official Name: Mary Wohlgemuth, co-AO Office: NOAA/NESDIS/NCEI Phone: 828-271-4848 Email: mary.wohlgemuth@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: WOHLGEMUTH.MARY.STANFORD.1228710519 Digitally signed by WOHLGEMUTH.MARY.STANFORD.1228710519 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=WOHLGEMUTH.MARY.STANFORD.1228710519 Date: 2018.03.15 17:33:50 -04'00' Date signed:	**Bureau Chief Privacy Officer** Name: Office: Phone: Email: I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 16:27:26 -04'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
National Centers for Environmental Information – NC NOAA5009

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Centers for Environmental Information – NC (NCEI-NC)

Unique Project Identifier: [006-48-00-00-01-3209-00-108-023]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: NOAA's National Centers for Environmental Information (NCEI)-NC maintains the world's largest climate data archive and provides climatological services and data to every sector of the U.S. economy and to users worldwide. Records in the archive range from paleoclimate data to centuries-old journals to data less than an hour old. The Center's mission is to preserve these data and make them available to the public, business, industry, government, and researchers.

NCEI-NC develops national and global datasets, which maximize the use of our climatic and natural resources while also minimizing the risks caused by climate variability and weather extremes. NCEI has a statutory mission to describe the climate of the United States and it acts as the "Nation's Scorekeeper" regarding the trends and anomalies of weather and climate. NCEI-NC's climate data have been used in a variety of applications including agriculture, air quality, construction, education, energy, engineering, forestry, health, insurance, landscape design, livestock management, manufacturing, national security, recreation and tourism, retail, transportation, and water resources management.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI-NC coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service. NCEI-NC manages and contributes to a variety of climate service partnerships including the Regional Climate Services Directors, Regional Climate Centers, State Climatologists, and Cooperative Institute for Climate and Satellites North Carolina. To facilitate a global data and information exchange, the Center also operates two World Data Centers one for meteorology and one for paleoclimatology and plays an active role in professional societies and user engagement activities.

NCEI-NC is a general support system with approximately 310 users that connect within NCEI-NC's security boundary. The NCEI-NC user environment consists mainly of web developers,

scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, graphic designers, order fulfillers, and computer operators. The system is located inside the Veach-Baley Federal Complex in Asheville, NC. The system interconnects with NOAA5006, NOAA5010, NOAA5011, NOAA5040, and NOAA-NWAVE. The NOAA5006, NOAA5010, and NOAA5011 interconnects provide user access to internal NCEI-NC resources. The NOAA5010 and NOAA-NWAVE interconnects provide a path to external resources.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

___Yes. *Please describe the activities which may raise privacy concerns.*

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

_X__ Companies
_X__ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X__ DOC employees
_X__ Contractors working on behalf of DOC
_X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the National Centers for Environmental Information NC and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the National Centers for Environmental Information NC and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Jason Symonds

Signature of ISSO or SO: SYMONDS.JASON.T.1366777411 Digitally signed by SYMONDS.JASON.T.1366777411 Date: 2018.03.09 07:53:44 05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Nancy DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.06 07:16:54 05'00' Date: 03/06/2018

Name of Authorizing Official (AO):

Mary Wohlgemuth

Signature of AO: WOHLGEMUTH.MARY.STANFORD.1228710519 Digitally signed by WOHLGEMUTH.MARY.STANFORD.1228710519 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=WOHLGEMUTH.MARY.STANFORD.1228710519 Date: 2018.03.15 17:36:27 04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO):

Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 16:25:09 04'00' Date: _____

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, March 21, 2018 7:33 AM
To:	Sarah Brabson NOAA Federal
Cc:	Jean Apedo NOAA Federal; Hadona Diep; Amit Sharma NOAA Affiliate
Subject:	Re: FW: Signature for PTA
Attachments:	NOAA1300_PTA_FY18 AO signed mhg.pdf

Hi Guys,

Looks good here it is signed. Thanks again

(b)(5) [redacted].

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) [redacted] (C)

On Mon, Mar 19, 2018 at 1:25 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, for your signature in anticipation of the PIA to be written.
> Forwarded message
> From: **Douglas Perry - NOAA Federal** <douglas.a.perry@noaa.gov>
> Date: Mon, Mar 19, 2018 at 1:24 PM
> Subject: Re: FW: Signature for PTA
> To: Jean Apedo NOAA Federal <jean.apedo@noaa.gov>
> Cc: Patrice Coleman NOAA Federal <patrice.coleman@noaa.gov>, Amit Sharma NOAA Affiliate <amit.sharma@noaa.gov>, Sarah Brabson <Sarah.Brabson@noaa.gov>
>
> See signed PTA.
>
> On Wed, Mar 14, 2018 at 10:37 AM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:
>
> > Doug,
> >
> > Attached is NOAA1300 PTA for your review. The document is being submitted due to the annual review requirement. Currently, NSDesk does not collect any sensitive data, but they will be doing so in the next few months. When that comes, we will be updating the PTA and generating a new PIA.

Thank you.

From: Sarah Brabson - NOAA Federal [mailto:sarah.brabson@noaa.gov]
Sent: Friday, March 09, 2018 2:11 PM
To: Jean Apedo - NOAA Federal
Cc: Amit Sharma - NOAA Affiliate
Subject: Re: Signature for PTA

I did already, sorry, Jean! No comments!

On Fri, Mar 9, 2018 at 1:49 PM, Jean Apedo NOAA Federal <jean.apedo@noaa.gov> wrote:

Doug

~~~~~~

Douglas A. Perry

Deputy Chief Information Officer
National Oceanic and Atmospheric Administration

Office: (301) 713-9600

www.noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6) [redacted]
~~~~~~

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA1300 NOAA National Service Desk (NSDesk)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOAA1300

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

NOAA1300 is system comprised of a cloud hosted service provided by ActioNet Inc, based upon their ActioNet Service Desk (ASD). Services are provided using infrastructure at two physically separate sites supporting Service Desk Agents, a cloud hosted environment providing the ServiceNow (SNow) application, and by an Automated Call Distribution (ACD) solution by Cisco to integrate voice with SNow for communication and collaboration. The Cisco ACD solution allows for call monitoring and recording for Service Desk staff to transfer to, or conference in other technicians. The ACD system is configured to answer calls in rotation. Queued calls are answered by the next free NSDesk technician.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X___ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden

name, etc..."

____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
__X__ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

__X__ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X___ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

__X___ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Amit Sharma NOAA1300 Information System Security Officer

Signature of ISSO or SO: SHARMA.AMIT.KUMAR.1399395000 Digitally signed by SHARMA.AMIT.KUMAR.1399395000 Date: 2018.03.09 12:00:40 05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Jean Apedo NOAA Information Technology Security Officer

Signature of ITSO: APEDO.JEAN.1188076064 Digitally signed by APEDO.JEAN.1188076064 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=APEDO.JEAN.1188076064 Date: 2018.03.14 10:31:35 04'00' Date: _____

Name of Authorizing Official (AO): Douglas A. Perry

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.03.19 13:23:21 04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.21 07:25:37 -04'00' Date: _____

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Tuesday, March 20, 2018 6:23 PM
To:	Sarah Brabson NOAA Federal
Cc:	Robert Swisher NOAA Federal; Ed Kearns NOAA Federal
Subject:	DEPT 18 Reviewed
Attachments:	DEPT 18 currently posted version mhg edits.docx

Hey Sarah,

Here is the currently posted version of DEPT 18 with a few proposed changes, including the yellow highlighted revisions you'd already identified need to be added.

Where this is the Department's SORN, if you could invite Mike T. to discuss any of the changes if he has questions or concerns in adding the proposed language. The two notable changes I suggested are:

(b)(5)

Other than these, I think we're good. Is there anything you see that I'm missing?

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, March 21, 2018 11:42 AM
To:	Maria Gonzalez NOAA Federal
Subject:	Re: Orientation Briefing for FOIA
Attachments:	FOIA Privacy and DLP Overview Final.pptx; NOAA FOIA Litigation as of 03.21.18.docx

Thank you Maria. In anticipation of the meeting, please find the attached files that go over the substance of the briefing, so that Kristen has them available.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

2018 03 21 11:39 GMT 04:00 <maria.j.gonzalez@noaa.gov>:

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

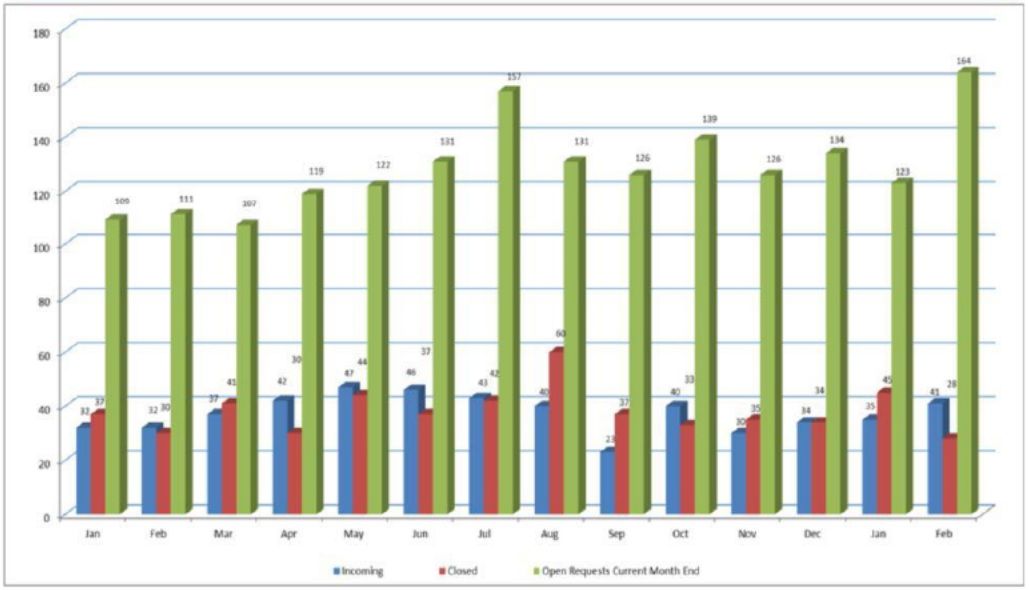
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

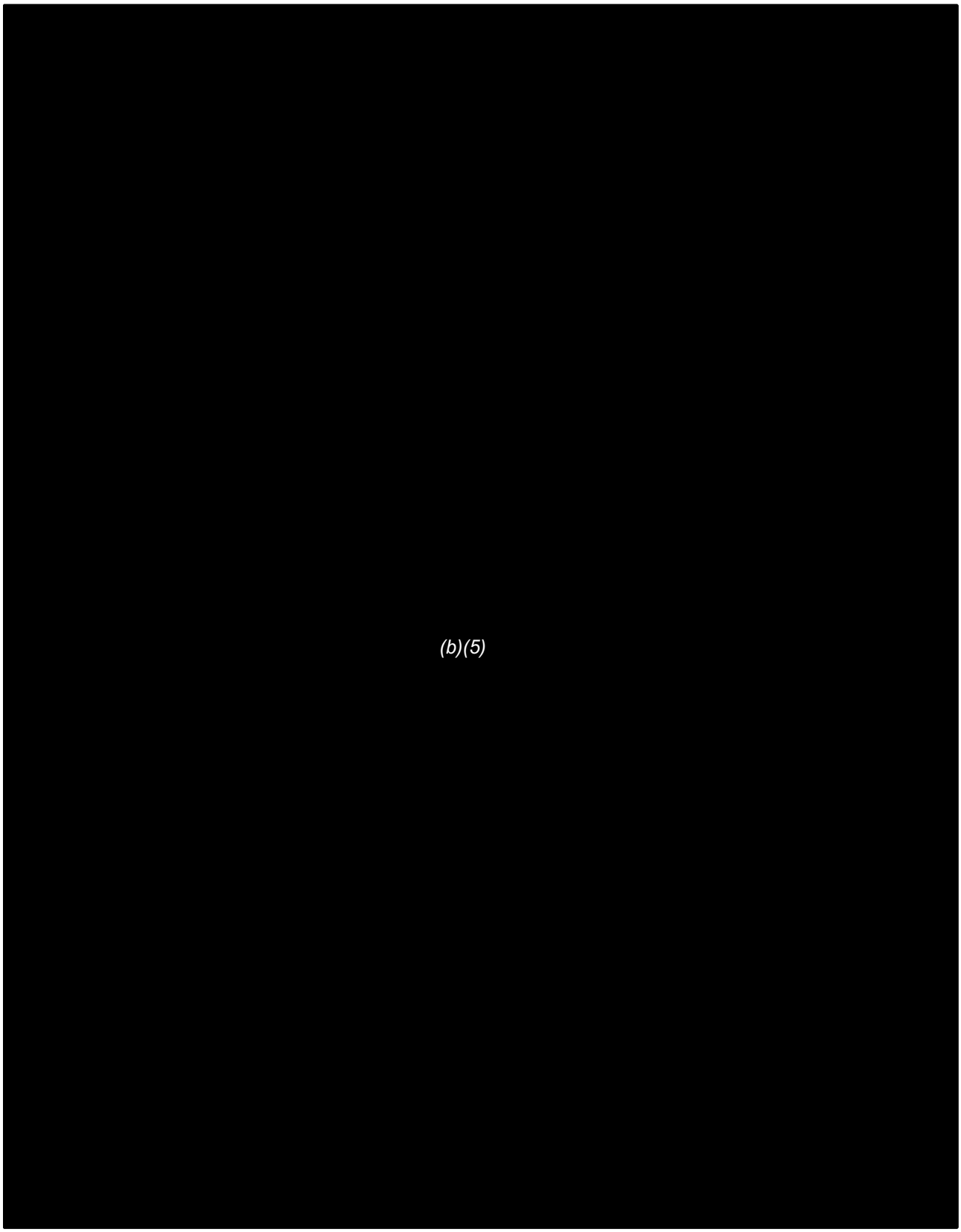
NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 21, 2018



Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, March 21, 2018 2:47 PM
To:	Kristen Koch NOAA Federal
Subject:	Slide Deck
Attachments:	NOAA FOIA Litigation as of 03.21.18.docx; FOIA Privacy and DLP Overview Final.pptx

As we are currently discussing.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

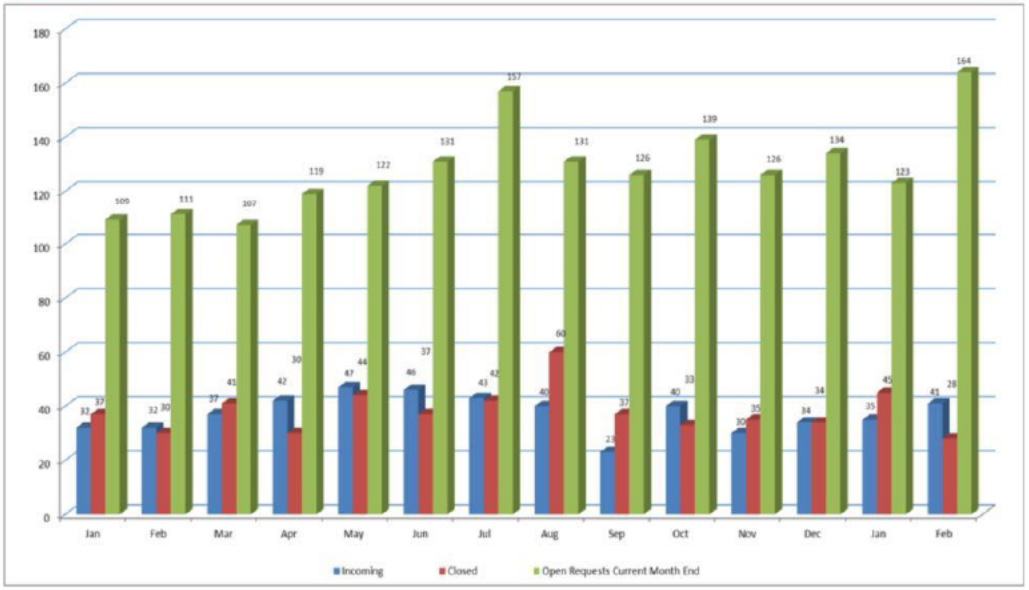
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

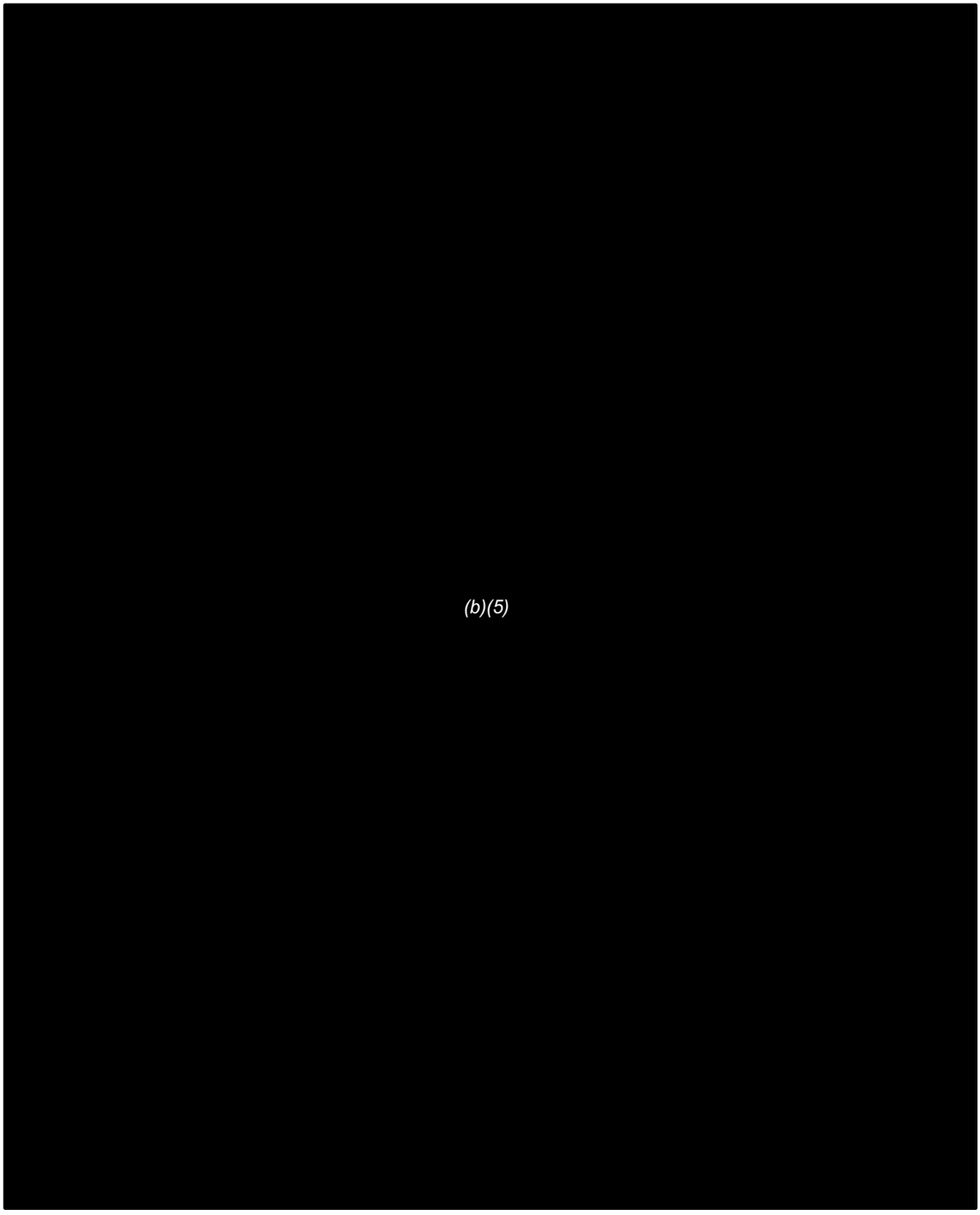
NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 21, 2018



Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, March 21, 2018 2:56 PM
To:	Gioffre, Kathy (Federal); CPO; Ferguson, Dorrie
Cc:	Mark Graff NOAA Federal; Jason Symonds NOAA Federal; Nancy Defrancesco
Subject:	NOAA5009 certification docs
Attachments:	NOAA5009_PTA_March 2018 v2 mhg.pdf; NOAA5009 certification 2018 for MHG signature mhg.pdf; NOAA5009_PIA2018 mhg.pdf

Kathy, attached are the NOAA5009 certification, the re signed PIA and a new PTA.

The ATO date is 8 6 18.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: National Climatic Data Center Local Area Network

FISMA Name/ID (if different): NOAA5009

Name of IT System/ Program Owner: Juanita Sandidge

Name of Information System Security Officer: Jason Symonds

Name of Authorizing Official(s): Mary Wohlgemuth, Irene Parker

Date of Last PIA Compliance Review Board (CRB): 6/22/17

(This date must be within three (3) years.)

Date of PIA Review: 2/28/2018

Name of Reviewer: Jason Symonds

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: SYMONDS.JASON.T.1366777411 Digitally signed by SYMONDS.JASON.T.1366777411 Date: 2018.03.05 12:36:08 -05'00'

Date of Privacy Act (PA) Review: 3/19/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 03 19 13 00 23 04'00'

Date of BCPO Review: 3/20/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 03 20 16 42 10 04'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Climatic Data Center Local Area Network (NOAA5009)

Reviewed by: _____Mark Graff_____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/National Climatic Data Center Local Area Network

Unique Project Identifier: 006-48-00-00-01-3209-00-108-023

Introduction: System Description

(a) NOAA's National Centers for Environmental Information (NCEI)-NC, a general support system, maintains the world's largest climate data archive and provides climatological services and data to every sector of the U.S. economy and to users worldwide. Records in the archive range from paleoclimate data to centuries-old journals to data less than an hour old. The Center's mission is to preserve these data and make them available to the public, business, industry, government, and researchers.

NCEI-NC develops national and global datasets, which maximize the use of our climatic and natural resources while also minimizing the risks caused by climate variability and weather extremes. NCEI has a statutory mission to describe the climate of the United States and it acts as the "Nation's Scorekeeper" regarding the trends and anomalies of weather and climate. NCEI-NC's climate data have been used in a variety of applications including agriculture, air quality, construction, education, energy, engineering, forestry, health, insurance, landscape design, livestock management, manufacturing, national security, recreation and tourism, retail, transportation, and water resources management.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI-NC coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service. NCEI-NC manages and contributes to a variety of climate service partnerships including the Regional Climate Services Directors, Regional Climate Centers, State Climatologists, and Cooperative Institute for Climate and Satellites North Carolina. To facilitate a global data and information exchange, the Center also operates two World Data Centers one for meteorology and one for paleoclimatology and plays an active role in professional societies and user engagement activities. *Data available through these partnerships does not require access accounts.*

NCEI-NC has approximately 310 users that connect within NCEI-NC's security boundary. The NCEI-NC user environment consists mainly of web developers, scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, graphic designers, order fulfillers, and computer operators.

(b) A typical transaction conducted on the system, where PII is collected, includes public access to data products via an ordering mechanism for customized order fulfillment.

(c) Information sharing is conducted by the system. As it relates to PII, NCEI-NC will share usernames with other NOAA entities in support of NOAA Incident Response (the system does not share this information directly with DOC). In addition, NCEI sends, to a FEDRAMP authorized cloud service (SalesForce at The Landmark @ One Market Suite 300 San Francisco, CA 94105), public customer name/address info that was collected during order placement. NCEI is trying to get meaningful information such as which products are important to a particular group of users or what particular variables within products customers from various sectors are asking for (ex. temperature, precipitation, irradiance). We are also interested in seeing how those requests change over time so that we can make sure NCEI is not under- or over-investing in any particular product or portfolio. If possible, we would also like to capture benefits that users derive from the data. Without some individual identifier, we could not determine how customer needs change, we would only be able to see the mass movement of users as a whole or an entire sector.

(d) The legal authority for collection of information addressed in this PIA is: 5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records; additional authorities: 44 U.S.C. 3101, Records Management by Agency Heads; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; Government Paperwork Elimination Act (Pub. L. 105 277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD 12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

(e) NOAA5009 is categorized as a FIPS 199 moderate system.

NCEI-NC has various requirements to collect PII from its employees. These include employee contact information for contingency planning, information related to performance plans, photographs for internal use, and biometric information used to authenticate certain employees to restricted areas. The following information is collected and maintained:

A. Employee's Name
B. Personal email address
C. Personal phone number
D. Photograph for internal use (voluntary posting to intranet for face recognition)
E. Dates for the period of performance
F. Title, Series, and Grade of the position

G. Employee's Division
H. Information about the employee's work and work performance, constituting the plan or appraisal
I. Photograph (copied from government issued PIV card)
J. Fingerprint template file (copied from government issued PIV card)

NCEI-NC offers data to the public through its website. In order for the data to be shipped to the customer, the customer must provide their name and mailing address. It is optional for the customer to leave their phone number and email address as another way of communication. NCEI-NC website utilizes a third party for submitting and authorizing credit cards for data product purchase that require payment. Those credit card numbers are entered directly into the Pay.gov system. The credit card numbers are not stored at NCEI-NC. The information collected is as follows:

A. Name
B. Address
C. Email address (optional)
D. Phone number (optional)

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
_ __ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X__ This is an existing information system in which changes do not create new privacy risks and for which there is an SAOP-approved PIA.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance information					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X*	d. Photographs	X**	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

*From the CAC, to generate the building registration card.

** From the CAC, and for internal use after signed consent.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics*	X
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

*A physical access control system (PACS) is in place to authorize employees who require access to the computer room. This system requires the employee to present their government issued PIV card and their fingerprint to register; once registered, the CAC only is required. The PACS system stores the PIV information on a database in a restricted network where only IT Security personnel have access.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

- Entry points into the computer room and within the computer room are under video surveillance, with warning signs posted. The cameras record on motion and the video files stored on an air gapped system. Access to that system is restricted to the computer operators (staff and contractors) and the IT Security team.

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Continuity of Operations (COOP); Physical Access Control Authorization; Cybersecurity Incident Response			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

NCEI-NC has various requirements to collect PII from its employees. These include employee contact information for contingency planning, information related to performance plans, photographs for internal use, and biometric information used to authenticate certain employees to restricted areas. The following information is collected and maintained:

A. Employee's Name
B. Personal email address
C. Personal phone number
D. Photograph for internal use (voluntarily posted to the intranet for face recognition)
E. Dates for the period of performance
F. Title, Series, and Grade of the position
G. Employee's Division
H. Information about the employee's work and work performance, constituting the plan or appraisal
I. Photograph (copied from government issued PIV card) for computer room access
J. Fingerprint template file (copied from government issued PIV card) for computer room access

Information is not shared outside the bureau unless there is a breach notification.

NCEI-NC offers data to the public through its website. If data delivery is not feasible online, then an alternative method is direct shipment to the customer. In order for the data to be shipped, the customer must provide their name and mailing address. It is optional for the customer to leave their phone number and email address as another way of communication. The NCEI-NC website utilizes a third party for submitting and authorizing credit cards for data product purchase that require payment. Those credit card numbers are entered directly into the Pay.gov system. The credit card numbers are not stored at NCEI-NC. The information collected is as follows:

A. Name
B. Address
C. Email address (optional)
D. Phone number (optional)

This information is not shared outside the bureau except with Salesforce, for data analytics.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			

Private sector		X	
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: National Geophysical Data Center (NGDC)/NOAA5011, National Oceanographic Data Center (NGDC)/NOAA5010. HR info may be shared because the support services division has employees from each FISMA system who may need to access information on employees in another NCEI system. DOC authorized cloud service (SalesForce): NCEI sends public customer name/address info that was collected during order placement, for generation of analytic reports to understand representation by sector of those entities ordering data. Physical and logical access to PII/BII is restricted to authorized personnel only. Encryption is used for PII/BII in transit. Media is sanitized prior to disposal or reuse.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. A Privacy Act Statement is available at the NCDC customer order page and a form for PACs permission with a PAS is included at the end of this PIA, as it is a paper form. The NCEI Privacy Policy is also located on the customer order page of the online store. Link: https://www.ncei.noaa.gov/privacy.	
X	Yes, notice is provided by other means.	Specify how: Before an employee's/contractor's photograph can be used for internal use, notice is provided by means of the DOC written consent form requesting permission and obtaining the

		employee's signature. A Privacy Notice is posted at the registration station to those employees who require unescorted access to restricted areas. The notice reads, "As part of the registration process for the system granting access to the restricted area, the photo and fingerprint template will be collected from the CAC. This information is protected under the Privacy Act. Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent access to the restricted area." The authentication system requires the collection of the information stored on their government issued PIV card (photograph and fingerprint template.)
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: When ordering public data, the customer can choose not to enter their personal email address and phone number and still receive the data they ordered. Additionally, they can choose not to provide name and address but if so, they will be unable to receive the requested data. In the following circumstance individuals are provided instruction on the forms that they may decline to provide the information, but the related services could then not be provided: Employees must provide the General Personal Data and Social Security number (in hardcopy form) in order to receive an identification card once they have accepted employment. Employees/contractors may decline the use of their photographs for internal use by not granting permission via consent form. Employees who require unescorted access to restricted areas may also decline to provide a copy of the data on their PIV card (photograph, fingerprint template) (both the Privacy Act Statement and the sign state that the collection is voluntary) but this will affect their unescorted access.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Customers are provided a link to the Privacy Act Statement on the customer order page for data. The NOAA Web site privacy policy states "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose. When users click the "Submit" button on any of the Web forms found on our site, they are indicating voluntary consent to use of the information they submit for the stated purpose."

		Employee and contractor General Personal Data information is required for ID and emergency notifications. Employees are informed in writing (OF 306) of the use of their data at the time the information is collected when they are onboarding. This form is not stored in NOAA5009. Employees who require unescorted access to the restricted areas provide verbal consent to the collection of the information stored on their government issued PIV card (photograph and fingerprint template). Written consent is required before using employee photographs.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Customers ordering data can change their PII information under their account settings. Employees review and discuss performance plans with supervisors during annual performance plan meetings. Any updates will be made at this time. The NCEI-NC Contingency Plans are updated annually. Employees are requested to update their personal information. When employees who require access to restricted areas are issued new PIV (CAC) credentials. Their previous PIV information (photograph and fingerprint template) is deleted and replaced with the updated information on the PIV card.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: PII/BII on the system is located in access restricted folders. Access or attempted access to these folders is recorded in system logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/6/2017

	☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Physical and logical access to PII/BII is restricted to authorized personnel only.

All NOAA5009 monitors and printers are operated within NOAA5009 controlled spaces. Server consoles are located in the multi-factor access controlled computer room. NOAA5009 positions monitors away from windows whenever possible. Cubicle configuration within the financial branch are completely enclosed and designed with high partition walls.

Encryption is used for PII/BII in transit.
Backup tapes are encrypted and transported in locked containers.
Media is sanitized prior to disposal or reuse.
Shredders are available to NCEI personnel.

The physical access system database containing fingerprints and photos is encrypted at rest.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: NOAA-11, Contact Information for Members of Public Requesting or Providing Information Related to NOAA's Mission, COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies, COMMERCE/DEPT-25, Access Control and Identity Management System, GSA/Govt-7, Federal Personal Identity Verification Identity Management System.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 1: Civilian Personnel Records, GRS 20, item 3: Electronic Records That Replace Temporary Hard Copy Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: NOAA5009 maintains very little sensitive PII. The potential adverse effects of the PII collected (name, address, phone number) is limited.
X	Quantity of PII	Provide explanation: If NOAA5009 had a breach of PII, the number of employees affected would be less than 300.

X	Data Field Sensitivity	Provide explanation: NOAA5009 does not maintain sensitive PII on the information system.
X	Context of Use	Provide explanation: Cybersecurity Incident Response and employee performance information are part of the context.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Physical and logical access controls are in place.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

PACS Consent Form

As part of the registration process for the system granting access to the restricted area, the photo and fingerprint template will be collected from the CAC. This information is protected under the Privacy Act of 1974 (5 U.S.C. Section 552a).

Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations and 15 U.S.C. 1512, Powers and duties of Department.

Purpose: Authentication for access to restricted areas.

Routine Uses: Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among Department staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-25 (http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html), Access Control and Identity Management System.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent access to the restricted area.

By signing this document I consent to providing the information stored on my CAC (name, photograph, and fingerprint) for use in gaining access to the computer room.

_____

Print Name

_____

Signature

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Jason Symonds, ISSO Office: NOAA/NESDIS/NCEI Phone: 828-271-4733 Email: Jason.Symonds@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: SYMONDS.JASON.T.1366777411 Digitally signed by SYMONDS.JASON.T.1366777411 Date: 2018.03.09 07:52:04 -05'00' Date signed:	**Information Technology Security Officer** Name: Nancy A. DeFrancesco Office: NOAA/NESDIS/ACIO-S Phone: 301-713-1312 Email: Nancy.DeFrancesco@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.06 07:42:18 -05'00' Date signed: 03/06/2018
Authorizing Official Name: Mary Wohlgemuth, co-AO Office: NOAA/NESDIS/NCEI Phone: 828-271-4848 Email: mary.wohlgemuth@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: WOHLGEMUTH.MARY.STANFORD.1228710519 Digitally signed by WOHLGEMUTH.MARY.STANFORD.1228710519 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=WOHLGEMUTH.MARY.STANFORD.1228710519 Date: 2018.03.15 17:33:50 -04'00' Date signed:	**Bureau Chief Privacy Officer** Name: Office: Phone: Email: I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 16:27:26 -04'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
National Centers for Environmental Information – NC NOAA5009

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Centers for Environmental Information – NC (NCEI-NC)

Unique Project Identifier: [006-48-00-00-01-3209-00-108-023]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: NOAA's National Centers for Environmental Information (NCEI)-NC maintains the world's largest climate data archive and provides climatological services and data to every sector of the U.S. economy and to users worldwide. Records in the archive range from paleoclimate data to centuries-old journals to data less than an hour old. The Center's mission is to preserve these data and make them available to the public, business, industry, government, and researchers.

NCEI-NC develops national and global datasets, which maximize the use of our climatic and natural resources while also minimizing the risks caused by climate variability and weather extremes. NCEI has a statutory mission to describe the climate of the United States and it acts as the "Nation's Scorekeeper" regarding the trends and anomalies of weather and climate. NCEI-NC's climate data have been used in a variety of applications including agriculture, air quality, construction, education, energy, engineering, forestry, health, insurance, landscape design, livestock management, manufacturing, national security, recreation and tourism, retail, transportation, and water resources management.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI-NC coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service. NCEI-NC manages and contributes to a variety of climate service partnerships including the Regional Climate Services Directors, Regional Climate Centers, State Climatologists, and Cooperative Institute for Climate and Satellites North Carolina. To facilitate a global data and information exchange, the Center also operates two World Data Centers one for meteorology and one for paleoclimatology and plays an active role in professional societies and user engagement activities.

NCEI-NC is a general support system with approximately 310 users that connect within NCEI-NC's security boundary. The NCEI-NC user environment consists mainly of web developers,

scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, graphic designers, order fulfillers, and computer operators. The system is located inside the Veach-Baley Federal Complex in Asheville, NC. The system interconnects with NOAA5006, NOAA5010, NOAA5011, NOAA5040, and NOAA-NWAVE. The NOAA5006, NOAA5010, and NOAA5011 interconnects provide user access to internal NCEI-NC resources. The NOAA5010 and NOAA-NWAVE interconnects provide a path to external resources.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

___Yes. *Please describe the activities which may raise privacy concerns.*

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

_X__ Companies
_X__ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X__ DOC employees
_X__ Contractors working on behalf of DOC
_X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the National Centers for Environmental Information NC and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the National Centers for Environmental Information NC and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Jason Symonds

Signature of ISSO or SO: SYMONDS.JASON.T.1366777411 Digitally signed by SYMONDS.JASON.T.1366777411 Date: 2018.03.09 07:53:44 05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Nancy DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.06 07:16:54 05'00' Date: 03/06/2018

Name of Authorizing Official (AO):

Mary Wohlgemuth

Signature of AO: WOHLGEMUTH.MARY.STANFORD.1228710519 Digitally signed by WOHLGEMUTH.MARY.STANFORD.1228710519 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=WOHLGEMUTH.MARY.STANFORD.1228710519 Date: 2018.03.15 17:36:27 04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO):

Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 16:25:09 04'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, March 21, 2018 3:01 PM
To:	Gioffre, Kathy (Federal); CPO; Ferguson, Dorrie
Cc:	Mark Graff NOAA Federal; Nancy Defrancesco; Brian.Little
Subject:	NOAA5044 certification docs
Attachments:	NOAA5044 Annual Review Certification Form for MHG signature mhg.pdf; NOAA5044 PIA_Feb18 mhg.pdf; NOAA5044_PTA_Feb2018_BL_ND_VG for MHG signature mhg.pdf

Kathy, attached are the certification, the re signed PIA and a new PTA.

The ATO is not till 12 15 2018 but since this is ready we are sending.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2015

U.S. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA)

Privacy Impact Assessment
for the
NOAA5044
NOAA Satellite Operations Facility (NSOF) Administrative LAN

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
[NESDIS/NOAA5044]

Unique Project Identifier: 006-000351101 00-00-02-00-02-00

Introduction: System Description

System Description:

(a) General Description NSOF Admin LAN (NOAA5044) is physically located in the NOAA building at 4231 Suitland Road, Suitland, Maryland, a suburb of Washington, D.C. The building is owned by NOAA and managed and secured by the General Services Administration. The NSOF Admin LAN provides standard office automation for all NESDIS employees located within the NSOF. It also provides access to the Internet. The LAN provides end-to-end connectivity and network access to all LAN Federal employee and contract users, to increase productivity through the use of applications, data resources, or other electronic office automation tools.

The two types of applications supported by the NSOF Admin LAN -- server applications and client applications -- are considered minor applications in that they are accredited as a GSS rather than separately. There are no major applications (as defined by OMB A-130) in the NSOF Admin LAN environment.

There are five user communities located in the NSOF: the Office of Satellite Ground Systems (OSGS), the Office of Satellite and Product Operations (OSPO), the General Services Administration (GSA), the National Ice Center (NIC) and the Defense Meteorological Satellite Program (DMSP). These user communities have dedicated workstations connected to the NSOF Admin LAN.

NOAA5044 provides access to automated programs and systems supporting administrative programs such as budget and financial management, personnel management, procurement, building operation and management, interagency programs, IT planning, and IT security. The system also supports access to the Internet.

There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking.

DOC and DOD performance evaluation are also compiled and maintained in the system. The appropriate forms are completed on the NOAA5044 Manager's secure home directory. They are then printed, hand-carried for signature, and then transferred via the agency-specific secure electronic transfer procedure.

There is also ESPC account management, collecting contact information from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored in restricted areas of the shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.

In addition, the NOAA5044 collects PII of NSOF LAN personnel on a voluntary basis for purposes of Continuity of Operations Planning (COOP). This data is stored on a LAN shared drive only accessible by authorized personnel.

(c) The PII/BII information collected by NOAA5044 is shared with other agencies or parties on a case-by-case basis, as described below. If any of the data is sensitive or For Official Use Only (FOUO), then the data is restricted by drives and folders to only NSOF Admin LAN personnel authorized to access the information.

Transfers - The system collects PII of DOC (NOAA employees only) and DOD civilian and military personnel to the extent necessary for preparation of performance, promotion, and awards for these personnel. The NSOF Admin LAN contains personally assigned network shares (H:\), which are accessible only by the person assigned the shared drive.

DOC electronic personnel related forms (NOAA employees only) may be transferred to DOC Bureau HR personnel in bulk or on a case-by-case basis via DOC Accellion (for DOC records only) or via tracked United Parcel Service (UPS) package.

(d) Authority - Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1512 (Powers and Duties of the Department of Commerce)
- 5 USC 2101 to 10210 (Government Organizations and Employees, Part III, Employees)
- 5 USC 301 (Departmental Regulations)
- 10 USC 8010 to 9448 (Armed Forces - Air Force - Organization, Personnel, and Training)
- 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.
- E.O. 9397; E.O. 12931; 40 U.S.C. Sec. 501 502.
- 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended

by 13478, 9830, and 12107.

- 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107 347, Sec. 203), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105 277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD 12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.
- Sections 1104, 3321, 4305, and 5405 of Title 5, U.S. Code, and Executive Order 12107.
- Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c); FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989)
- E-Government Act of 2002 (Pub. L. 107 347) Section 204; Davis-Bacon and Related Acts: 40 U.S.C. 3141 3148 40 U.S.C. 276a; 29 CFR parts 1, 3, 5, 6 and 7; Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113 101.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
- Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016)

(e) Categorization NOAA5044 NSOF Admin LAN is a FIPS 199 moderate impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

X This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII)

is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	X
b. Taxpayer ID		f. Driver's License	X**	j. Financial Account	X
c. Employer ID		g. Passport	X**	k. Financial Transaction	X***
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Performance and award forms require the individual's SSN. *The Navy requires SSN in its performance evaluation guidance (document provided with PIA). See Section 5.1, Item 5.* **For CAC ***Contract information					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
Offeror responses to RFIs and RFPs, confidential/proprietary

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	X
Video surveillance		Electronic purchase transactions	X
Other (specify):			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

1) There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking. The documents are usually completed by the individual or preparer (administrative person that prepares the document for an individual employee). The files are sent to an HR system via DOC Accellion, but copies are stored on the NSOF Admin LAN. This information is not shared with anyone beyond those that are required to process it within the respective bureau.
2) For contractual and budgetary purposes, the NSOF admin LAN stores procurement and contract information, purchase requests, and accounting information which is stored locally or in restricted areas of the shared drive accessible only by authorized personnel.
3) The system's audit logs collect User ID, IP Address, Date/Time of Access, Queries Run, and ID Files accessed on the network and stored locally or into restricted areas of the server that are only accessible by authorized personnel. The NOAA Directory collects PII in the form of name, email and contact number for Continuity Of

Operations Plan (COOP). This information is stored on the NSOF Admin LAN and is accessible by authorized personnel.

4) Environmental Satellite Processing Center (ESPC), NOAA5045, account management processes typically collect name, address, phone number, and email address from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored locally or into restricted areas of the shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.
5) Performance awards that contain full Social Security Numbers for military and civilians assigned to the Naval Ice Center are stored on the NSOF Admin LAN. Access to the folder is restricted to those that have a need to know.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	
DOC bureaus	X		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*With OPM if an employee hired by another agency

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA WFMO Recruitment Analysis Data System (RADS). NOAA5044 uploads data in specified formats to RADS. NSOF LAN has media protection controls in place as well as user procedures on how to protect this information.

	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.ospo.noaa.gov/Organization/About/access.html. The COOP form with PAS was enclosed in the cover email. It is not posted on the Web but kept in a shared drive.	
X	Yes, notice is provided by other means.	Specify how: a. Written notice is included on all personnel forms that employees complete. b. For DOC and DOD performance/award documents, employees are informed by their supervisors that the evaluations are in process. Employees have access to view the official documents. c. For NSOF LAN COOP or emergency recall in the NOAA directory, employees are notified in writing when collecting the applicable information. d. For ESPC, information is voluntarily submitted when a user completes the account request form. e. For responses to solicitations, notice is given on the request for information (RFI) or request for proposal (RFP).
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: a. An individual may decline to provide PII when applying for a position, by not completing all required

		forms, but his or her employment status may be affected. b. For DOD and DOC personnel data, employees may opt not to provide PII – at the time of the request, and in writing to the personnel administration representative who is assisting them - but this information is needed for processing awards. Performance information is part of the official personnel record for DOD and DOC employees and information is added to the eOPF in conjunction with the employee mid-year and annual reviews. The performance record/information is required in order to conduct performance evaluations. c. For NSOF LAN COOP or emergency recall in the NOAA directory, employees are asked permission in writing by their supervisors when collecting the applicable information, and may decline at that time. This information is not required. d. For ESPC, information is voluntarily submitted through email and is stored locally. An individual may choose not to provide the information, by not answering the questions, but then will not have access to requested information. e. Responses to RFPs/RFIs are voluntary, based on the offeror's decision to respond.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: a. There is only one use for information provided during employee onboarding. b. Consent is included on all personnel forms that employees complete, and consent to the uses explained on the forms is implied by completion of the forms. c. For DOD and DOC personnel data, employees may opt not to provide PII – at the time of the request, and in writing to the personnel administration representative who is assisting them, but this information is needed for processing awards. Performance information is part of the official personnel record for DOD and DOC employees and information is added to the eOPF in conjunction with the employee mid-year and annual reviews. The performance record/information is required in order to conduct performance evaluations. This is the only use. d. For NSOF LAN COOP or emergency recall, there is only one use, and consent to that use is implied by the voluntary provision of the information for that intended use.

		e. For ESPC, the only use is to provide information as requested. f. For contract offerers, there is only one use of the BII information provided and acceptance of that use is implied by proposal submission.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: a. An employee may update information on personnel forms at any time by contacting their HR representative This is explained during employee orientation. b. For DOD personnel data, employees may update their PII– by contacting their HR representative, as explained during orientation. Employees review information in the eOPF and notify HR of errors. c. b. For Emergency and COOP information, the employee may not review the information, because it contains other staff's PII unless there is need-to-know, but may request updates from the assigned administrative staff, as explained by that staff when requesting the information. d. For ESPC, information can be updated by contacting the ESPC help desk. – as stated on the Web page. e. Offerors will contact the office with updated BII information.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: If someone who doesn't have access and attempts to access to a folder containing PII/BII, then a failed access log is created. Audit logs from each computer system are recorded and monitored with various tools including Tripwire, Solarwinds and ArcSight. NOAA5044 has local monitoring tools on the servers having PII, such as FireEye Agent and Tripwire Enterprise/Log Center. FireEye Agent is managed by NOAA to monitor any potential threats to the system and data. Tripwire Enterprise/Log Center provides real time monitoring and threat alerts.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 12/15/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): As stated in the NSOF Admin LAN System Security Plan (SSP), all employees and contractors undergo a national agency check with inquiries (NACI) security check when employed or contracted. This involves a check of Federal and local law enforcement records to help ensure the trustworthiness of the employee. The user (internal or external) signs the NSOF LAN Rules of Behavior (ROB) indicating that they have read and understand the ROB. To protect mobile information, all NSOF Admin LAN laptops are fully encrypted using the NOAA enterprise supplied encryption software.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

PII/BII is protected through a combination of measures, including operational safeguards, privacy specific safeguards, and security controls. Policies and awareness training are provided annually. The minimum amount of PII necessary to meet the mission is collected.
Security controls are in place, such as access controls limiting access to PII/BII. This information has restricted access limited to authorized NOAA staff. Further, if someone that doesn't have access attempts to access to a folder containing PII/BII, then a failed access log is created. The NSOF Admin LAN has a dedicated drive with user access restrictions for those that store PII/BII.
The NSOF Admin LAN has NIST 800-53 Rev 4 security controls in place, including, but not limited to: the Access Control family, limiting access to allow only the necessary functions for users to operate within the NSOF Admin LAN. Account privileges are tied directly to job function and designed to enable the user to accomplish only what the job requires and no more. The Audit and Accountability family utilizes tools such as Tripwire to record, store and manage logs for auditable events. For the Identification and Authentication family, NOAA5044 utilizes two factor to identify and authenticate users. The Media Protection family to monitor access to stored data and the approved sanitation methods for all media. NOAA5044 uses approved DOD sanitization software to ensure no data remains on NOAA5044 media. NOAA5044 is monitored using various tools including Solarwinds, Nessus, McAfee, and Cisco IPS. Also, NOAA5044 has enterprise monitoring tools, such as FireEye. FireEye is managed by NOAA and provides real time monitoring of potential threats to the system and data.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: DEPT-13, *Investigative and Security Records* DEPT-18, *Employees Information Not Covered by Records of Other Agencies*. NOAA-11, *Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission*; OPM/GOVT-1, *General Personnel Records*, OPM/GOVT-2, *Employees Performance File Records*, GSA-GOVT-6, *GSA SmartPay Purchase Charge Card Program*, GSA-GOVT -7, *Federal Personal Identity Verification Identity Management System (PIV IDMS)*, GSA-GOVT-9, *System for Award Management*, GSA-GOVT-10, *Federal Acquisition Regulation (FAR) Data Collection System*
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Chapter 100 – General, Chapter 200 – Administrative and Housekeeping Records, and Chapter 300 – Personnel.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified based on the PII stored.
X	Quantity of PII	Provide explanation: There is a large amount of PII in the system.
X	Data Field Sensitivity	Provide explanation: There are several types of sensitive PII/BII collected.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access to PII is restricted to need to know. If someone that doesn't have access and attempts to access to a folder

		containing PII/BII, then a failed access log is created. We also employ security monitoring tools that can detect PII in unauthorized locations. We also employ security monitoring tools that can detect PII in unauthorized locations.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Brian Little Office: DOC\NOAA\OSPO Phone: (301) 817-3899 Email: Brian.Little@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 Date: 2018.03.13 14:00:35 -04'00' Date signed:	**Information Technology Security Officer** Name: Nancy DeFrancesco Office: DOC\NOAA\NESDIS Phone: (301) 713-1312 Email: Nancy.DeFrancesco@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.13 15:23:20 -04'00' Date signed: 03/13/2018
Authorizing Official Name: Vanessa L. Griffin Office: DOC\NOAA\NESDIS\OSPO Phone: (301) 817-4607 Email: Vanessa.L.Griffin@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.15 16:36:00 -04'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: DOC\NOAA\CPO Phone: (301) 628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 16:04:41 04'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA/NSOF Administrative LAN (NSOF Admin LAN) (NOAA5044)

FISMA Name/ID (if different): NSOF Administrative LAN (NSOF Admin LAN) / NOAA5044

Name of IT System/ Program Owner: Andre' Hammond

Name of Information System Security Officer: Brian Little

Name of Authorizing Official(s): Vanessa Griffin

Date of Last PIA Compliance Review Board (CRB): 11/02/2017

(This date must be within three (3) years.)

Date of PIA Review: 2/20/2018

Name of Reviewer: Brian Little

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 Date: 2018.02.20 11:34:29 -05'00'

Date of Privacy Act (PA) Review: 3/16/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 03 16 12 23 09 04'00'

Date of BCPO Review: 3.20.18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 03 20 16 02 25 04'00'

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA5044
NOAA Satellite Operations Facility (NSOF) Administrative LAN

U.S. Department of Commerce Privacy Threshold Analysis

NOAA5044

NOAA Satellite Operations Facility (NSOF) Administrative LAN

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

General Description NSOF Admin LAN (NOAA5044) is a FIPS 199 moderate designated general support system that is physically located in the NOAA building at 4231 Suitland Road, Suitland, Maryland, a suburb of Washington, D.C. The building is owned by NOAA and managed and secured by the General Services Administration. The NSOF Admin LAN provides standard office automation for all NESDIS employees located within the NSOF. It also provides access to the Internet. The LAN provides end-to-end connectivity and network access to all LAN Federal employee and contract users, to increase productivity through the use of applications, data resources, or other electronic office automation tools.

The two types of applications supported by the NSOF Admin LAN -- server applications and client applications -- are considered minor applications in that they are accredited as a GSS rather than separately. There are no major applications (as defined by OMB A-130) in the NSOF Admin LAN environment.
There are five user communities located in the NSOF: the Office of Satellite Ground Systems (OSGS), the Office of Satellite and Product Operations (OSPO), the General Services Administration (GSA), the National Ice Center (NIC) and the Defense Meteorological Satellite Program (DMSP). These user communities have dedicated workstations connected to the NSOF Admin LAN. NOAA5044 provides access to automated programs and systems supporting administrative programs such as budget and financial management, personnel management, procurement, building operation and management, interagency programs, IT planning, and IT security. The system also supports access to the Internet. There is electronic personnel related information about NOAA employees and prospective employees maintained on the NSOF Admin LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone

Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking. Version Number: 01-2015

DOC and DOD performance evaluation are also compiled and maintained in the system. The appropriate forms are completed on the NOAA5044 Manager's secure home directory. They are then printed, hand-carried for signature, and then transferred via the agency-specific secure electronic transfer procedure.
There is also ESPC account management, collecting contact information, such as name, work phone number and work email address from individuals or organizations wishing to access ESPC data via its distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored in restricted areas of the NSOF Admin LAN shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.
In addition, the NOAA5044 collects PII of NSOF LAN personnel on a voluntary basis for purposes of Continuity of Operations Planning (COOP). This data is stored on a LAN shared drive only accessible by authorized personnel.
The PII/BII information collected by NOAA5044 is shared with other agencies or parties on a case-by-case basis, as described below. If any of the data is sensitive or For Official Use Only (FOUO), then the data is restricted by drives and folders to only NSOF Admin LAN personnel authorized to access the information.

NSOF Admin LAN currently has interconnections with 6 other NOAA systems. NOAA5044 is connected to NOAA0100 via network using SSL Protection transmitting and receiving unclassified information. NOAA5044 is connected to NOAA0200 via network using SSL protection to send but not receive unclassified data. NOAA5044 is connected to NOAA5006 via network using a site to site VPN to transmit and receive unclassified data. NOAA5044 is connected to NOAA5008 via network using a site to site VPN to send unclassified data. NOAA5044 is connected to NOAA5032 via network using a site to site VPN to send unclassified data. NOAA5044 is connected to NOAA5040 via network using SSL Protection transmitting and receiving unclassified information.

Transfers - The system collects PII of DOC (NOAA employees only) and DOD civilian and military personnel to the extent necessary for preparation of performance, promotion, and awards for these personnel. The NSOF Admin LAN contains personally assigned network shares (H:\), which are accessible only by the person assigned the shared drive.
DOC electronic personnel related forms (NOAA employees only) may be transferred to DOC Bureau HR personnel in bulk or on a case-by-case basis via DOC Accellion (for DOC records only) or via tracked United Parcel Service (UPS) package.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_X_ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

_X_ Companies
_X_ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X_ DOC employees
_X_ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA5044 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA5044 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Brian Little, NOAA5044 ISSO

Signature of ISSO or SO: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 Date: 2018.03.13 15:03:02 04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Nancy A. DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.13 15:21:20 04'00' Date: 03/13/2018

Name of Authorizing Official (AO): Vanessa L. Griffin

Signature of AO: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.15 16:34:59 04'00' Date: 03/15/2018

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 16:06:22 -04'00' Date: 3/20/18

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 22, 2018 9:06 AM
To:	Sean Mcmillan NOAA Federal
Cc:	_OMAO HQ ITSO; Mark Graff NOAA Federal
Subject:	Re: NOAA2220 NOAA Ship Fleet Support System
Attachments:	NOAA2220 Annual Review Certification Form _BCPO signature required mhg.pdf; NOAA2220 PTA_01_23_2018_final_v2_requires_signatures_itso_isso_AO mhg.pdf

Here are the certification and the PTA.

On Thu, Mar 22, 2018 at 9:02 AM, Sean Mcmillan NOAA Federal <sean.t.mcmillan@noaa.gov> wrote:

> hmm..can you please resend me the other too?
> Thanks
>
> Sean T. McMillan (CISSP, C|EH, GIAC(GCIH))
> Information System Security Officer (ISSO)
> Office of Marine and Aviation Operations (OMAO)
> Marine and Aviation Cyber Center (MACC)
> Office: 863-500-3924
> sean.t.mcmillan@noaa.gov
>
> On Thu, Mar 22, 2018 at 8:48 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > I sent you the signed PIA. Did I not send you the other two docs after Mark signed? Or do you just mean the website posting?
> >
> > On Thu, Mar 22, 2018 at 7:07 AM, Sean Mcmillan NOAA Federal <sean.t.mcmillan@noaa.gov> wrote:
> >
> > > Sarah,
> > >
> > > Thank you. I will check back with you in 3 days for the privacy compliance documents.
> > >
> > > Sean T. McMillan (CISSP, C|EH, GIAC(GCIH))
> > > Information System Security Officer (ISSO)
> > > Office of Marine and Aviation Operations (OMAO)
> > > Marine and Aviation Cyber Center (MACC)
> > > Office: 863-500-3924
> > > sean.t.mcmillan@noaa.gov
> > >
> > > On Wed, Mar 21, 2018 at 5:37 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> > >
> > > > Here you go!!
> > > > Forwarded message
> > > > From: **Gioffre, Kathy (Federal)** <KGioffre@doc.gov>
> > > > Date: Wed, Mar 21, 2018 at 4:43 PM
> > > > Subject: NOAA2220 NOAA Ship Fleet Support System
> > > > To: "Brabson, Sarah (Federal)" <Sarah.Brabson@noaa.gov>, "Graff, Mark (Federal)" <Mark.Graff@noaa.gov>
> > > > Cc: CPO <CPO@doc.gov>, "Murphy, Tahira (Federal)" <TMurphy2@doc.gov>, "Ferguson, Dorrie (Federal)" <dFerguson@doc.gov>, "Martin, Lisa (Federal)" <LMartin1@doc.gov>

Good evening,

Attached is the SAOP approved PIA for NOAA2220 NOAA Ship Fleet Support System. The privacy compliance documents will be published on our website within three days.

Thanks,

Kathy

Kathleen (Kathy) Gioffre

Deputy Director and Chief Privacy Compliance Officer

U.S. Department of Commerce

Office of Privacy and Open Government

Room 52010

Office: (202) 482-9119

Email: kgioffre@doc.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: Ships Fleet Support System (SFSS) NOAA2220

FISMA Name/ID (if different): NOAA2220

Name of IT System/ Program Owner: CDR Ieshia k. Jones

Name of Information System Security Officer: Sean T. McMillan

Name of Authorizing Official(s): CDR Joseph Baczkowski

Date of Last PIA Compliance Review Board (CRB): 15 April 2017

(This date must be within three (3) years.)

Date of PIA Review: 24 January 2018

Name of Reviewer: Sean T. McMillan, ISSO

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: MCMILLAN.SEAN.T.1185814382 Digitally signed by MCMILLAN.SEAN.T.1185814382 Date: 2018.01.24 13:53:11 05'00'

Date of Privacy Act (PA) Review: 1/24/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 02 02 10 31 29 05'00'

Date of BCPO Review: 2/6/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark H. Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 02 06 17 01 38 05'00'

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Ships Fleet Support System (SFSS) NOAA2220

U.S. Department of Commerce Privacy Threshold Analysis

NOAA Ship Fleet Support System

Unique Project Identifier: 006-48-01-15-02-3601-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *NOAA2220 is an amalgamation of sixteen ships with similar general functions and operating characteristics, security needs, and operating environments. Common functions of all of the ship backbone subsystems are to provide network connectivity, domain authentication, internet connectivity and general business support services. While each ship has common (or class similar) configurations, mission requirements require each to have a unique configuration.*

The NOAA fleet of ships are managed, operated and maintained by NOAA's Office of Marine and Aviation Operations (OMAO), Marine operations centers (MOC), located in Norfolk, Virginia and Newport, Oregon. Additional ship specific support is provided through port office facilities in Woods Hole, Massachusetts; Charleston, South Carolina; Pascagoula, Mississippi; Davisville RI, and Ford Island, Hawaii. Ships are also maintained pier side in Newport, RI and Kodiak, Alaska.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__X_ This is an existing information system in which changes do not create new privacy risks. *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

- NOAA2220 ships have a Closed Circuit Television (CCTV) system that is used to record video throughout the ship for the purpose of safety. Ships personnel are notified by signs located throughout the ship that state that these premises are under video surveillance and cameras in use.
- NOAA2220 Aircraft record Crew Members and Scientific Partners names that participate in the flight and publish those names on the internet with the data for the flight in which they participated in.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X_ I certify the criteria implied by one or more of the questions above **apply** to the Ship Fleet Support System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

____ I certify the criteria implied by the questions above **do not apply** to the Ships Fleet Support System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Sean T. McMillan

Signature of ISSO or SO: MCMILLAN.SEAN.T.1185814382 Digitally signed by MCMILLAN.SEAN.T.1185814382 Date: 2018.01.31 12:52:47 05'00' Date: 24 Jan 2018

Name of Information Technology Security Officer (ITSO): James Jones IV, LCDR, USPHS

Signature of ITSO: JONES.JAMES.IV.1049453465 Digitally signed by JONES.JAMES.IV.1049453465 Date: 2018.01.29 12:16:39 -05'00' Date: _____

Name of Authorizing Official (AO): Joseph Baczkowski, CDR, USPHS

Signature of AO: BACZKOWSKI.JOSEPH.PADES.1167987300 Digitally signed by BACZKOWSKI.JOSEPH.PADES.1167987300 DN: c US, o U.S. Government, ou DoD, ou PKI, ou USPHS, cn BACZKOWSKI.JOSEPH.PADES.1167987300 Date: 2018.02.06 16:52:33 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.07 11:09:25 -05'00' Date: _____

Purvis, Catrina (Federal)

Subject:	CRB NOAA8884
Location:	Open Office 52017 (SMC) Md Conf Rm dial in information is (b)(6) [redacted]
Start:	Thursday, March 29, 2018 10:30 AM
End:	Thursday, March 29, 2018 11:00 AM
Recurrence:	(none)
Meeting Status:	Not yet responsed
Organizer:	Purvis, Catrina (Federal)
Attachments:	NOAA8884 PIA 011618 Final_SO ITSO Signature mhg.pdf; NOAA8884 PTA 01162018 Final_SO ITSO Signed mhg.pdf

Mark/Sarah,

Please ensure all PIAs/PTAs are submitted to OCIO to obtain system security concurrence. Ensure all required attendees are present at this telecom (dial in information (b)(6) [redacted] meeting, such as the ITSO, System Owner, etc., and other attendees who are able to respond to questions related to the systems identified above.

Also, if any of the systems are classified, please provide a hard copy of the SARs and POA&Ms for each system identified above to Catrina Purvis 2 days prior to the meeting date.

Warm Regards,

Dorrie Ferguson,
Management and Program Analyst
Office of Privacy & Open Government
Error! Hyperlink reference not valid.
Office: (202) 482-8157

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Southern Region General Support System (GSS) (NOAA8884)

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA / Southern Region General Support System (GSS) (NOAA8884)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. The GSS is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions and the scientific and technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

All administrative functions relating to people and PII are conducted on-line with these systems: MARS, CBS and NFC. The system does not keep any information local, since all information can be accessed via the on line databases.

Personally Identifiable Information (PII) maintained in the system is:

1. Located in a local database at the local Weather Forecast Office/River Forecast Center that maintains information on volunteers who provide weather reports to them.
2. Located in an encrypted Folder located on the Regional HQ NAS device, under the user of the Regional ISSO. This information is required for locally stationed contractors that require CAC authorization. This data is compiled by the Trusted Agent (TA) for submittal to the OSY for background checks and input to the TASS system.

No information is shared except with OSY, for the Trusted Agent information and in the case of security or privacy breach (see Section 6.1)

The statutory authorittycovering the collection of this data is 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce].

Authorities from DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

Authorities from DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

This is a moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
__ _ This is an existing information system with no new privacy risks.
__X__ This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	

b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X*
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

**NOAA8205 was incorporated into this collection.*

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: See authorities from DEPT-18 in the system description.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth	X	n. Financial Information	
c. Alias	X	i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): General description of volunteer's home location.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources				
Public Organizations	Private Sector		Commercial Data Brokers	
Third Party Website or Application				
Other (specify): Cooperative observers.				

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	X	Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	X
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	**X**	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): Information on weather volunteers.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

There are local databases at the local WFO/RFC that maintain information on volunteers who provide weather reports to them. The databases hold contact information on these volunteers, in order to contact them when needed and as a record of who provides the information.

All of this information is voluntary and the Co-Op Observer has the right to opt-out of the program at any time. This information is entered into a NOAA database called the Cooperative Station Service Accountability (CSSA), located and maintained by NWS Office of Climate Weather and Water Services (OCWWS).

A locally assigned NWS staff person is responsible for entry of this information into the CSSA database. A limited amount of this data is retained in the local office for quick access to contact the Co-Op in case of equipment outages.

This information is collected from members of the public.

The Regional ISSO has been assigned the Trusted Agent (TA) duties for multiple contractors. All badging paperwork and OSY Security/Investigative coversheets for the contractors are being saved to the ISSO's system. All transmission of PII data flows to other organizational entities (OSY) via secured Acellion SFTP server. All PII data residing on the NOAA8884 system is encrypted at rest with the use of McAfee Endpoint Security protection. This is an encrypted Directory only assessable from the user with CAC authentication.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X*		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach. For DOC bureaus, also for submission of CAC documents to OSY.

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	**X**
Contractors*	X		
Other (specify):			

*Contractors log in to review their information before the TA approves.

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and

	discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and privacy policy can be found at: http://www.nws.noaa.gov/om/coop/index.htm _____.	
X	Yes, notice is provided by other means.	Specify how: There are privacy act statements on the federal-wise forms used by the TA. Notice to volunteers is provided when information is collected,
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: All of this information is voluntary, as part of the cooperative agreement to work with the NWS on providing observations. The only means of providing the PII is by completing and signing the cooperative agreement form. Prospective contractors may decline, but their employment would be affected.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: The only use of the information is for contact purposes, which is given as part of the signed agreement. No other uses are suggested or specified. For the clearance, there is only one use for the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: The local manager visits each volunteer twice monthly to monitor equipment and answer questions. Updates can be made then, or emailed, as explained by the manager during orientation. Contractors can log into the TA system to review their information but cannot make changes.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation**: Any access to the local Database is logged and saved.** **AD maintains logging of all access to file system**
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A):_____**4/19/2017**_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. **MODERATE**
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access to the system maintaining the PII is controlled by access via Active Directory and the use of CAC (PIV) cards. Only employees with authority to maintain this database are allowed access to the information.

Trusted Agent data is located in an encrypted Folder located on the Regional HQ NAS device, under the user of the Regional ISSO. Can only be decrypted by use of CAC card using McAfee Files and Folders encryption for the ISO only.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN).

	COMMERCE/NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission; COMMERCE/DEPT-13, Investigative and Security Records. COMMERCE/DEPT-25, Access Control and Identity Management
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1300- Weather, 1307-05
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	**X**	Overwriting	
Degaussing	**X**	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	**Individual's PII are in the system.**

X	Quantity of PII	Provide explanation: Only name and contact information for volunteers, and names of employees, are in the system.
X	Data Field Sensitivity	**Application data has many sensitive fields filled out.**
X	Context of Use	**Voluntary submission of PII for internal use only**
	Obligation to Protect Confidentiality	
X	Access to and Location of PII	**Secured local database managed by limited Federal employees**
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

System Owner or Information System Security Officer

Name: John Duxbury
Office: NWS/SR
Phone: 682-703-3703
Email: john.duxbury@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature:

DUXBURY.JOHN.C.1365877730
2018.01.17 11:58:34 -06'00'

Information Technology Security Officer

Name: Andrew Browne
Office: NOAA NWS Office of the CIO
Phone: 301-427-9033
Email: beckie.koonge@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature:

BROWNE.ANDREW.PATRICK.1472149349
Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.01.22 15:39:20 -05'00'

Authorizing Official

Name: Steven Cooper
Office: NWS/SR
Phone: 682-703-3700
Email: steven.cooper@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature:

COOPER.STEVEN.G.1365850930
Digitally signed by COOPER.STEVEN.G.1365850930
Date: 2018.01.22 14:11:48 -06'00'

Bureau Chief Privacy Officer

Name: Mark Graff
Office: NOAA Privacy Office
Phone: 301-628-5658
Email: mark.graff@noaa.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: GRAFF.MARK.HYRUM.1514447892
Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.01.24 10:56:25 -05'00'

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2018

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Southern Region GSS (NOAA8884)

U.S. Department of Commerce Privacy Threshold Analysis

Southern Region GSS (NOAA8884)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. This system is designed and used to support the collection, processing, and dissemination of data that supports the mission of the origination. It also supports the administrative functions and the scientific & technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web-based server systems. The system supports a variety of users, functions, and applications; including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development and collaboration.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): *NOAA8205 was incorporated into this collection.					

____ This is an existing information system in which changes do not create new privacy risks. *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

__X__ Yes. *Please describe the activities which may raise privacy concerns.*

The Regional ISSO has been assigned the Trusted Agent (TA) duties for multiple contractors. All badging paperwork and OSY Security/Investigative coversheets for the contractors are being saved to the ISSO's system.
All transmission of PII data flows to other organizational entities (OSY) via secured Acellion SFTP server.
All PII data residing on the NOAA8884 system is encrypted at rest with the use of McAfee Endpoint Security protection. This is an encrypted Directory only assessable from the user with CAC authentication.

____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
_X___ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__**X**__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ ☐ I certify the criteria implied by one or more of the questions above **apply** to the Southern Region GSS (NOAA8884) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

____ ☐ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

John Duxbury (SO)

Signature of ISSO or SO: DUXBURY.JOHN.C.1365877730 2018.01.18 07:50:53 06'00' Date: _____

Name of Information Technology Security Officer (ITSO):

_Andrew Browne (ITSO)

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.01.22 15:38:35 -05'00' Date: _____

Name of Authorizing Official (AO):

__Steven Cooper

Signature of AO: COOPER.STEVEN.G.1365850930 Digitally signed by COOPER.STEVEN.G.1365850930 Date: 2018.01.22 14:10:31 06'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): ____Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.01.24 10:52:07 05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 22, 2018 1:48 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA 3 SORN updated and in new template
Attachments:	NOAA 3 SORN in new template_032118.docx

Mark, (b)(5) [redacted]

[redacted].

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6) [redacted]

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 22, 2018 1:50 PM
To:	Toland, Michael; Gitelman, Steve (Contractor); PrivacyAct
Cc:	Mark Graff NOAA Federal
Subject:	NOAA 3 SORN updated and in new template
Attachments:	NOAA 3 SORN in new template_032118.docx

I had just completed this, and I noticed there's a SORN agenda item on the call scheduled for Tuesday, so wanted to make sure my percentage of completeness increased accordingly :)

I have two more to go NOAA 1, about which I need to ping the NOAACorps director again, and NOAA 13.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, March 26, 2018 10:20 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA5032 Privacy Impact Assessment for BCPO Signature
Attachments:	NOAA5032 PTA_01 2017_for MHG signature mhg.pdf; NOAA5032_PIA_Annual_Review_Certification_Form_with_PA_Officer__20180301_signed_PA officer mhg.pdf; NOAA5032 2017 PIA revised 20180306 For NOAA BCPO Signature mhg.pdf

Here are all three together. I think I already sent you the PIA, but I don't think I'd sent you the Re Cert. Here it is with the PIA and PTA.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Thu, Mar 8, 2018 at 10:34 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

> Got it looks good. Here you go signed.
>
> Mark H. Graff
> FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> National Oceanic and Atmospheric Administration
> (301) 628 5658 (O)
> (b)(6) (C)
>
>
>
> On Thu, Mar 8, 2018 at 10:24 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > NOAA5032 PIA for certification, for your sig.
> >
> > Also, Nancy is wanting the NOAA5010 PTA soonest. Yes, it just expired, but I was the one that had to tell Juanita several weeks ago that it was going to . .
> >
> > thx
> >
> > Forwarded message

From: **Jeffrey VanDam - NOAA Affiliate** <jeffrey.vandam@noaa.gov>
Date: Thu, Mar 8, 2018 at 10:20 AM
Subject: Fwd: NOAA5032 Privacy Impact Assessment for BCPO Signature
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>

Hi Sarah, here is the email I sent to Mark Graff. Sorry I think you were supposed to send it.

Thank you,
Jeff Van Dam
ISSO Support
NSOF 1450
301 817 3915

Forwarded message
From: **Jeffrey VanDam - NOAA Affiliate** <jeffrey.vandam@noaa.gov>
Date: Thu, Mar 8, 2018 at 10:13 AM
Subject: NOAA5032 Privacy Impact Assessment for BCPO Signature
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>
Cc: Nancy DeFrancesco <nancy.defrancesco@noaa.gov>, Eric Most NOAA Federal <eric.most@noaa.gov>, James Schreiber NOAA Federal <james.schreiber@noaa.gov>, Mark Hall NOAA Federal <mark.o.hall@noaa.gov>, Bob Clark NOAA Federal <bob.clark@noaa.gov>, _NESDIS OSPO IT Security <ospo.itsecurity@noaa.gov>, Isaac Sanvee NOAA Affiliate <isaac.sanvee@noaa.gov>

Hi Mark,

Will you please sign and return the attached PIA for NOAA5032. Thank you.

Thank you,
Jeff Van Dam
ISSO Support
NSOF 1450
301 817 3915

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA5032
Wallops Command and Data Acquisition Station (WCDAS)
Administrative Local Area Network (LAN)

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA WCDAS Administrative LAN

Unique Project Identifier: NOAA5032 (not affiliated with an Exhibit 300).

Introduction: System Description

The WCDAS (Wallops Command and Data Acquisition Station) Administrative LAN (NOAA5032) is located within the WCDAS computer facility in Wallops Island, VA. The WCDAS Administrative LAN supports the NESDIS mission by providing IT resources to WCDAS personnel. Although the system does not collect or store PII (other than employee contact information) or BII, the system does support office functions that distribute PII and BII such as electronic mail, purchasing, logistics, facility management, inventory, human resource, and contract administration. *These functions use paper files as the source of the PII and BII distributed; for purchasing and human resources functions, information from paper files is typed into portals or emails (HR information by email is covered by the NOAA1200 PIA approved by DOC on March 24, 2017). No sensitive PII from HR functions is stored within the accreditation boundaries.*

WCDAS Administrative Local Area Network (LAN) is a standard office automation environment that relies on the NOAA NOC (NOAA 0200) for VPN access to the NSOF Administrative LAN (NOAA5044), and Internet connectivity.

Employee PII is collected for Emergency Contact information.

The WCDAS Administrative LAN does not share this information with any agency. Information is shared within the bureau on a case by case basis.

Authorities: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks.
__X__ This is an existing information system with no changes that create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth*		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name*	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice		f. Vascular Scan		i. Dental Profile	

Recording/Signatures					
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The Business Continuity Plan (BCP) is used for emergency contact of WCDAS employees. This information is collected from Federal Employees only.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors			
Other (specify): Limited Administrative personnel			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found on the	
X	Yes, notice is provided by other means.	Specify how: Notification is provided in writing by the employee's supervisor or by the administrative staff. Verbal notices is provided to employees when requesting information for COOP activities.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Federal employees have an opportunity to decline to provide PII to their supervisors, in writing, but they would not be contacted during an emergency.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Individuals may choose not to be contacted during an emergency, by declining in writing to their supervisors. This is the only use of the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals may consult administrative personnel who have access to their PII and provide updates to them. This information is conveyed in writing as part of the employee orientation.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

PII/BII on this IT system is protected through the use of hardware and software firewalls, Cisco ASA Firewalls, Cisco IPS; Windows software firewalls; Tripwire Enterprise; Tripwire Log Center; ArcSight deployed and reporting back to NOAA Enterprise Security Services; HSPD-12 compliant with two factor authentication; McAfee Data Loss Prevention enabled, blocking all unauthorized USB drives and external hard drives.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: DEPT-18, Employees Personnel Files not Covered by Notices of Other Agencies.
	Yes, a SORN has been submitted to the Department
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Chapter 200-01
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.

	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: Contact information only is maintained for a BCP.
X	Data Field Sensitivity	Provide explanation: There is no sensitive PII.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:

X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Johnny R. Clark Office: NESDIS/OSPO/WCDAS Phone: 757-824-7328 Email: bob.clark@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK.JOHNNY.R.1365842791 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn CLARK.JOHNNY.R.1365842791 Date: 2018.03.06 15:06:38 05'00' Date signed: 3/6/2018	**Information Technology Security Officer** Name: Nancy DeFrancesco Office: NESDIS ACIO-S Phone: 301-713-1312 Email: nancy.defrancesco@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.07 14:57:35 -05'00' Date signed: 03/07/2018
Authorizing Official Name: Vanessa Griffin Office: NESDIS/OSPO Phone: 301-713-7311 Email: vanessa.griffin@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.08 08:47:48 -05'00' Signature: Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.08 10:32:08 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA5032 (WCDAS Administrative LAN)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA5032 WCDAS Administrative LAN

Unique Project Identifier: NOAA5032

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
The WCDAS Administrative LAN (NOAA5032) is located within the WCDAS computer facility in Wallops Island, VA. The WCDAS Administrative LAN supports the NESDIS mission by providing IT resources to WCDAS personnel. Specifically the WCDAS Admin LAN is used to support electronic mail, purchasing, logistics, facility management, inventory, human resource, contract administration, general management functions and office automation functions. Wallops Command and Data Acquisition Station (WCDAS) Administrative Local Area Network (LAN) is a standard office automation environment that relies on the NOAA NOC (NOAA 0200) for e-mail, VPN access to NSOF (NOAA5044), and Internet connectivity.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X__ This is an existing information system in which changes do not create new privacy risks. *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

NOAA5032/WCDAS LAN

____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Charles S. Bryant

Signature of ISSO or SO: Bryant, Charles S. (GSFC-416.0)[NOAA] Digitally signed by Bryant, Charles S (GSFC 416 0) [NOAA] DN cn Bryant, Charles S (GSFC 416 0)[NOAA], o USDOC/NOAA/NESDIS, ou GOES R Ground Segment, email charles s bryant@noaa gov, c US Date 2017 01 13 18 25 08 05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Nancy A. DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn DEFRANCESCO.NANCY.A.1377370917 Date: 2017.01.30 08:08:16 05'00' Date: 01/30/2017

Name of Authorizing Official (AO):

Vanessa L. Griffin

Signature of AO: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRIFFIN.VANESSA.L.1204308663 Date: 2017.02.14 10:17:37 05'00' Date: 02/14/2017

Name of Bureau Chief Privacy Officer (BCPO):

Mark H. Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2017.02.15 10:55:45 05'00' Date: _____

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA5032 PIA

FISMA Name/ID (if different): NOAA5032 (WCDAS ADMIN LAN)

Name of IT System/ Program Owner: Johnny R. Clark

Name of Information System Security Officer: Mark O. Hall

Name of Authorizing Official(s): Vanessa Griffin

Date of Last PIA Compliance Review Board (CRB): 08/16/2016

(This date must be within three (3) years.)

Date of PIA Review: 3/6/2018

Name of Reviewer: Johnny R. Clark

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK JOHNNY R 1365842791
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn CLARK JOHNNY R 1365842791
Date 2018 03 06 13 58 59 05'00'

Date of Privacy Act (PA) Review: 3/8/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488
Date 2018 03 08 12 52 51 05'00'

Date of BCPO Review: 3/26/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892
Date: 2018.03.26 10:17:03 -04'00'

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, March 29, 2018 2:33 PM
To:	Chi Kang NOAA Federal
Subject:	Possible Solution Eagle Horizon Inject
Attachments:	OS 64 OITS GSS PIA SAOP Approved.pdf

Hey Chi,

(b)(5) [redacted]

[redacted]

Thoughts (b)(5) [redacted].

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) [redacted] (C)

U.S. Department of Commerce
Office of the Chief Information Officer
Office of the Secretary

Privacy Impact Assessment
Office of Information Technology Services General Support System (OS064)

Reviewed by: Kathy Gioffre

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS
DN: c US, o U.S. Government, ou Department of Commerce, ou Office of the Secretary, cn CATRINA PURVIS, 0.9.2342.19200300.100.1.1 13001002875743
Date: 2018.03.06 12:56:04 05'00' August 16, 2017

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

Office of Information Technology Services-General Support System (OS064)

Introduction: System Description

Web Application Services: The Department of Commerce Office of Information Technology Services General Support System (OITS-GSS) security impact category is moderate. Web Applications is a component of the OITS-GSS.

The Department of Commerce (DOC) and its operating units use various websites and applications, such as commerce.gov, open.commerce.gov and ESA.gov, to engage in dialogue, share information, and collaborate with the public. These sites contain official information from the DOC; they are the authoritative source of official Department information. The DOC owns these websites and applications. These websites and applications continue to grow in size and diversity.

These websites and applications are used to collaborate and share information online by facilitating public dialogue, providing information about or from the DOC, make information and services more widely available, and to improve customer service. Our use of these websites and applications offer important opportunities for promoting the goals of transparency, public participation, and collaboration. Through these services, individuals or groups can create, organize, edit, comment on, combine, and share content of mutual interest.

The Department and its operating units use internal websites and applications to interact with one another, share information, and collaborate. The internal websites are only accessible to Department personnel. Department personnel information, business information and documentation is shared on these internal websites.

The system collects name, day and month of birth, education, general work related data, and photographs of Department personnel, as well as standard system administration/logging data. This information will be stored on the OITS-GSS. Department personnel biographies will be shared with the public and Department personnel. The PII collected by this system will not be monitored or destroyed until the system is decommissioned. Records will be retained and disposed of in accordance with applicable records schedules.

Typical transactions

a) Media where official DOC users may have an account to use applications tailored to the specific website.

b) Video and image websites where official DOC users may have an account to post videos and images. Public users do not need an account to submit comments.

c) Blogs and similar websites where official DOC users may have an account to post.

d) On internal websites, biographical pages about Department personnel are updated to

share information with other personnel. On external websites, biographical pages about Department personnel are updated to share information with the public.

e) Work related information and documentation are posted on internal websites to be accessed by Department personnel.

Authorities supporting the DOC's use of websites and applications:

a) 5 U.S.C. § 301, The Federal Records Act

b) The President's Memorandum on Transparency and Open Government, January 21, 2009

c) The OMB Director's Open Government Directive Memorandum, December 8, 2009

d) OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010

File and Printer Services: The Department of Commerce (DOC) Office of Information Technology Services General Support System (OITS-GSS) provides enterprise applications, local area network (LAN) services, network management and office automation services. The OITS-GSS is located at the Herbert Clark Hoover Building (HCHB) located at 1401 Constitution Avenue, Northwest, Washington, DC.

Programs, Typical Transactions, Information Sharing and Legal Authorities

Twenty-three (23) Business Operating Units (BOU) within DOC use OITS-GSS services for data storage and retrieval of program information supporting official daily responsibilities and the organization's mission. Information use is limited to: developing policies, managing programs and providing oversight for collaborative efforts with business customers. The official needs of the BOU determine the extent of the information sharing with other organizations. The organization restricts and controls the use of all personally identifiable information (PII) and business identifiable information (BII); an individual's job roles and responsibilities determine accessibility within each respective program office. The following BOUs are users of these services:

Office of the Secretary:

1) **Office of Business Liaison (OBL)**

Typical transaction

As part of the OBL's responsibilities, the names and contact information for key individuals from the private sector and relevant industry associations are collected, stored in excel files on internal shared drives and, as appropriate, shared internally with other officially relevant DOC bureaus. The business processes also include compiling the data on spreadsheets and using the information to extend invitations to relevant events hosted by the DOC and/or to arrange one-on-

one meetings with members of the team. Collection and use of this data are critical to the OBL's official mission of representing private sector interests through strategic engagement.

Information sharing

Information is shared within OBL internally and with other officially relevant DOC bureaus.

Legal authority to collect

The authority for maintenance of the systems includes the following sources with revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107; E.O. 131614; 41 U.S.C. 433(d); Executive Order (E.O) 11625; DOO 25-4A and 15 U.S.C. § 1512.

2) Center for Faith Based and Neighborhood Partnerships (CFBNP)

Typical transaction

The collection of PII is for submission for meetings and events on behalf of Commerce employees. CFBNP collects Web Automatic Verification of Enrollment System security information for meetings at the White House conducted with external stakeholders and/or Commerce staff.

Information sharing

The CFBNP shares information with the White House Liaison Office and essential White House staff members to obtain entry clearance for authorization to attend meetings on the White House premises.

Legal authority to collect

The authority for maintenance of the systems includes the following sources with revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107; E.O. 13164; 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; Department Administrative Order 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

3) Office of Acquisition Management (OAM)

Typical transaction

A typical transaction involving BII is one in which Civil Applicant System (CAS) receives proposals in response to published solicitations. Depending required method to receive these documents (e.g., postal mail, electronic or hand-delivery, some BII may be received through the CAS. If the information is received by CAS, OAM prints and maintains copies in the contract

file; the electronic files received in the CAS are archived in an e-mail folder maintained by the contracting officer/specialist.

Information sharing

As necessary, information is shared between the Office of Inspector General, the Legal Office, Policy Office and the Office of Small and Disadvantaged Business Utilization when solicitation protests require legal review and potential action.

Legal authority to collect

The legal authorities to collect BII include: DOO 20-26 and the Federal Acquisition Regulation (FAR) 9.104-1. According to FAR 9.104-1, there are a number of actions the contractor/vendor must prove to the government in order to be considered as a prospective contractor.

4) Office of Facilities and Environmental Quality (OFEQ)

Typical transaction

A typical transaction involving non-sensitive PII is one in which a user account is created with a user name and an e-mail. The email is used by the system to send automated email notifications of pending required corrective actions that are based upon a previously conducted environmental assessment. The user name is used to create logon ability to the system's environmental databases; these databases consist of two types: 1) existing federal and state environmental regulations and 2) the individual facility assessment results.

Information sharing

OFEQ does not disseminate PII/BII information on the OITS-GSS.

Legal authority to collect

Compliance with all environmental laws and regulations is required by Executive Order 12088.

5) Office of Budget (OB)

Typical transaction

The OB does not have a routine requirement to collect PII. However, OB occasionally collects PII from DOC personnel attending OB meetings at the New Executive Office Building. This pre-clearance information is required by the Office of Management and Budget (OMB) for building access.

Information sharing

The PII collected for the includes: name, city/ state of residence, date of birth, social security number and country of birth. This information is transmitted to OMB using the DOC/OCIO Accellion Secure File Sharing service.

Legal authority to collect

The authority for OB is derived from 15 USC §1501. Establishment of Department; Secretary; seal There shall be at the seat of government an executive department to be known as the Department of Commerce, and a Secretary of Commerce, who shall be the head thereof, who shall be appointed by the President, by and with the advice and consent of the Senate, and whose term and tenure of office shall be like that of the heads of the other executive departments; and the provisions of title 4 of the Revised Statutes, including all amendments thereto, shall be applicable to said department. The said Secretary shall cause a seal of office to be made for the said department of such device as the President shall approve, and judicial notice shall be taken of the said seal.

6) Office of Civil Rights (OCR)

Typical transaction

Typical transactions would include events as a part of formal complaints describing actions and the dates of these actions. Transactions of this information would include: assignment of an investigator, hearing requested by complainant and agency's decision issuance.

Information sharing

Information is shared between Office of Civil Rights (OCR) and the Equal Employment Opportunity (EEO) Offices at the National Institute of Standards and Technology (NIST), National Oceanic and Atmospheric Administration (NOAA) and the U.S. Census Bureau (Census) based on customized, role-based levels of bureau and user access. For example, OCR users can access data entered by Census EEO staff and some OCR users can edit that data for official business. Census EEO staff can access data entered by OCR, but access is limited to Census cases and OCR entries are read-only for Census staff.

Legal authority to collect

The authority for processing discrimination complaints within the DOC has been delegated to the OCR Director IAW DOO 20-10, Office of Civil Rights. The DOC's internal discrimination complaint program is described by DAO 215-9.

The authority for the Department's EEO complaint processing program is contained in the regulations of the Equal Employment Opportunity Commission (EEOC) at 29 CFR § 1614 and policy guidance provided by EEOC Management Directive 110. Related laws and regulations governing DOC's authority to process complaints of discrimination include: 42 U.S.C. 2000e-16; 29 U.S.C. 633a; 29 U.S.C. 791 and 794a; 29 U.S.C. 206(d); E.O. 10577; 3 CFR 218 (1954-1958 Comp.); E.O. 11222, 3 CFR 306 (1964-1965 Comp.); E.O. 11478, 3 CFR 133 (1969 Comp.); E.O. 12106, 44 FR 1053 (1978) and Reorganization Plan No. 1 of 1978, 43 FR 19807 (1978).

7) Office of Financial Management (OFM)

Four distinct OFM programs use OITS-GSS services for data storage and retrieval of program information to support official daily responsibilities: Passport/Visa Access Database, Travel Card Program, Sunflower Personal Property Management System and OFM Data Analytics.

Example 1:
Typical transaction

Passport/Visa Access Database is used to track and maintain official and diplomatic passports and visas for various bureau Federal employees, their spouses, and dependents traveling with a Department of Commerce (DOC) employee. This database is an internal system accessed only by the Travel Management Staff. The passports, visas, and applications are tracked to and from various embassies and the Department of State. A typical transaction would be to enter the employee's information into the database and extract various reports. Traveler Information includes: full names, email address, Bureau, Department, title, relationship to DOC traveler, name(s) of spouse and/or dependents traveling with DOC employee, Dates (separation, departure, reviewed, granted, issuance, expiration, employee notification, Hold information, cancelation instructions and return address. Visa Application Information includes: Passport number, Embassy name (location and dates - returned, approved, sent to Embassy), application status, picked up (date and by whom), Visa/Passport holder notification date.

Information sharing

The information in the database is not shared only Travel Management Staff have access to the database.

Legal authorities to collect

Budget and Accounting Act of 1921, Accounting and Auditing Act of 1950, and Federal Claim Collection Act of 1966.

Example 2:
Typical transaction

JP Morgan Chase System is used to manage the Travel Card Program. A typical transaction conducted in the system is to check for delinquent accounts and extract various reports.

Information sharing

The information is shared - Department Level 1 Agency/Organization Program Coordinator (A/OPC) has access to the entire system, Bureau Levels 2 & 3 A/OPCs have access to only their

travelers' information, and Travel Card holders have access to their account information only. Information is transmitted through an encrypted application process.

Legal authority to collect

Budget and Accounting Act of 1921, Accounting and Auditing Act of 1950, and Federal Claim Collection Act of 1966.

Example 3:
Typical transaction

Sunflower Personal Property Management System is used to maintain accountability of all personal property assets and fleet of vehicles across the Department. A typical transaction conducted in the system is to enter traveler information, visa information, and extract reports.

Information sharing

The information is shared within DOC with all Bureau Property Officials including those in the field offices and the Sunflower Contractor.

Legal authorities to collect

5 U.S.C. 301, 44 U.S.C. 3101, 40 U.S.C. 481-92, and 15 U.S.C. 1518.

Example 4:
Typical transaction

OFM Data Analytics The OFM is currently implementing a data analytics program with the objective of developing the capability to identify trends, anomalies and other meaningful patterns in financial programs. This program will analyze data from three DOC programs: purchase card transactions, travel card transactions and payroll (mainly time and attendance). The system will use data from the system of records for the time and attendance record keeping (WebTA), payroll management (NFC), purchase and travel card transactions system (PaymentNet).

OFM data analytics program will involve the development of continuous monitoring processes for sensitive programs. The monitoring process will include several steps to request, transform and load data into existing databases where analytical tests will be applied to assist in identifying trends, anomalies and other meaningful pattern in the data.

Data processing for the program includes data calls to the WebTA database administrator, who

will use scripts that have been provided by the program developers to extract the requested data; a request for data will also be sent to the NFC database administrator and the administrator for the PaymentNet database. Once the extracts are received, tests are performed to verify the completeness of each data set. Integrity tests include comparing employee headcount between the two systems.

Tests run against the data include stratifications for payroll day types such as; regular and premium pay types sorted by; bureau, pay time, employee and date. Additionally tests are performed to look for and identify instances where controls have been compromised and/or circumvented, examples for payroll include, unapproved leave and/or premium pay, self-certification of timesheets, inappropriate use of federal holidays, night and Sunday differential. Compromised purchase and travel card controls are identified using a risk-ranking process to review each transaction and cardholder. Risk rankings include but are not limited to: adult entertainment, duplicative payment-same vendor, non-zero sales tax, split payment-same employee, transaction over purchase limit, potential conflict of interest, and potentially personal transaction.

Information sources

The source for each data element comes from OS and other DOC bureaus.

a) PaymentNet purchase and travel card transactions for DOC employees.

b) WebTA time and attendance activity for DOC employees.

c) NFC payroll information for DOC employees.

Information sharing

OFM staff and OFM contractors will have access to the data. OFM contractors will run the initial tests, as identified in the statement of work for the applicable contract. OFM staff will review for instances where controls have been compromised and/or circumvented. The testing results are compiled and presented to DOC and Bureau management on a case-by-case basis. The purpose of presenting these results is to determine the areas that require additional review and follow-up. If needed, Departmental and Bureau management will prepare and maintain corrective action plans designed to prevent future breakdowns in controls.

Legal authorities to collect

Title 5 U.S.C.; Title 31 U.S.C. 66a, 492; Title 44 U.S.C. 3101, 3309; Title 5 U.S.C.; Title 31 U.S.C. 66a, 492; Title 44 U.S.C. 3101, 3309; Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; Federal Claim Collection Act of 1966; 31 U.S.C. 3321 and 40 U.S.C. 486(c).

8) Office of Human Resource Management (OHRM)

Typical transaction

The OHRM uses a wide variety of the Department's Human Resources Information Technology (HRIT) systems to provide Department-wide human resources services. The typical transactions are loaded into HRIT systems via online entry into web-based forms by Human Resource (HR) personnel. Bulk transfers of information occur from DOC to Office of Personnel Management (OPM) and U.S. Department of Agriculture (USDA) National Finance Center (NFC) via approved and tested electronic interfaces. These interfaces have approved information interconnection agreements. The OHRM has full responsibility for the design and development of the following IT systems to support HR programs:

a) Automated Classification System (ACS) ACS contains key position data that supervisors use to create and simultaneously classify Demonstration Project position descriptions. In addition to creating new position descriptions, the ACS stores descriptions in a local user database and allows the user to create a new description based on one in the database; to revise, review, print, or delete position descriptions; or to review and report on the position descriptions in the database.

b) Performance Payout System (PPS) PPS provides the functionality to record, document and report the annual employee performance rating, performance increase, and bonus payout, calculate the annual comparability increase (ACI) for the employees who are under the Commerce Alternative Personnel System (CAPS) pay plans and transmit updated data to the U.S. Department of Agriculture's National Finance Center (NFC), the Department's Payroll System of Record.

c) Executive Resources Information System (ERIS) End of Year - Senior Executive Service (SES) Bonus Pool (BP) SES BP provides the functionality to record and report the annual performance ratings, performance increases, and bonus recommendations, calculate ACIs for the SES employees, and transmit the updated data to NFC.

d) DOC-Hiring Management System (DOC-HMS) HMS tracks and reports on the timeliness of the 80 day hiring process, and hiring actions initiated by the DOC's Human Resources Operations Center (DOCHROC), as part of the overall human resources management measurement project. This system tracks all the hiring steps from the job announcement to the day a new employee reports for duty. It tracks each step of the process and produces the necessary reports to measure the process effectiveness and efficiency.

e) Honor Awards Nominee System (HANS) HANS is an automated Gold and Silver Honor Awards Program nomination and reporting system. This system provides users access to nominate employees and vote on nominations, and produce reports including certificate citations, program booklets, and seating charts.

f) WebTA WebTA is Kronos Proprietary software. It is used to record DOC employees' time and attendance data. The employees enter their own time and attendance data. The data is transmitted bi-weekly to NFC for employees pay processing.

g) Executive Resources Information System-Top Level (ERIS-TL) ERIS-TL provides information regarding the incumbency status of all key positions to a limited cadre of the most senior Department of Commerce (DOC) executives to aid in Executive Level (SES) Staffing decisions.

Information sharing

Information is shared within Commerce Bureau/Operating Units (BOU) on a case by case basis. Information is shared with OPM and NFC via bulk transfer.

Legal authority to collect

The authority to deliver, maintain and approve Department-wide and approve bureau-specific automated human resources systems and serve as the focal point for collection and reporting of human resources information within the Department of Commerce is delegated to the Office of Human Resources Management in DOO 20-8 - SECTION 4, the Office of Human Resources Management.

The authority for maintenance of the systems includes the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107; E.O. 131614; 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; E.O. 12554, P.L. 100-71, dated July 11, 1987, and Office of Financial Management (OFM) Page 62.

9) Office of Privacy and Open Government (OPOG)

OPOG collects PII as part of the normal duties. The information may contain a variety of sensitive and non-sensitive. The amount of and type would be based on the type of program transaction and submission manner. The information is collected from federal employees, contractors, non-government personnel, and foreign nationals.

Example 1:
Typical transaction

The typical OPOG transaction would be the following: Freedom of Information Act (FOIA)/Privacy Act (PA) transactions include the requester's name, home or business address, personal or business email address, home or business telephone number, and a description of the requested records. FOIA requests are logged into a FOIA tracking system, FOIAonline; see separate DOC FOIAonline Privacy Impact Assessment for more details.

PA transactions include the requester's name, home or business address, personal or business email address, home or business telephone number, and a description of the requested records. Privacy Act transactions include:

a) FOI/Privacy Act Officer receives request
b) FOI/Privacy Act Officer or designee logs in request in to appropriate system
c) FOI/Privacy Act Officer assigns request
d) FOIA Specialist or assigned office conducts search for responsive records
e) FOIA Specialist or assigned office reviews records and redacts, as needed
f) Response and responsive records are released to requester
g) FOIA Specialist closes out request

Example 2:
Typical transaction

Privacy incident transactions can include any type of sensitive or non-sensitive personally identifiable information (PII). PII incidents are reported and tracked in accordance with Commerce policy following the published guidance. Information sharing conducted on case by case with a need to know basis within the agency and with other federal agencies as required by law, regulations and guidance. PII incident transactions include:

1. Employee, Contractor, etc. reports PII incident to bureau/operating unit (BOU) Computer Incident Response Team (CIRT).
2. BOU CIRT reports PII incident to DOC-CIRT.
3. For cyber related incidents DOC-CIRT notifies the Chief Privacy Officer (CPO), US Computer Emergency Readiness Team (US CERT), and notifies the BCPO within one (1) hour. For non-cyber related incidents, DOC-CIRT notifies the CPO and BCPO within one (1) hour.
4. Bureau Chief Privacy Officer (BCPO) evaluates incident and rates risk level.
5. BCPO closes low risk incidents and recommends closure to CPO for moderate and high incidents
6. BCPO notifies DOC-CIRT of updates and closure of the incident.
7. DOC-CIRT closes the PII incident with notification to US CERT, if applicable.

Information sharing

Information sharing is performed on a case by case basis with Commerce BOUs and other federal agencies.

Legal authority to collect

The authority to deliver, maintain and approve Department-wide programs for FOIA, Privacy, Open Government, FACA and Directives Management and serve as the focal point for collection and reporting of OPOG program's within the Department of Commerce is delegated to the

Office of Privacy and Open Government in DOO 20-31 - SECTION 3, the Office of Privacy and Open Government.

Authority for maintenance of systems

The authority for OPOG programs include the following, with all revisions and amendments: 5 U.S.C. 552; E.O. 12024; E.O 12838; OMB Circular No. A-135; Section 204 of P.L.104-4; P.L. 92-463; 5 U.S.C. App; 5 U.S.C. § 552; Title 15 CFR, Part 4; E.O. 13392; 5 U.S.C. 552a; FISMA of 2002, 44 U.S.C. § 3541; OMB M-03-22; M-06-15; M-06-16; M-06-19; M-07-16; M-11-02, and M-15-01.

10) Office of Performance, Evaluation, and Risk Management (OPERM)

Typical transaction

Typical transactions that involve non-sensitive PII are ones in which:

a) U.S. Government Accountability Office (GAO) or DOC Office of Inspector General (OIG) contacts the Department to provide notification that an audit is being conducted which includes names and contact information for the audit team. OPERM stores this information in the system and responds to the GAO or OIG with the names of audit liaisons and Department staff who will work with the auditors.

b) Department or bureau staff contacts OPERM to request accounts in the Audit Management System (AMS). OPERM will send this information to the system administrator (a contractor) and request that accounts are set up, using a user name and email. The email may be used by the AMS to send automated email notifications. The user name is used to create a log-on ability.

c) Names and contact information for bureau and Department staff working with the Enterprise Risk Management and Performance programs are stored in the system and used to contact the individuals regarding program activities. Contact lists may be shared with other bureau and Department staff. For example, a NOAA employee may request the name(s) and contact information of NOAA staff with risk management or performance responsibilities.

Information sharing

OPERM staff may manually refer to records in the system for names and contact information stored in them and forward the information as needed within the course of performing our office missions. However, there is no automated sharing of OPERM information within the OITS-GSS.

Legal authority to collect

a) Enterprise Risk Management - The Federal Managers' Financial Integrity Act of 1982 (FMFIA); the Office of Management and Budget (OMB) Circulars A-123 and A-11, and other authorities cited in DAO 216-20, Enterprise Risk Management.

b) Performance Excellence Program and Performance Evaluation - Government Performance and Results Act (GPRA) Modernization Act of 2010, and OMB Circular A-11.

c) Office of Inspector General (OIG) / Government Accountability Office (GAO) Audit Liaison and Follow-up the GAO Act of 1980, the Legislative Reorganization Act of 1970, OMB Circular A-50, and other authorities cited in DAO 213-1 GAO Liaison and Audit Follow-up.

d) Non-financial internal control implementation and management - Federal Managers' Financial Integrity Act of 1982 (FMFIA) and OMB Circular A-123.

11) Office of Security (OSY)

Typical transaction

The information is collected from federal employees, contractors, Departmental non-government personnel, and foreign nationals. The data is maintained in the system as a system of record and to verify existing data. The data is then used to determine if employment with the Department is viable. The information is maintained as historical information.

Information sharing

The data is disseminated to the Department of Justice (DOJ) and Office of Personnel Management (OPM) for the individual background checks.

Legal authority to collect PII and/or BII

DOO 20-6, 5 CFR 731, 5 CFR 732, Executive Orders (EO) 10450, 12968, 13488, 13467.

12) Office of Small and Disadvantaged Business Utilization (OSBDU)

OSBDU is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

13) Office of the CIO, Office of Cyber Security (OCS)

OCS is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

14) Office of the CIO, Office of the Chief Technology Officer & Deputy Chief Information Officer, Office of Policy and Strategic Planning (OPSP)

OPSP is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

15) Office of the CIO, Office of the Chief Technology Officer & Deputy Chief Information Officer, Office of IT Services (OITS)

Typical transaction

OITS obtains a user name which will be used to create a system account which includes the general support system and secure file transfer.

Information sharing

No information sharing is conducted by the system.

Legal authority to collect PII and/or BII

5 U.S.C. § 301, The Federal Records Act; The President's Memorandum on Transparency and Open Government, January 21, 2009; The OMB Director's Open Government Directive Memorandum, December 8, 2009.

16) Office of the Executive Secretariat

Office of the Executive Secretariat is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

17) Office of General Counsel (OGC)

Typical Transaction

OGC collects sensitive PII/BII from employees and contractors to support its daily mission. The information is used for operational purposes including: budgeting, human resources management, property management, travel management, and contract management. The information is collected via forms completed by employees and contractors and contract copies received for products and services acquired.

General Litigation receives claims via Government standard forms SF-91 and SF-95 electronically or by mail. Certain PII/BII is collected to review and process claims made against the government to determine whether payment is appropriate.

Information sharing

Administrative information is shared internally within the office. Litigation information is shared within the bureau, the US Government, and foreign entities.

Legal authority to collect PII and/or BII

Form 95 Authority to collect 5 U.S.C. 301, 28 U.S.C 501 et seq. , 28 U.S.C. 2671., 28 C.F.R.

18) Office of Legislative and Intergovernmental Affairs (OLIA)

Typical transaction

The Office of Legislative and Intergovernmental Affairs collects Public/Government PII and sends it in to the White House or the Department of Commerce's White House Liaison's office through the secure file transfer system. The PII is collected so that the individuals requiring access to the White House may be processed.

Information sharing

Information is shared with the White House or Department of Commerce's White House Liaison Office.

Legal authority to collect PII and/or BII

DOO 25-4B Section 6.

19) Office of Public Affairs (OPA)

Typical transaction

The Office of Public Affairs (OPA) has the potential to store information, such as PII and BII to conduct the work of the office in setting up media interviews, disseminating public information as it pertains to the Department and its bureaus, and maintaining media lists and business contact lists. This PII and BII is usually stored as contacts, as a media list, database or as a stand-alone document. Only OPA staff members can access data entered by OPA staff and only OPA users can edit that data.

Information sharing

In a typical transaction, media contacts and outlets along with organization information is shared between OPA and the twelve Department of Commerce bureaus. This information may also be shared with other U.S. government agencies such as the White House, Department of Interior, etc. on an as needed basis.

Legal authority to collect PII and/or BII

DOO 15-3 Section 3
DAO 219-1 Sections 4, 5, 6, 7, 8, 9, 10, 11 and 14

20) Business USA (BUSA)

Typical transaction

BUSA collects non-sensitive PII/BII from employees and contractors to support its daily mission. The information is used for operational purposes including: budgeting, human resources management, property management, travel management, and contract management. The information is collected via forms completed by employees and contractors and contract copies received for products and services acquired.

Information sharing

Contract information is not shared.

Employee information is shared in the form of contact lists with BUSA internal staff.

The OITS-GSS has the potential to store information such as personally identifiable information (PII), business identifiable information (BII) and financial records in support of the mission needs of the Office of the Secretary (OS), supporting bureaus and operating unit components (BOUs). The OITS-GSS also has the potential to process and/or transfer these types of information. In accordance with Federal Information Processing Standard (FIPS) 199, OITS-GSS has a system categorization level of Moderate.

Legal authority to collect PII and/or BII

5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 131614, 41 U.S.C. 433(d); 5U.S.C. 5379; 5 CFR Part 537;DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999, DAO 210-110; Executive Order 12554, Public Law 100-71, dated July 11, 1987.

Other DOC Bureaus:

21) Economic and Statistics Administration (ESA)

The ESA uses enterprise and network services to support their daily mission. The ESA does not collect, maintain or disseminate PII nor does the ESA collect, maintain or disseminate BII such as trade secrets, commercial information or financial information.

22) Economic Development Administration (EDA)

Typical transaction

The EDA downloads grant information from https://www.grants.gov. These downloads may contain sensitive and non-sensitive PII and BII data. These forms are grant applications for local and state governments, education organizations, public housing organizations, nonprofit organizations, for-profit organizations, small businesses, individuals and foreign applicants.

Additionally, the EDA's Business USA Office may collect, maintain and disseminate PII and BII in support of the Revolving Loan Fund Program. This program supplies small businesses and entrepreneurs with gap financing to start or finance businesses.

Information sharing

Grantor and applicant information is shared between Grants.gov and the EDA utilizing the Grants.gov System-to-System feature and the Revolving Loan Fund (RLF).

Legal authority to collect

The collection and maintenance of the BII data information for the Revolving Loan Fund (RLF) program is authorized by the Public Works and Economic Development Act of 1965, as amended by the Economic Development Administration Reauthorization Act of 2004 (Public Law(P.L.) 108-373).

23) Minority Business Development Agency (MBDA)

Typical transaction

The MBDA customer records management system captures the telephone numbers, names and email addresses of each business involved in transactions. This system also includes some personal information of the individuals such as name and phone number associated with the businesses, and source information about the businesses (financial information for contracts, loans, bonding; number of jobs created and retained; professional capacities and certifications such as SBA 8(a) and state minority certifications). MBDA's online tools also capture some BII, such as opportunities for contracts secured or pending in the private and public sectors; and communications between business centers and clients.

Information sharing

Information is shared by the forty-four (44) MBDA Business Development Centers with the MBDA Headquarters located in Washington, D.C.

Legal authority to collect

The authority for collecting the name, addresses, company size, transaction type and amounts, contract amounts, loan amounts, and jobs created of minority business enterprises that receive technical business assistance from the MBDA Business Centers (grantees) is provided in 2 C.F.R. Section 200.328(b)(1) of the Office of Management and Budget's (OMB) Rules for Grant Administration which provides in part: "[t]he non-Federal entity (grantee) must submit performance reports at the interval required by the Federal awarding agency."

The authority for MBDA's grant program is contained in Executive Order 11625, which authorizes the Secretary of Commerce to provide financial assistance to public and private organizations so that they may render technical and management assistance to minority business enterprises. The Secretary's authority was delegated to the National Director of MBDA in Section 3 of Department Organization Order (DOO) 25-4A, Minority Business Development Agency. The MBDA grant program is also authorized by 15 U.S.C. § 1512.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____This is a new information system.

_x__This is an existing information system with changes that create new privacy risks *(check all that apply).*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained or disseminated *(check all that apply).*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID	X	i. Credit Card	X
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	X
c. Employer ID	X	g. Passport	X	k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:

OGC – SSN required as part of travel processing for repayment of vouchers.

MBDA – SSN are sometimes received inadvertently through resumes for new hires, center directors, and clients of business centers.

OCR – SSNs are no longer collected but some older records retained due to litigation holds contain them.

OHRM – SSNs are used as a unique identifier, for a number of HR related systems.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	X
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X

c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	X
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	X
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. XJob Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
OCR – Narrative information regarding claims of discrimination.

2.2 Indicate sources of the PII/BII in the system (*check all that apply*).

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify):					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed (*check all that apply*).

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	X
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns (*check all that apply*).

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated (*check all that apply*).

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation	X	For criminal law enforcement activities	
For civil enforcement activities	X	For intelligence activities	

To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Grant program requirements			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

s.

In general, twenty-three (23) Business Operating Units (BOU) within DOC use OITS-GSS services for data storage and retrieval of program information supporting official daily responsibilities and the organization's mission. Information use is limited to: developing policies, managing programs and providing oversight for collaborative efforts with business customers. The official needs of the BOU determine the extent of the information sharing with other organizations.

The information is collected from federal employees, contractors, Departmental non-government personnel, and foreign nationals based on OITS-GSS customer missions. All information access is controlled based on user business roles which restrict the ability to view, copy, modify, and delete the information. The data is restricted for dissemination based on business office documented requirements in accordance with published guidelines.

The actual use of the GSS services is described in more detail in the "Typical Transaction" section under each BOU and below:

Economic and Statistics Administration (ESA)

ESA is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Economic Development Administration (EDA)

Grant applications/forms:

The forms used for the grants' request requires the information. The information is used to determine eligibility.

Revolving Loan Fund (RLF) Program:

The type of business identifiable information (BII) contained in RLFMS is primarily financial data and could include business names, bank information, borrow loan account information,

and additional grantee and borrower information. The information is collected to be in compliance with the semi-annual RLF reporting requirements.

Minority Business Development Administration (MBDA)

The Minority Business Development Agency uses potentially sensitive BII and race/ethnicity information collected from minority business enterprises to determine eligibility for participation as clients of the MBDA Business Center program. The information collected is from members of the public

MBDA maintains and collects PII when conducting HR actions such as hiring new employees. These are for administrative matters pertaining to contractors and federal employees.

Office of Business Liaison (OBL)

As part of our office's responsibilities, we collect names and contact information for key individuals from the private sector and relevant industry associations. Part of the business processes include compiling the data in spreadsheets and using the information to extend invitations to relevant events hosted by DOC and/or set-up one-on-one meetings with members of the team. Collection and use of this data is critical to our office's mission of representing private sector interests through strategic engagement.

Center for Faith Based and Neighborhood Partnerships (CFBNP)

CFBNP collects this information to bring people to meetings with White House staff that are focused on key Commerce and White House programming around economic development, job creation, business development, trade, and other areas of community improvement.

Office of Acquisition Management (OAM)

The information from System for Award Management (SAM) is used to fulfill policy requirements set forth by the FAR and to ensure that every action awarded to a vendor/contractor meets the needs and requirements of the Department of Commerce.

Office of Facilities and Environmental Quality (OFEQ)

Information collected is used for building user access tables to allow assignment of user privilege, and assignment of access passwords.

All information collected will be from federal employees. No contractors, foreign nationals, or visitor information will be collected.

Office of Budget (OB)

The information is collected from federal employees and transmitted to OMB. Federal security personnel for NEOB use the information to verify an attendee's identify in order to grant access to the building. Meetings with the EOP are a necessary aspect of coordinating the preparation and presentation of the Department's annual budget request.

Office of Civil Rights (OCR)

EEO complaints are filed by employees of the Department and applicants seeking employment contact information for the complainant (attorney/representative/union representative) and representatives (OGC's attorney assigned to the case) for either the complainant or the Department. This provides both parties (individuals working with the complainant and the Department representatives) with the notices, reports, decisions, and supporting documents related to the complaint. A complainant is required to provide the demographic and employment information relevant to his or her claim of discrimination. This enables OCR to determine if the complaint meets procedural and/or jurisdictional requirements necessary to direct the scope of the investigation and adjudication of the complaint, which is directly related to OCR's core mission of enforcing nondiscrimination laws.

The BII maintained in OCR's systems contains contact information for law firms, unions and other agencies that represent each individual complainant. Other BII identifies the following: name of the firm contracted to investigate the case, name and contact information of the assigned subcontractor, and the costs associated with the investigation. This category of BII allows OCR to manage its investigative contracts to ensure costs allocated is controlled appropriately and the work is distributed in accordance with the contract statement of work. The contractors and subcontractors do not have access to OCR systems. They are, however vetted to ensure they qualify for the acquisition process related to the complaint filed. Once that process is completed and the contract has been awarded, the case is assigned to a case-worker.

PII and BII are disseminated only within the framework of administrative complaint processes, and/or related litigation in federal court. Information is provided to the OGC's Employment and Labor Law Division, EEOC, Merit Systems Protection Board and/or Assistant U.S. Attorneys on a case-by-case basis. PII may also be shared with the servicing Human Resources Office (SHRO) to the extent required to carry out personnel actions ordered as corrective action, or the agreed terms for settlement.

Statistical data from the system is annually provided to the EEOC, the Office of Personnel Management, the Department of Justice and selected members of Congress in compliance with The No Fear Act and the EEOC Form 462 report.

Office of Financial Management (OFM)

1. The purpose of the Passport and Visa database is to track and maintain official and diplomatic passports and visas for various bureau Federal employees, their spouses, dependents, or otherwise traveling with a DOC employee. The Department of State determines if an employee is eligible to receive a passport and the Travel Staff only records the reason for denial in the database.

2. The purpose of the JP Morgan Chase System is to manage the Department's Travel Card

Program for Departmental Federal employees.

3. The purpose of the Sunflower Personal Property Management System is to maintain accountability of all personal property assets and fleet of vehicles across the Department for Federal employees and contractors.

4. The OFM data analytics program will receive PII data from existing systems of records; WebTA, NFC and PaymentNET using FIPS compliance data transfer. The results of the data analytics are then analyzed and compiled for presentation to Department of Commerce management on a case-by-case basis. A continuous monitoring function is anticipated for the program, where previously collected data are maintained and combined with current data as part of the analytic process.

Office of Human Resource Management (OHRM)

1. Automatic Classification System (ACS) contains key position data that supervisors use to create and simultaneously classify Demonstration Project position descriptions.

2. PPS information collected is intended to ensure accurate rating and ranking of CAPS employees' performance and based on the performance rating, calculate salary increase and bonus payout.

3. ERIS-TL information collected is intended to ensure that the most senior Departmental executives have access to accurate and up-to-date information as to the incumbency status of all key SES positions. It is also referenced in the course of key Departmental decision-making with regard to executive staffing.

4. SES Bonus Pool information collected is intended to ensure the accurate rating, pay adjustment and bonus information of SES employees compiled for the Departmental Executive Resources Board's (DERB) consideration.

5. HANS' intended use is for a more efficient and effective program administration for nominating an employee for gold and silver honor awards and a more efficient process of selecting and ranking the nominees.

6. WebTA is used to track DOC employees' hours; so each employee can be paid or compensated accordingly.

Office of Privacy and Open Government (OPOG)

The PII/BII data will also be used to contact requesters, other federal agencies, and staff fulfilling requests for information, as well as by requesters following up on the status of their requests.

The PII/BII identified in Section 2.1 of this document is in reference to federal employees / contractors, members of the public and private entities.

In order to ensure protection of PII/BII OPOG tracks, maintains metrics, and reports PII

incidents in accordance with OMB guidance. This reporting may contain various elements of PII for investigation and notification.

Office of Performance, Evaluation, and Risk Management (OPERM)

GAO & OIG Audit Liaison & Follow-up:

- Name and business contact information (telephone, email, business address) and job title of (a) Government Accountability Office (GAO) and Commerce Office of Inspector General (OIG) points of contact for audits and other engagements with GAO and OIG, and (b) Commerce and Commerce Bureau employees who participate in GAO and OIG engagements, or are stakeholders in the process, and (c) contacts at other federal agencies that we interact with in connection with Audit Liaison & Follow-up activities. The information is used for OPERM to contact the individuals. It may also be shared with Bureaus/Department Offices or with GAO and OIG for the purpose of advising them of points of contact or attendance at meetings.

Risk Management:

- Name and business contact information (telephone, email, business address) and job title of (a) Department and Bureau employees with a role in the Enterprise Risk Management (ERM) process (such as Risk Management Officers and Enterprise Risk Management Council Members, (b) Commerce and Commerce Bureau employees who are stakeholders in the ERM process, and (c) contacts at other federal agencies who we deal with on interagency risk management efforts. This information may be shared with Bureaus/Department Offices for the purpose of advising them on points of contact or attendance at meetings.

Federal Financial Manager's Integrity Act (FMFIA) and Internal Controls:

- Email distribution list of individual names and email addresses to receive notices and instructions for completing an annual FMFIA report; bureau submission of business information summarizing its internal control and risk management activities.

Program Evaluation:

- Individual names and email addresses to provide instruction and guidance on program evaluations and reviews.

Performance Excellence:

- Individual names and email addresses to provide instruction and guidance on performance excellence.

Office of Security (OSY)

The information is collected from federal employees, contractors, Departmental non-government personnel, and foreign nationals. The data is maintained in the system as a system of record and to verify existing data. Fingerprint data is disseminated to DOJ for the individual background checks. SF 85 and SF 86 form data is disseminated to OPM. The data is then used to determine if employment with the Department is viable. The information is maintained as historical information.

Office of Small and Disadvantaged Business Utilization (OSBDU)

OSBDU is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Office of the Chief Information Officer (OCIO), Office of Cyber Security (OCS)

OCS is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Office of the CIO, Office of the Chief Technology Officer & Deputy Chief Information Officer, Office of Policy and Strategic Planning (OPSP)

OPSP is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Office of the CIO, Office of the Chief Technology Officer & Deputy Chief Information Officer, Office of IT Services (OITS)

The Office of Information Technology Services manages the HCHB digital network, telecommunications services, and network-enabled services, such as emergency broadcast, voice mail, and Internet Domain Name Service. The Office manages Department-wide telecommunications services, such as FTS2001 and WITS, and coordinates telecommunication and networking operations across the Department.

PII is collected from federal employees and contractors so that system accounts can be created on the GSS.

Office of the Executive Secretariat

Office of the Executive Secretariat is not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS.

Office of General Counsel (OGC)

OGC collects this information for disciplinary actions, position advancement, granting access for visitors of senior General Counsel staff, and to provide litigation services for the Secretary

of Commerce and all Operating Units. This information is collected from federal employees, contractors, members of Public who visit commerce facilities.

Office of Legislative and Intergovernmental Affairs (OLIA)

The Office of Legislative and Intergovernmental Affairs collects Public/Government PII and sends it in to the White House or the Department of Commerce's White House Liaison's office through the secure file transfer system. The PII is collected so that OLIA staff members requiring access to the White House may be processed.

Office of Public Affairs (OPA)

The type PII/BII that is collected, maintained, or disseminated by the Office of Public Affairs includes the following:

- Business names
- CEO and business leader contact information
- Media organizations
- Reporter emails and phones
- Additional business/company information that may be important to disseminating Department information publically
- Additional media outlet or reporter information as it pertains to an interview request, event or engagement.

The information collected is pertinent to setting up media interviews, disseminating information as it pertains to the Department and its bureaus, and maintaining media and business contract list. Only information that is required for responding to a public information request, interview request or correspondence is collected and stored.

Business USA (BUSA)

The PII/BII that is collected is used for human resources, acquisitions, and travel. The information collected is from federal employees, contractors, and contracts.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared (*check all that apply*).

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X

DOC bureaus	X	X	X
Federal agencies	X	X	x
State, local, tribal gov't agencies	X		X
Public	X		
Private sector	X		X
Foreign governments	X		
Foreign entities	X		
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
x	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII (*check all that apply*).

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system (*check all that apply*).

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.

X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.commerce.gov/page/privacy-policy .	
X	Yes, notice is provided by other means.	Specify how: ESA – Not collecting, maintaining, or disseminating PII/BIIEDA – Individuals are notified at the Grants.gov website by OMB which is not under the control of EDA. MBDA – Individuals are notified in the MBDA Business Center engagement form. OBL – Individuals are notified verbally during collection process by the OBL POC. CFBNP – Individuals are notified by the CFBNP POC that it is for WAVES purposes to provide to the White House and used to clear them to get into the building by the CFBNP POC. OAM – Individuals are notified during Sam.gov registration. OFEQ – Individuals are notified verbally during the collection process by the OFEQ POC. OB – Individuals are notified by OB POC that it is for WAVES and that their information will be provided to OMB to gain access to the NEOB by the OB POC. OCR – Individuals are notified on the Formal Discrimination Complaint Form. OFM – Individuals are notified in the JPMC Statement of Understanding and Agreement. OFM Data Analytics Program – Under initial collection for the following systems: WebTA, NFC, PaymentNet. OHRM – Individuals are notified in the Onboarding Form. OPOG – Individuals are notified via web form, verbally, and through Privacy Notification by OPOG POC. OPERM – Individuals are notified via email and verbal communications by OPERM POC. OSY – Individuals are notified on the SF-86, SF-85, or SF85p. OSBDU –Not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS. Planning (OPSP) and Office of IT Services (OITS). OCIO, OCS - Not collecting, maintaining, or disseminating PII/BII. OCIO, OCTO&DCIO, OPSP –Not collecting, maintaining, or disseminating PII/BII. OCIO, OCTO&DCIO, OITS – Individuals are notified during interview process by OITS POC for gathering account information. OES – Not collecting, maintaining, or disseminating PII/BII. OGC –Notification is provided via the SF-95 form. OLIA – Individuals are notified during the collection process by the collector and/or DOC employee. OPA – Individuals are notified via email and verbal

		communications by OPA POC. BUSA – Individuals are notified via email communications and Discrimination Form (CD-498), which contains a Privacy Act notice.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: ESA – Not collecting, maintaining, or disseminating PII/BII. EDA - Grant data: The individual can decline to provide the data. The individual has to provide information on the form to process their grant request. MBDA – Individuals can decline verbally or in writing to the MBDA or MBDA Business Center. OBL – Individuals can decline verbally to the OBL POC. CFBNP – Individuals can decline verbally to the CFBNP POC. OAM – Individuals can decline during Sam.gov registration. OFEQ – Individuals can decline via the application for parking. OB – Individuals have the ability to decline verbally to the OB Coordinating Analyst. OCR – Refusal to provide information relevant to the investigation and adjudication of the complaint may result in dismissal of the complaint. OFM – Individuals can decline by not signing the application and/or agreement. OFM Data Analytics Program – Under initial collection for the following systems: WebTA, NFC, PaymentNet. OHRM – Individuals can decline by not accepting the position of employment verbally or in writing to the OHRM POC. OPOG – Individuals can decline by not filling out web form or verbally with the OPOG POC. OPERM – Individuals can decline via email and verbal communications with the OPERM POC. OSY - Individuals can decline to provide the requested information online by not submitting the information. OSBDU – Not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS. OCIO, OCS - Not collecting, maintaining, or disseminating PII/BII. OCIO, OCTO&DCIO, OPSP – is not collecting, maintaining, or disseminating PII/BII OCIO, OCTO&DCIO, OITS – Individuals can decline by refusing to complete account request forms. OES – Not collecting, maintaining, or disseminating PII/BII. OGC – Individuals can decline to provide PII at the time of filling out SF-91 or SF-95. Denial of submitting certain PII could result in denial of claim.

		OLIA – Individuals may decline verbally or in writing to the OLIA POC. OPA – Individuals can decline verbally or in writing to the OPA POC. BUSA – Individuals can decline to Product Manager via an email response to sender.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: EDA – RLF data: No individuals will have the opportunity to decline providing information as there are currently no voluntary collections within RLFMS. Many parts of the data contained with RLFMS are mandatory and must be provided for proper use of reporting the RLF portfolios. Failure to provide the information may render it impossible for EDA to correspond with the requestor.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: ESA – Not collecting, maintaining, or disseminating PII/BII. EDA - Grant data: The individual can decline to provide the data. The individual has to provide information on the form to process their grant request. MBDA – Individuals can decline verbally or in writing to the MBDA or MBDA Business Center. OBL – Individuals can decline verbally to the OBL POC. CFBNP – Individuals can decline verbally to the CFBNP POC. OAM – Individuals can decline during Sam.gov registration. OFEQ – Individuals can decline via the application for parking. OB – Individuals have the ability to decline verbally to the OB Coordinating Analyst. OCR – Refusal to provide information relevant to the investigation and adjudication of the complaint may result in dismissal of the complaint. OFM – Individuals can decline by not signing the application and/or agreement. OFM Data Analytics Program – Under initial collection for the following systems: WebTA, NFC, PaymentNet. OHRM – Individuals can decline by not accepting the position of employment verbally or in writing to the OHRM POC. OPOG – Individuals can decline by not filling out web form or verbally with the OPOG POC. OPERM – Individuals can decline via email and verbal communications with the OPERM POC. OSY - Individuals can decline to provide the requested information online by not submitting the information. OSBDU – Not collecting, maintaining, or disseminating

		PII/BII information on the OITS-GSS. OCIO, OCS - Not collecting, maintaining, or disseminating PII/BII. OCIO, OCTO&DCIO, OPSP – is not collecting, maintaining, or disseminating PII/BII OCIO, OCTO&DCIO, OITS – Individuals can decline by refusing to complete account request forms. OES – Not collecting, maintaining, or disseminating PII/BII. OGC – Individuals can decline to provide PII at the time of filling out SF-91 or SF-95. Denial of submitting certain PII could result in denial of claim. OLIA – Individuals may decline verbally or in writing to the OLIA POC. OPA – Individuals can decline verbally or in writing to the OPA POC. BUSA – Individuals can decline to Product Manager via an email response to sender.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: MBDA - No separate distinction on use for particular purposes; e.g., transfer to ESA for studies or other uses.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: ESA – Not collecting, maintaining, or disseminating PII/BII. EDA - Via the RLF program reporting process which is semi-annual. MBDA – Individuals can contact MBDA or their operating MBDA Business Center verbally or in writing OBL – Individuals can review/update through the Office of the Secretary Scheduling Office CFBNP – In writing to the CFBNP POC. OAM – Individuals can review/update at Sam.gov OFEQ – Employees notify the OFEQ POC when administrative PII requires updating. OB – Individuals provide their updated information directly to OB for transmission to OMB. OCR - Individuals can contact OCR compliance staff to review or add updates to their files. OFM - Over the phone and online to the PFM POC. OFM Data Analytics Program – Data has been previously collected from users through other systems and/or applications. Data received for this program is for analysis only and not changes can be made to it once received by OFM. OHRM – Individuals update via their employee official

		personnel file (e-OPF) via their online account. OPOG - Through the Privacy Act individuals have the opportunity to review/update PII/BII pertinent to them. They can submit updated web forms. OPERM - Individuals provide updated contact information by email, phone, or hard copy to the OPERM POC. For information maintained in contact lists, updates are periodically requested by the OPERM POC. OSY – Individuals may contact Human Resources personnel to review or update their personal information. OSBDU – Not collecting, maintaining, or disseminating PII/BII information on the OITS-GSS. OCIO - Employees notify the OCIO POC when administrative PII requires updating. OCS – is not collecting, maintaining, or disseminating PII/BII OCIO, OCTO&DCIO, OPSP – is not collecting, maintaining, or disseminating PII/BII OCIO, OCTO&DCIO, OITS – they resign the acceptable use policy on the annual basis where they are required to verify their information OES – is not collecting, maintaining, or disseminating PII/BII OGC – Individuals can review and update their PII online via electric online personnel file (EOPF) OLIA – OLIA is only forwarding the information provided by the applicant. OPA – Verbally and in writing to the OPA POC BUSA – An email may be sent to the Product Manager to confirm the accuracy of information.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system (*check all that apply*).

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: OFM Data Analytics Program – Contractor access is limited to contractor staff who have signed non-disclosure agreements and are escorted by OFM staff, after signing-in and clearing security to enter the building. Access is monitored by physical observation by OFM staff. Laptop is located in a secure section of the building with auto-locking doors before and after core working hours. In addition, the area has security cameras which are monitored by building security.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): June 16, 2016 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.

X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

The OITS-GSS systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in-transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Use of trusted internet connection (TIC)
- Anti-virus software to protect host/end-user systems
- HSPD-12 compliant PIV cards
- Access controls

The OITS-GSS systems also follow the National Institute of Standards and Technology (NIST) standards, including special publications 800-53, 800-63, 800-37, etc… Any system within the organization that contains, transmits or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The organization also employs data loss prevention (DLP) solutions as well. The DLP is an e-mail scan of unencrypted e-mail traffic, to included attachments, to detect inappropriate transport of sensitive information.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice [SORN] is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN).

	Provide the SORN name and number **COMMERCE/DEPT 1 – 23,** COMMERCE /DEPT-1—Attendance, Leave, and Payroll Records of Employees and Certain Other Persons COMMERCE /DEPT-2—Accounts Receivable COMMERCE /DEPT-3— Conflict of Interest Records, Appointed Officials COMMERCE /DEPT-4— Congressional Files COMMERCE /DEPT-5— Freedom of Information and Privacy Request Records COMMERCE /DEPT-6— Visitor Logs and Permits for Facilities Under Department Control COMMERCE /DEPT-7— Employee Accident Reports COMMERCE /DEPT-8— Employee Applications for Motor Vehicle Operator's Card COMMERCE /DEPT-9— Travel Records (Domestic and Foreign) of Employees and Certain Other Persons COMMERCE /DEPT-10— Executive Correspondence Files COMMERCE /DEPT-11— Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees COMMERCE /DEPT-12—OIG Investigative Records COMMERCE /DEPT-13— Investigative and Security Records COMMERCE /DEPT-14— Litigation, Claims, and Administrative Proceeding Records COMMERCE /DEPT-15— Private Legislation Claimants-Central Legislative Files COMMERCE /DEPT-16— Property Accountability Files COMMERCE /DEPT-17— Records of Cash Receipts COMMERCE /DEPT-18—Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE /DEPT-19— Department Mailing Lists COMMERCE /DEPT-20— Biographical Files and Social Networks COMMERCE /DEPT-22— Small Purchase Records COMMERCE /DEPT-23—Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs **EEOC GOV-1** EEOC /GOVT-1—Equal Employment Opportunity in the Federal Government Complaint and Appeal

	Records.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance (*check all that apply*).

X	There is an approved record control schedule. Provide the name of the record control schedule: **National Archives and Records Administration (NARA) General Record Schedules –** General Record Schedule 1, General Record Schedule 3, General Record Schedule 9, General Record Schedule 14, General Record Schedule 16, General Record Schedule 18, General Record Schedule 23
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII (*check all that apply*).

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Pubication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels (*check all that apply*).

X	Identifiability	Provide explanation: Certain PII is uniquely and directly. Identifiable.
X	Quantity of PII	Provide explanation: Large PII datasets are present on the system.
X	Data Field Sensitivity	Provide explanation: Certain combinations of system PII data fields are sensitive.
X	Context of Use	Provide explanation: OFM Data Analytics Program – Statistical analysis will be performed on the data collected from each system.
	Obligation to Protect Confidentiality	Provide explanation: OFM Data Analytics Program – Any *PII included in the results of processing may be transferred offsite on a case by case basis to DOC bureaus not located in HCHB. Files are transmitted using the approved DOC secure file transfer processing.*
X	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: HR functions will provide privacy notices with forms used for the collection of PII (this includes paper forms and data-entry forms) until permanent solution is implemented.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Ensure encryption of data at rest for all databases containing sensitive PII and ensure mandatory use of HTTP(S) for public-facing websites.
	No, the conduct of this PIA does not result in any required technology changes.

Vanessa Rini-Lopez - NOAA Federal

From:	Vanessa Rini Lopez NOAA Federal
Sent:	Thursday, March 29, 2018 9:16 AM
To:	Mark Graff NOAA Federal
Subject:	GSA login.gov agreement
Attachments:	LOGIN.GOV_NOAA_MOA20170517 V1.docx

Hi, DOC gave us the go ahead to get the attached agreement cleared. I want to make sure you are okay with it before I submit it to DOC for clearance.

Thanks.

Vanessa Rini-López
Management and Program Analyst, Resource Management Division
DOC/NOAA/OCIO
SSMC3, 9745, Silver Spring, MD
Office: 301-628-5744
Cel (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 29, 2018 3:08 PM
To:	Gioffre, Kathy (Federal); CPO
Cc:	Mark Graff NOAA Federal; Nancy Defrancesco
Subject:	NMOAA5032 certification docs
Attachments:	NOAA5032 2017 PIA revised 20180306 For NOAA BCPO Signature mhg.pdf; NOAA5032_PIA_Annual_Review_Certification_Form_with_PA_Officer__20180301_signed_PA officer mhg.pdf; NOAA5032_PTA_Feb2018_for OSPO coAO signature vig mhg.pdf

(Kathy, this is not the one I was just calling you about, but I was hanging onto and am now sending).

ATO: 8 16 18

Last CRB: 8 4 17.

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA5032
Wallops Command and Data Acquisition Station (WCDAS)
Administrative Local Area Network (LAN)

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA WCDAS Administrative LAN

Unique Project Identifier: NOAA5032 (not affiliated with an Exhibit 300).

Introduction: System Description

The WCDAS (Wallops Command and Data Acquisition Station) Administrative LAN (NOAA5032) is located within the WCDAS computer facility in Wallops Island, VA. The WCDAS Administrative LAN supports the NESDIS mission by providing IT resources to WCDAS personnel. Although the system does not collect or store PII (other than employee contact information) or BII, the system does support office functions that distribute PII and BII such as electronic mail, purchasing, logistics, facility management, inventory, human resource, and contract administration. *These functions use paper files as the source of the PII and BII distributed; for purchasing and human resources functions, information from paper files is typed into portals or emails (HR information by email is covered by the NOAA1200 PIA approved by DOC on March 24, 2017). No sensitive PII from HR functions is stored within the accreditation boundaries.*

WCDAS Administrative Local Area Network (LAN) is a standard office automation environment that relies on the NOAA NOC (NOAA 0200) for VPN access to the NSOF Administrative LAN (NOAA5044), and Internet connectivity.

Employee PII is collected for Emergency Contact information.

The WCDAS Administrative LAN does not share this information with any agency. Information is shared within the bureau on a case by case basis.

Authorities: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks.
__X__ This is an existing information system with no changes that create new privacy risks.

(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth*		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name*	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice		f. Vascular Scan		i. Dental Profile	

Recording/Signatures					
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The Business Continuity Plan (BCP) is used for emergency contact of WCDAS employees. This information is collected from Federal Employees only.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors			
Other (specify): Limited Administrative personnel			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found on the	
X	Yes, notice is provided by other means.	Specify how: Notification is provided in writing by the employee's supervisor or by the administrative staff. Verbal notices is provided to employees when requesting information for COOP activities.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Federal employees have an opportunity to decline to provide PII to their supervisors, in writing, but they would not be contacted during an emergency.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Individuals may choose not to be contacted during an emergency, by declining in writing to their supervisors. This is the only use of the information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals may consult administrative personnel who have access to their PII and provide updates to them. This information is conveyed in writing as part of the employee orientation.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/16/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

PII/BII on this IT system is protected through the use of hardware and software firewalls, Cisco ASA Firewalls, Cisco IPS; Windows software firewalls; Tripwire Enterprise; Tripwire Log Center; ArcSight deployed and reporting back to NOAA Enterprise Security Services; HSPD-12 compliant with two factor authentication; McAfee Data Loss Prevention enabled, blocking all unauthorized USB drives and external hard drives.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: DEPT-18, Employees Personnel Files not Covered by Notices of Other Agencies.
	Yes, a SORN has been submitted to the Department
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Chapter 200-01
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.

	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: Contact information only is maintained for a BCP.
X	Data Field Sensitivity	Provide explanation: There is no sensitive PII.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:

X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Johnny R. Clark Office: NESDIS/OSPO/WCDAS Phone: 757-824-7328 Email: bob.clark@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK.JOHNNY.R.1365842791 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn CLARK.JOHNNY.R.1365842791 Date: 2018.03.06 15:06:38 05'00' Date signed: 3/6/2018	**Information Technology Security Officer** Name: Nancy DeFrancesco Office: NESDIS ACIO-S Phone: 301-713-1312 Email: nancy.defrancesco@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.03.07 14:57:35 -05'00' Date signed: 03/07/2018
Authorizing Official Name: Vanessa Griffin Office: NESDIS/OSPO Phone: 301-713-7311 Email: vanessa.griffin@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.08 08:47:48 -05'00' Signature: Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.08 10:32:08 -05'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA5032 PIA

FISMA Name/ID (if different): NOAA5032 (WCDAS ADMIN LAN)

Name of IT System/ Program Owner: Johnny R. Clark

Name of Information System Security Officer: Mark O. Hall

Name of Authorizing Official(s): Vanessa Griffin

Date of Last PIA Compliance Review Board (CRB): 08/16/2016

(This date must be within three (3) years.)

Date of PIA Review: 3/6/2018

Name of Reviewer: Johnny R. Clark

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK JOHNNY R 1365842791
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn CLARK JOHNNY R 1365842791
Date 2018 03 06 13 58 59 05'00'

Date of Privacy Act (PA) Review: 3/8/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488
Date 2018 03 08 12 52 51 05'00'

Date of BCPO Review: 3/26/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892
Date: 2018.03.26 10:17:03 -04'00'

U.S. Department of Commerce (DOC)
National Oceanic and Atmospheric Administration (NOAA)
National Environmental Satellite, Data, and Information Service (NESDIS)

Privacy Threshold Analysis (PTA)
For the
Wallops Command and Data Acquisition Station Administrative Local Area Network (NOAA5032)

Version: 1.0
February 12, 2018

U.S. Department of Commerce Privacy Threshold Analysis

Office of Satellite and Product and Operations (OSPO)

Unique Project Identifier: NOAA5032

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
(a) The Wallops Command and Data Acquisition Station (WCDAS) Administrative LAN (NOAA5032) is a General Support, office automation system that (b) is located within the WCDAS computer facility in Wallops Island, VA. (c) NOAA5032 relies on the NOAA NOC (NOAA 0200) for e-mail, and VPN access to NSOF (NOAA5044) for Internet connectivity. (d) The WCDAS Administrative LAN supports the NESDIS mission by providing IT resources to WCDAS personnel. Specifically, it is used to support electronic mail, purchasing, logistics, facility management, inventory, human resource, contract administration, general management functions and office automation functions (e) The WCDAS Administration LAN enables communication among OSPO and various NOAA groups to conduct administrative functions which include daily, weekly, monthly, and annual reports. The WCDAS Administration LAN is used to support electronic mail (GMAIL) through the use of Google, purchasing, logistics, facility management, inventory, human resource, contracts administration, general management functions, and office automation functions. (f) Types of data transiting thru or residing on the WCDAS Administration LAN include administrative email messages, data concerning time and attendance reports, status reports, travel orders, Federal grants, environmental monitoring, budget and capital planning, contingency planning, facilities management, workplace policy, human resources, goods acquisition, and IT infrastructure management. Data transiting or resident on the WCDAS Administrative LAN are typically in the form of e-mail messages, Excel spreadsheets, word processing documents, CAD drawings and simple databases resident on individual workstations. (g) The Users community of the WCDAS Administration LAN include management, technical, operations and administrative staff located at the Wallops Command and Data Acquisition Station. (h) Workstations located in the users' offices are used by the operational personnel, to log into their own user accounts on the WCDAS Domain where they can perform various administrative functions, and print to local and / or network printers. (i) A

dedicated DS-3 link provides the Wide Area Network (WAN) access from WCDAS Administration LAN to and from the Internet through the NOAA NOC.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

___ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X_ I certify the criteria implied by one or more of the questions above **apply** to the Wallops Command and Data Acquisition Station Administrative Local Area Network and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Wallops Command and Data Acquisition Station Administrative Local Area Network and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Owner (SO): Johnny R. Clark

Signature of SO: CLARK.JOHNNY.R.1365842791 Digitally signed by CLARK.JOHNNY.R.1365842791 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=CLARK.JOHNNY.R.1365842791 Date: 2018.02.14 09:32:40 05'00' Date: 2/14/2018

Name of Information Technology Security Officer (ITSO): Nancy A. DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digitally signed by DEFRANCESCO.NANCY.A.1377370917 Date: 2018.02.14 15:01:31 -05'00' Date: 02/14/2018

Name of Authorizing Official (AO): Vanessa L. Griffin

Signature of AO: GRIFFIN.VANESSA.L.1204308663 Digitally signed by GRIFFIN.VANESSA.L.1204308663 Date: 2018.03.01 14:40:34 05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark H. Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.01 16:00:06 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, March 29, 2018 3:15 PM
To:	Gioffre, Kathy (Federal); CPO
Cc:	Mark Graff NOAA Federal; Tahir Ismail; Karl Mueller NOAA Federal
Subject:	NOAA4800 certification docs
Attachments:	NOAA4800 PIA 03 15 2018 rev3 mhg.pdf; NOAA4800 PIA Annual Review Certification Form for MHG signature mhg.pdf; NOAA4800 PTA 02 07 2018 signed (1) mhg.pdf

Kathy, the last CRB was 5 12 17 and we were concerned that we would go past this anniversary.

The next ATO date is 11 20 18.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 04-2017

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA4800 - Alaska Fisheries Science Center (AKFSC) Network

Reviewed by: _____, Bureau Chief Privacy Officer
Catrina D. Purvis

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA4800 - Alaska Fisheries Science Center (AKFSC) Network

Unique Project Identifier: NOAA4800

Introduction: System Description

NOAA4800 is a moderate level system with three data sets that contain either PII or BII within its boundaries.

NORPAC Database (Observer Data)

NORPAC refers to the observer data collection within the North Pacific by the Fisheries Management and Analysis (FMA) division within NOAA4800. In the past, it was referred to simply as the Observer Database. It is not a true acronym. The database consists of various data collected by fishery biologists while deployed on board commercial fishing vessels or at shoreside processing plants participating in the Bering Sea and Gulf of Alaska groundfish fisheries. Data collection activities began in 1973 and they continue to date. While deployed at their assignments, observers collect data on the catch size, fishing locations, catch composition, length frequencies, age structures, marine mammal interactions, and a variety of research projects. The specific data components collected are outlined in the Groundfish Observer Manual. Once received by FMA, these data are extensively checked for quality and are then entered onto an Oracle database and made available to authorized staff. The database also stores observer training records and performance evaluations.

All of these data are collected cooperatively from private commercial fishing interests and are protected from general release by confidentiality statutes. This protects the private business interests of industry while still providing NOAA Fisheries with the detailed information necessary to effectively manage the ecosystem.

NMFS Groundfish Tagging Program

The collection of information for the National Marine Fisheries Service (NMFS) Groundfish Tagging Program has been in operation since the early 1970s. This information collection covers the Groundfish Tagging Program on the West Coast and Alaska. The NMFS Groundfish Tagging Program provides scientists with information necessary for effective conservation, management, and scientific understanding of the groundfish fishery resources off Alaska. Data from the releases and recoveries that are collected through this program have been used to examine movement patterns, evaluate areal apportionment strategies of annual catch quota, validate ageing methods, and to examine growth.

When a tag is recovered, typical information given by the respondent is: (1) tag number, (2) date of capture, (3) location of capture, (4) size of fish, (5) sex of fish, (6) depth of capture, (7) gear type, (8) vessel name, and (9) name and address of reward recipient. The standard tag recovery form is attached to a prepaid business reply envelope. Individuals use this envelope to submit and record recovery information for each tag. Each recovery envelope contains a confidentiality

statement. Submitting tag recovery information is voluntary, and the amount of information received can vary with each recovery.

Submitting tag recovery information is voluntary. Tags (recovery information) are generally collected from fishermen and processors. Tags can be sent in directly from these individuals, as well as from observers and port samplers with NMFS, the Alaska Department of Fish and Game (ADFG), and Canada Department of Fisheries and Oceans (DFO). Information sent in by NMFS observers includes the vessel captain's signature approving the collection and use of the provided data.

Economic Data Report (EDR) Dataset

The EDR data collection forms collect confidential business data on costs, revenues, ownership, employment, and physical plant characteristics from vessels, processors, and Quota Share permit holders licensed to participate in federally managed crab and groundfish fisheries in Alaska. In addition to business data, the forms also include name, title, telephone and fax numbers, and email address of the person submitting the EDR form; name and address of the owner or leaseholder of the vessel or plant; Federal Fishery processor or vessel permit number, Coast Guard vessel registration number, federal license number, Registered Crab Receiver number, State of Alaska seafood processor number, and ADF&G Commercial Crew License or CFEC Gear Operator Permit number of vessel crew members.

EDR data is collected on an annual basis from vessels, processors, and quota share holders participating in selected catch share programs developed by North Pacific Fishery Management Council and administered by NMFS Alaska Regional Office, specifically, the Bering Sean and Aleutian Islands (BSAI) Crab Rationalization Program, American Fisheries Act pollock fishery, Amendment 80 Non-pollock Groundfish Trawl fishery, and Gulf of Alaska groundfish trawl fisheries. To monitor changes in the economic performance of the affected fisheries following rationalization and subsequent management changes, the NPFMC developed the respective EDR data collections to provide analysts with economic information not available from other sources. The EDR data collections also contribute to meeting the requirements of the MSA for catch share program evaluation.

NORPAC Information Sharing:

The staff authorized to use these data include NOAA Fisheries' scientists and managers participating in a broad range of activities including:

- stock assessments,
- marine mammal interactions,
- food habits,
- fish age analyses,
- economic analyses,
- fishery management plan development,
- in-season fishery management.

The data are also shared with other authorized users in the Alaska Department of Fish and Game (ADF&G) and North Pacific Fishery Management Council (NPFMC) staff with similar responsibilities.

Aggregations of observer data which protect confidentiality are periodically developed and released to the public. Observer data serve as essential building blocks for numerous public analyses, reports, and scientific documents.

Groundfish Tagging Information Sharing:
Only the data steward regularly accesses data contained in the system to input new data, and to analyze and report on the status of the NMFS Groundfish Tagging Data. Other people who have direct access to the ABL Tag data are limited staff and contractors of the Auke Bay Laboratories Division only if they are doing appropriate research, and have signed confidentiality agreements and ORACLE access approval forms. Any other NOAA employee or contractor would not have direct access to the system.

Data is often shared with the Northwest Fisheries Science Center (NWFSC), the Southwest Fisheries Science Center (SWFSC), the ADF&G, and the DFO. Shared data has been aggregated in a way that confidentiality (of fishing locations) hasn't been breached, and names/addresses are never shared. All publicly available data are aggregated so that no PII/BII information is provided.

EDR Data Sharing:

EDR data is treated as confidential federal fisheries data, and made available only to NMFS and ADF&G staff and contractors, after submission of non-disclosure agreement documentation.

Data collected in the EDR program is scientific data of a unique kind and is not subject to expiration. As such, the data is maintained indefinitely, under appropriate security protocols, for use by analysts and is not destroyed.

Legal authorities to collect PII and/or BII for NORPAC:
Magnuson Stevens Fishery Conservation and Management Act (MSA); Marine Mammal Protection Act; Endangered Species Act; and 50 CFR 660.16 Groundfish observer program.

Legal authorities to collect PII and/or BII for the Groundfish Tagging and Recovery Program:
The groundfish tagging and tag recovery program is part of the fishery resource assessment that NMFS conducts under the Magnuson-Stevens Act Coauthority as codified in 16 U.S.C. 1854 (e) and 1801 (a)(8).

Legal authorities to collect PII and/or BII for EDR:
BSAI Crab Rationalization: 50CFR680.6
American Fisheries Act (AFA)/Amendment 91: 50 CFR 679.65
Amendment 80:50 CFR 679.94
Gulf of Alaska () Trawl Regulations: 50 CFR 679.110

NOAA4800 is a moderate impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__X_ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
EDR: EDR records contain identifiers for the individual entities (corporate and/or natural persons) that provide the EDR data, including submitted name and address, fishery permit and license numbers held, identification numbers of fishing vessels owned/operated by the subject entities (ADF&G vessel id, USCG vessel id, and associated federal fishery permit numbers), and commercial fishing crew license numbers (ADF&G Commercial Crew and Commercial Fisheries Entry Commission (CFEC) Gear Operator Permit) for crewmembers of related fishing vessels .					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

NORPAC: Observers' emergency contact information (whom to contact in case of observer emergency)

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number		g. Salary	
b. Job Title		e. Email Address		h. Work History	
c. Work Address		f. Business Associates			
i. Other work-related data (specify): **NORPAC**: Observer deployments, official observer statements (also called incident reports, affidavits. Sometimes when an observer witnesses a potential violation, OLE requests them to fill out a statement regarding the event). Vessel length and type; vessel safety checklist, Work related Performance (Observer Training, Evaluations)					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
NORPAC: Observer collected data is comprised of: vessel characteristics information (name, United States Coast Guard (USCG) number, number of crew, captain name), fishing effort information (fishing locations, gear used, depth etc), catch information (species caught, retained and discard, species compositions), biological data (otoliths, lengths, tissue samples) and protected species information (takes, injuries, sightings, samples, specimen collection). **EDR** :In addition to individual identifiers described above, EDR data fields include annual aggregate information related to the subject operation regarding quantities and expenditures on operating costs and capital investments, quantity and value of seafood products produced and sold and royalties paid and received for fishery permits, employment and remuneration of vessel crew and processing line labor, individual crewmember, licenses, vessel and physical plant characteristics, and operational information including counts of days operating and rates of fuel consumption.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax	X	Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal	X	Foreign			

Other (specify

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization		For web measurement and customization	

technologies (single-session)		technologies (multi-session)	

Other (specify):

NORPAC: Observer data serve as essential building blocks for numerous public analyses, reports, and scientific documents.

NMFS Groundfish Tagging Program provides scientists with information necessary for effective conservation, management, and scientific understanding of the groundfish fishery resources off Alaska. Groundfish tagging programs in the northeastern Pacific Ocean and Alaska waters provide essential research data on groundfish life histories (validation of ageing methods, growth, and recruitment into the fishery), and migration patterns (evaluation of areal apportionment strategies of annual catch quota) that are necessary for implementing management regimes. Address data is requested so that the individual who returned the tag may receive a reward. The reward system improves participation in the program and increases the tag recovery rate.

EDR: To monitor changes in the economic performance of the affected fisheries following rationalization and subsequent management changes, the NPFMC developed the respective EDR data collections to provide analysts with economic information not available from other sources. The data are routinely used in decision support analyses conducted for NPFMC and NMFS fishery management deliberations and rule making.

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

All of the information in the data collections is in reference to members of the public who participate in the commercial fisheries of the North Pacific. The information is used in a variety of ways detailed below.

NORPAC: Information collected from vessels is used in fisheries management and stock assessments. Information collected by observers, including statements of fact from vessels in the fishery may also be used by law enforcement to investigate and prosecute potential violations or criminal activity. Information collected is from members of the public. Information collected is used to determine eligibility of applicants wishing to be trained as a federal fishery observer. There are educational and other requirements specified in the federal register that must be met for a person to be eligible. NORPAC also serves as the access point to NMFS Office of Law Enforcement (OLE) and USCG to view statements of fact and other incidents. Statements of fact are stored in the NORPAC database. Information collected is from members of the public, specifically the commercial fishing entities and the observers.

NMFS Groundfish Tagging Program: This program requests data on (1) tag number, (2) date of capture, (3) location of capture, (4) size of fish, (5) sex, (6) depth of capture, (7) gear type, (8) vessel name, and (9) name and address of reward recipient. This information provides scientists with information necessary for effective conservation, management, and scientific understanding of the groundfish fishery resources off Alaska. Address data is requested so that the individual who returned the tag may receive a reward. The reward system improves participation in the program and increases the tag recovery rate. Aggregated data and analyses are compiled annually and publicly distributed in the Blackcod Almanac, and periodically presented in a more thorough formal report for industry members. Information collected is from members of the public and NMFS, IPHC, and ADFG observers and portside samplers.

EDR: EDR data is collected on an annual basis from firms operating fishing vessels and processing plants, and entities holding fishery quota shares, Data elements collected as described in Section 1 above are needed to facilitate analyses of past and potential future changes in the economic performance of the affected vessel and processing operations, economic impact on associated fishery-dependent communities, and evaluation of magnitude and distribution of economic welfare effects that participate in fisheries for which following rationalization and subsequent management changes, The NPFMC developed the respective EDR data collections to provide analysts with information not available from other sources to perform the economic analyses required as part of regulatory review under NEPA and meeting catch share program evaluation requirements under MSA.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access

Within the bureau	X	X	X
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies	X*	X**	
Public			
Private sector			
Foreign governments	X*	X**	
Foreign entities			
Other (specify):			

*Alaska Department of Fish and Game and Canada Department of Fisheries and Oceans – NORPAC Data

** ADF&G and DFO – aggregate groundfish tagging data

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA4800 has Interconnection Security Agreements (ISAs) with two other NMFS entities- NOAA4000 and NOAA4600. These NMFS systems all use similar technical controls (encryption, proper labeling, audit logs, etc) to prevent any PII/BII leakage.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify): **NORPAC:** The staff authorized to use these data include NOAA Fisheries' scientists and managers participating in a broad range of activities. The data are also shared with other authorized users in the Alaska Department of Fish and Game (ADF&G) and North Pacific Fishery Management Council staff with similar responsibilities. **NMFS Groundfish Tagging Program**: Data is often shared with the NWFSC, the SWFSC, the ADFG, and the Canada DFO. Shared data has been aggregated in a way that confidentiality (of fishing locations) hasn't been breached, and names/addresses are never shared. All publicly available data are aggregated so that no PII/BII information is provided. **EDR**: EDR data is treated as confidential federal fisheries data consistent with NOAA Administrative Order 216-100, and made available only to NMFS and NPFMC scientific and fishery management staff, ADF&G management staff, and contractors/grantees. Prior to gaining access to EDR data records, all individual staff and contractors authorized to use EDR data to perform required work are required to submit signed nondisclosure agreements, which are kept on file at NMFS AKR.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at*: https://survey.psmfc.org*.	
X	Yes, notice is provided by other means.	Specify how: **NORPAC**: Vessel captains/owners receive letters from the permit office explaining the requirements when they apply for permits or individual fishing quota accounts. **NMFS Groundfish Tagging Program:** Notification is provided on the prepaid tag recovery business reply envelopes. **EDR:** Notification is printed on the cover of EDR data collection forms, and on the introductory landing screen of online EDR web forms.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: **NORPAC:** Vessel captains/owners may decline to provide PII/BII verbally or in writing to observers or observer program staff, but participation in a fishery requires consent to carry an observer when directed to by the agency and to provide information requested by the observer. If the individual declines, the vessel will be fishing out of compliance with the regulations and would be in violation. **NMFS Groundfish Tagging Program**: Participation in the tagging program is completely voluntary. In addition, individuals have the opportunity to provide as little data as they wish. For example, a fisherman at times may return a tag with all of the recovery information, and not provide his name, address, or vessel name. **EDR:** Individuals and firms that are subject to EDR reporting of PII/BII may decline to provide the required information by not completing the form. Compliance with EDR and other mandatory recordkeeping and reporting is a condition of participation in federal fisheries under mandated under federal fishery regulations. Failure to comply to EDR reporting requirements may be grounds for NMFS to revoke or deny issuance of federal fisheries permits and licenses required to participate legally in any federal fishery, or to undertake enforcement action by NMFS OLE.
	No, individuals do not have an opportunity to decline to provide	Specify why not:

	PII/BII.	

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: **NORPAC**: Vessel captains/owners may not consent to provide PII/BII (by not providing notification to observers of planned trips, or not allowing observers to board), but participation in a fishery requires consent to carry an observer when directed to by the agency and to provide information requested by the observer. Observer coverage of fisheries is required by regulation and to participate in the fishery, information must be collected for management uses, including stock assessments, and may also be used by law enforcement to investigate and prosecute potential violations or criminal activity. *There are no other uses.* **NMFS Groundfish Tagging Program:** Participation in the tagging program is completely voluntary. In addition, individuals have the opportunity to provide as little data as they wish. For example, a fisherman at times may return a tag with all of the recovery information, and not provide his name, address, or vessel name. Individuals are informed via a disclaimer attached to the tag recovery slips, that information they provide is treated as confidential. *There are no other uses.* **EDR**: Official use and dissemination of EDR data is proscribed under NOAA Administrative Order 216-100 and applicable laws. Apart from a regulated entity's option to be in noncompliance by declining to submit completed EDR forms, individual consent to specific uses of individual EDR data records submitted is not supported.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: **NORPAC**: Fisher information is collected from state or federal agencies where fishers submit the information in order to participate in the fishery. As stated on their permit notices and the AK Regional website, fishers may contact the Alaska Regional Office (AKRO) permitting office by email or telephone to update their contact information. **NMFS Groundfish Tagging Program:** Participants may contact the data steward by email or telephone to update their contact information. Individuals may also request removal of their original submissions of PII/BII if desired. The contact information is on the tag's envelope.

		EDR: NMFS grantee Pacific States Marine Fisheries Commission (PSMFC) acts as the primary data custodian for all EDR data collections, and is responsible for validating data submitted by the regulated entities. Data quality control is achieved by means of programmed data editing routines and third-party validation audit. Potential errors in submitted data records identified by PSMFCs validation procedures are confirmed with the reporting entity prior to revision of official records, and, as stated in the annual reporting reminder, data providers may contact PSMFC at any time to provide corrections voluntarily. Correct contact information is listed in the annual notifications of reporting requirement. All data edits to correct errors reported and/or confirmed by EDR submitters are incorporated and documented by PSMFC staff.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: **NORPAC**: all activity within the Oracle Database that houses the Observer data is recorded and auditable. This is accomplished using the logging and audit tools integrated into the Oracle database **EDR**: access to this data collection is managed by the PSFMC. **Groundfish Tagging Program**: access to this Oracle database is handled using the tools integrated into the Oracle platform.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): **11/20//2017** ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

NORPAC and NMFS Groundfish Tagging Program: The databases are contained within the NOAA4800 system boundaries. They are protected by several layers of controls using a defense in depth approach. For instance, access is authenticated using 2 factor authentication based on CACs and data at rest is encrypted. User accounts are controlled and issued only for documented need. Activity within the databases is logged and can be audited on demand. Whenever possible, data is de-identified prior to sharing it with authorized collaborators.

EDR: NMFS grantee Pacific States Marine Fisheries Commission (PSMFC) acts as the primary data custodian for all EDR data collections. The operational controls, including anonymization, protecting the PII/BII for this database are handled by PSMFC. Individual staff who access the EDR collections have been properly trained on handling files that contain PII/BII. This includes transmitting, sharing, and storing those files in a secure manner, including encryption at rest.

The Oracle Database Administrator confirm that encryption at rest is FIPS 140-2 - compliant.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/NOAA-15, Monitoring of National Marine Fisheries Service Observers; NOAA-16, Alaska Economic Data Reports; NOAA-6, Fishermen's Statistical Data
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: **NORPAC**: 1513-10 Observer Program Files **NMFS Groundfish Tagging Program**: 1200-01 Scientific and Technical Records - Project Case Files **EDR**: 1200-01 Scientific and Technical Records. Data collected in the EDR and Grounfish Tagging program are scientific data of a unique kind and are not subject to expiration. As such, the data is maintained indefinitely, under appropriate security protocols, for use by analysts and is not destroyed.

	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: The BII contained in all of these data collections easily identify commercial fishing entities in the North Pacific. The identity of each commercial entity can then be matched with commercially confidential information (for instance fishing locations or species specific revenue streams).
X	Quantity of PII	Provide explanation: **NORPAC and EDR**: these data collections contain information about all North Pacific commercial fishing entities in the middle to large size business category. The quantity of this information effectively represents the majority of the commercial groundfish and crab fisheries in the North Pacific.
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: All of the data collections are protected for confidentiality based on Magnuson-Stevens Act requirements. Unauthorized disclosure would seriously compromise the sharing of information from the

		commercial fishing sector with the AKFSC.
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation: **EDR**: Given that this data collection is managed by the PSFMC, the agreement between AFSC and PSFMC should be reviewed and updated. This new agreement could result in changes to business processes. **NORPAC**: the "Confidentiality guidelines for Observer Information" memo is almost 9 years old. A review and update of this memo is warranted. This could impact the business processes used to handle NORPAC data in the various scientific programs. **NMFS Groundfish Tagging Program**: additional review of their user account management process is warranted.
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation: **NMFS Groundfish Tagging Program**: we need to enable additional logging for audit purposes at the Oracle database level. This is related to the Groundfish Tagging item in 12.1.
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer	Information Technology Security Officer
Name: Karl Mueller Office: Alaska Fisheries Science Center Phone: 206-526-4022 Email:karl.mueller@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: MUELLER.KARL.ANTHONY.1365890206 Digitally signed by MUELLER.KARL.ANTHONY.1365890206 Date: 2018.03.15 09:57:33 07'00' Date signed:	Name: Catherine Amores Office: NMFS OCIO Phone: 301-427-8871 Email: catherine.amores@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2018.03.27 16:57:21 04'00' Date signed:
Authorizing Official	**Bureau Chief Privacy Officer**
Name: Jeremy Rusin Office: Alaska Fisheries Science Center Phone: 206-526-4621 Email: jeremy.rusin@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: RUSIN.JEREMY.DEWITT.1380624407 Digitally signed by RUSIN.JEREMY.DEWITT.1380624407 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn RUSIN.JEREMY.DEWITT.1380624407 Date: 2018.03.15 17:34:35 -07'00' Date signed:	Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.29 12:06:13 -04'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: Alaska Fisheries Science Center (AKFSC) Network

FISMA Name/ID (if different): NOAA4800

Name of IT System/ Program Owner: NOAA4800 / Ajith Abraham

Name of Information System Security Officer: Karl Mueller

Name of Authorizing Official(s): Jeremy Rusin

Date of Last PIA Compliance Review Board (CRB): 5/12/2017

(This date must be within three (3) years.)

Date of PIA Review: 03/15/2018

Name of Reviewer: Karl Mueller

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: MUELLER.KARL.ANTHONY.1365890206 Digitally signed by MUELLER.KARL.ANTHONY.1365890206 Date: 2018.03.26 13:17:45 -07'00'

Date of Privacy Act (PA) Review: 03/29/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Dig tally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 03 29 09 08 09 04'00'

Date of BCPO Review: 3/29/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer: GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF MARK HYRUM 1514447892
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892
Date 2018 03 29 11 42 30 04'00'

Version Number: 01-2017

U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the NOAA4800 - Alaska Fisheries Science Center (AKFSC) Network

U.S. Department of Commerce Privacy Threshold Analysis

National Oceanic and Atmospheric Administration
NOAA4800 - Alaska Fisheries Science Center (AKFSC) Network

Unique Project Identifier: 006-03-02-00-01-0511-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: The NOAA4800 system consists of a series of Local Area Networks (LANs) connected via a shared Wide Area Network (WAN) connection. The LANs are separated from the WAN by a firewall and router. Via the system identified as NOAA4000, NMFS CIO staff manage the WAN and all of the firewalls except for the Seattle LAN firewall. A common Active Directory, managed by the NMFS EAD staff, binds the LANs into one system. See diagram below.

System Specific Information:

a) NOAA4800 is a General Support System.

b) The primary site of NOAA4800 is Seattle, WA. Additional locations are Newport, OR, Juneau, AK, Anchorage, AK, Kodiak, AK, and Dutch Harbor, AK.

c) NOAA4800 is interconnected with the NMFS LAN (NOAA4000), which provides transport services.

d) The purpose of the NOAA4800 system is to provide information storage and computational resources for NOAA Fisheries scientists.

e) In order to achieve its purpose, NOAA4800 provides connectivity between individual end-user computers to infrastructure devices such as files servers, through networking devices such as firewalls, routers, and switches.

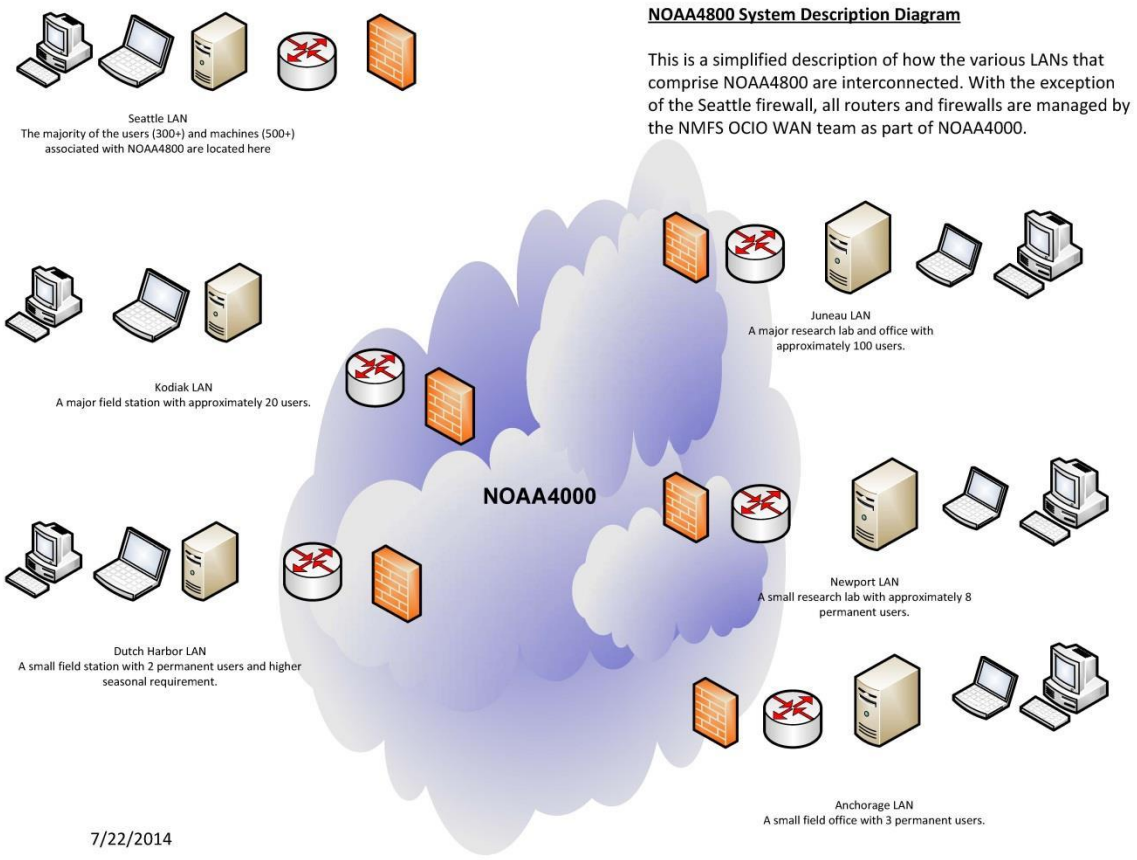
f) NOAA4800 collects, maintains, and uses several types of information, including natural resource data (conservation, marine ecosystems, and mammals), administrative data (budget formulation, budget planning), general workforce management data (number of contractors,

contracting budgets, etc.), and information technology data (help desk, infrastructure, system development, and security.

g) A staff of approximately 500 people composed of biologists, physical scientists, administrative, and support professionals have access to information on the NOAA4800 system.

h) Information is retrieved from servers to desktop and laptop computers via file sharing technologies.

i) Information is transmitted locally via file sharing protocols, and externally via NOAA4000.



Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the

submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

_X__ Companies
_X__ Other business entities

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
_X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

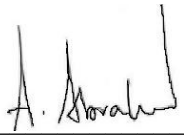
If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): _Ajith Abraham_____

Signature of SO:  Digitally signed by ABRAHAM.AJITH.1365899238 Date: 2018.02.07 08:22:31 -08'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2018.02.13 13:20:28 -05'00' Date: _____

Name of Authorizing Official (AO): _Jeremy Rusin_____

Signature of AO: RUSIN.JEREMY.DEWITT.1380624407 Digitally signed by RUSIN.JEREMY.DEWITT.1380624407 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn RUSIN.JEREMY.DEWITT.1380624407 Date: 2018.02.07 13:35:40 -08'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.02.14 09:16:08 -05'00' Date: _____

David Layton - NOAA Federal

From:	David Layton NOAA Federal
Sent:	Friday, March 30, 2018 7:23 PM
To:	Toland, Michael
Cc:	Ed Kearns NOAA Federal; Peter Grimm; Allison Soussi Tanani; Jeff de La Beaujardiere; David Herring NOAA Federal; Mike Gerber NOAA Federal; Kenneth Casey; Michael Chapman NOAA Affiliate; Laura Oremland NOAA Federal; John MCLaughlin NOAA Federal; Rich Baldwin NOAA Federal; Steve Ansari NOAA Federal; Jennifer Jencks NOAA Federal; Eric Kihn NOAA Federal; Mark Graff NOAA Federal; Genevieve Contey NOAA Federal; Adam Stephens NOAA Federal; Sameka McNeil NOAA Federal; Dennis Morgan; Rob Swisher; Zachary Goldstein
Subject:	Re: DATA CALL: Open Government Plan 5.0, due date timeline attached
Attachments:	Consolidated NOAA Input for 2018 DOC Open Govt Plan Update, 3 30 18.docx

Mike:

As requested and on behalf of Ed Kearns (as the NOAA OGSL), attached is NOAA's input for the 2018 update of the DOC Open Government Plan.

Thanks to the many folks across NOAA (cc'ed) who contributed content and provided comments.

Feel free to contact me with any questions, and looking forward to the next steps in the DOC vetting process.

Regards,
David Layton
NOAA Chief Enterprise Architect

On Tue, Jan 16, 2018 at 8:11 AM, Toland, Michael (Federal) <MToland@doc.gov> wrote:

> Dear OGSLs:
>
> We are the time of year where the work on the next iteration of our Open Government Plan, version 5.0, must begin. The process will culminate in the posting of our final approved Plan prior to September 14, 2018. While it may seem as though we have a lot of time between the start of the data call to the posting of the Plan on our web site, there are many activities that must take place between now and September 15 (please see the attached Open Government (OG) Plan timeline).
>
> Deliverable for this initial call:
>
> - BOU Draft OG Plan (see September 2016 Plan for example)

- **Due March 30, 2018**. No extensions will be granted because of the tight consolidation and review schedules involved.

- We will be sending to you in separate emails the draft plans that you submitted for version 4.5 last year. These may be helpful for drafting your 5.0 OG Plan.

Additionally, in 2016, OMB, through OMB memorandum M-16-16 (see attached memo), expanded and added several areas to the OG Plan to which we are asking you to pay specific attention:

- Open Data
- Proactive Disclosures
- Privacy
- Websites
- Open Innovation Methods
- Access to Scientific data and Publications
- Open Source Software
- Spending Information

We have a OGSL teleconference meeting scheduled for this afternoon. I plan to reschedule to next Tuesday, January 23, so that you have more time to review the deliverables schedule and be prepared to ask questions. More information about the meeting and data call requirements will follow, as necessary. We will also be able to discuss the Plan and progress on drafting it at our next OGSL Face-to-Face meeting scheduled on February 22, 2018.

Please feel free to contact me with any questions you may have or if you need additional information.

Regards,

Mike

Michael J. Toland, Ph.D.

Deputy Chief FOIA Officer,

Departmental FOIA Public Liaison Officer,

Departmental Privacy Act Officer, and

Deputy Director FOIA/Privacy Act Operations

U.S. Department of Commerce

Office of Privacy and Open Government

Office: (202) 482-3842

Email: mtoland@doc.gov

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, April 2, 2018 11:02 AM
To:	Peyton Robertson NOAA Federal
Subject:	Re: Slides
Attachments:	FOIA Privacy and DLP Overview Final.pptx; NOAA FOIA Litigation as of 03.21.18.docx

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Mon, Apr 2, 2018 at 11:00 AM, Peyton Robertson NOAA Federal <peyton.robertson@noaa.gov> wrote:

> Hi Mark I didn't get the slides.....
>
> Thx
>
> Sent from my iPhone

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

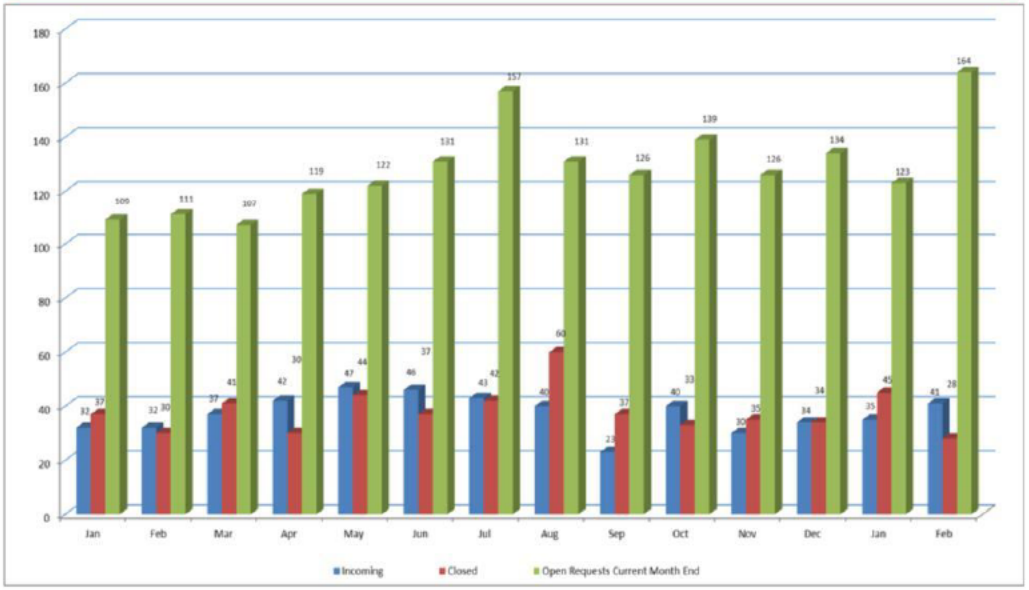
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 21, 2018

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, April 2, 2018 10:45 AM
To:	Shelley Moeller NOAA Federal; payton.robertson@noaa.gov; Michelle Mainelli NOAA Federal; Kenneth Graham NOAA Federal
Subject:	Presentation materials
Attachments:	FOIA Privacy and DLP Overview Final.pptx; NOAA FOIA Litigation as of 03.21.18.docx

Attached.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

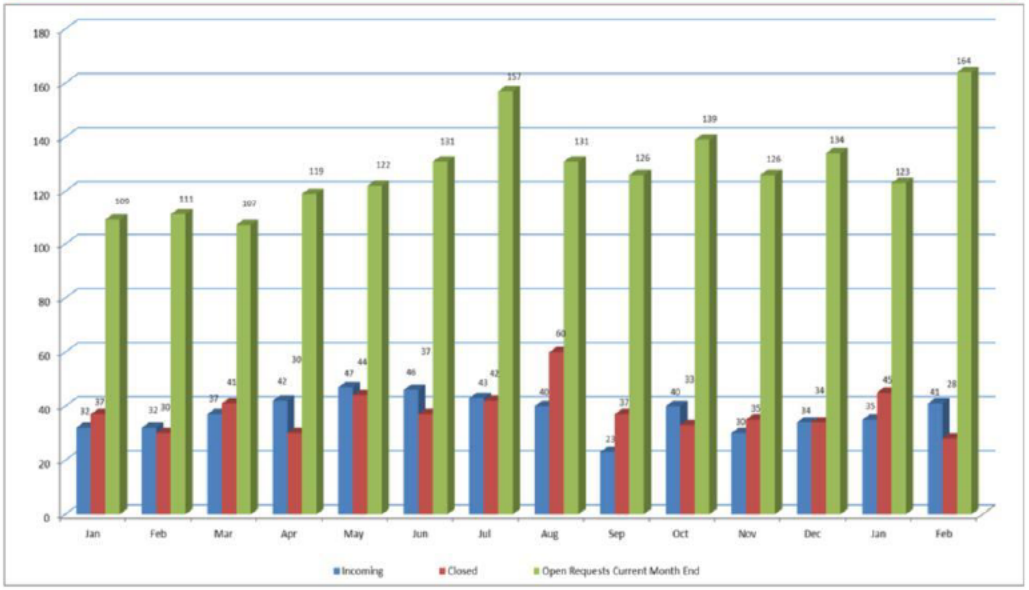
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 21, 2018

[redacted]

(b)(5)

Anthony Vandegrift - NOAA Federal

From:	Anthony Vandegrift NOAA Federal
Sent:	Tuesday, April 3, 2018 11:23 AM
To:	Sarah Brabson NOAA Federal
Cc:	Beckie Koonge NOAA Federal; Zachary Goldstein; Mark Graff NOAA Federal; Andrew Browne NOAA Federal; Ben Kyger NOAA Federal; Ann Rivers
Subject:	Re: NOAA8865 Tsunami Warning System Privacy Threshold Analysis
Attachments:	NOAA8865 PTA 03202018_av2.pdf

All,
Still awaiting signatures from Zach and Beckie before Mark can review and sign.
Please review and sign at your earliest convenience.

I've converted it to PDF as it seems to be faster to sign PDFs.

Thanks,
Anthony

On Tue, Mar 20, 2018 at 2:50 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Thanks, Anthony. Zach or Ann, please return to me for Mark's signature.
>
> This will be our last system that was lacking a PIA (which Mark is reviewing now).
>
> thx Sarah
>
> Zach
>
> On Tue, Mar 20, 2018 at 2:38 PM, Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov> wrote:
>
> > All,
> > Attached is the PTA for NOAA8865. It was identified earlier this year that previous PIA/PTAs were unsatisfactory as they failed to capture information about employee information stored on the IS as well as point of contact information from Seismic network points of contacts and emergency managers that we maintain email, phone, and fax information for.
> > Please review and sign at your convenience and reattach to this email string until the relevent parties have signed:
> > Beckie Koonge or Andrew Browne, NWS ITSO
> > Zachery Goldstein, NOAA8865 AO
> > Mark Graff, Bureau Privacy Officer
> >
> > CCed is Ben Kyger, NOAA8865 SO for his visibility.
> >
> >
> >
> > **Anthony Vandegrift**

Information System Security Officer
National Tsunami Warning Center
NOAA/NWS/NCEP/NTWS
910 S Felton Street
Palmer, AK 99645
Phone: 907-861-4225
Govt. Cel (b)(6)
anthony.vandegrift@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Anthony Vandegrift
Information System Security Officer
National Tsunami Warning System
NOAA/NWS/NCEP/NTWS
910 S Felton Street
Palmer, AK 99645
Phone: 907-861-4225
Govt. Cel (b)(6)
anthony.vandegrift@noaa.gov

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, April 2, 2018 11:04 AM
To:	Clay Porch NOAA Federal
Cc:	Maria Gonzalez NOAA Federal
Subject:	Re: Notification: FOIA Briefing Mark Graff @ Mon Apr 2, 2018 10:45am 11:15am (EDT) (clay.porch@noaa.gov)
Attachments:	NOAA FOIA Litigation as of 03.21.18.docx; FOIA Privacy and DLP Overview Final.pptx

Here you go.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Mon, Apr 2, 2018 at 11:02 AM, Clay Porch NOAA Federal <clay.porch@noaa.gov> wrote:

I am on the call, but I did not receive the presentation.

Clay

On Mon, Apr 2, 2018 at 10:34 AM, Google Calendar <calendar notification@google.com> wrote:

FOIA Briefing - Mark Graff more details »

Clay,

Please use the above # to call into this meeting, scheduled at 10:45am. Sorry sent the wrong date..

When Mon Apr 2, 2018 10:45am – 11:15am Eastern Time

Where Conference call in (b)(6) Pass code (b)(6) map)

Calendar clay.porch@noaa.gov

Who
- maria.j.gonzalez@noaa.gov organizer
- Mark Graff - NOAA Federal
- clay.porch@noaa.gov

Going? Yes - Maybe - No more options »

Invitation from Google Calendar

Clay E. Porch, Ph.D.
Director, Sustainable Fisheries Division
Southeast Fisheries Science Center

FOIA, Privacy, and Data Loss Prevention Overview

Prepared by Mark H. Graff
NOAA FOIA Officer/Bureau Chief
Privacy Officer
OCIO/GPD
mark.graff@noaa.gov; (301)-628-5658

NOAA FOIA Program

Background and NOAA Processing

- FOIA provides that any person has a right to obtain access to agency records, except those protected from public disclosure by one of nine FOIA exemptions or by one of three special law enforcement record exclusions. This right is judicially enforceable, and attorneys fees can be assessed if the Plaintiff substantially prevails.

- Since 2013, NOAA has processed requests through FOIAOnline, and historically, NOAA has routinely received, processed, and litigated more requests than any other Bureau in the Department. NOAA processes, on average, 2.9 times more requests than the average DOC Bureau.

NOAA FOIA Program

NOAA Leads Department in Production

NOAA processed 495 FOIA requests in FY17, more than any of the other 13 Bureaus with FOIA processing responsibilities.

NOAA has led the Department's Best Practices Working Group, Proactive Disclosures among the Bureaus, and coordinated the FOIA regulatory revisions with DOC General Counsel and DOC Office of Privacy and Open Government.

NOAA FOIA Program (Cont'd)

Structure and Efforts

- NOAA has a decentralized FOIA structure, with Line Offices searching for, and processing, records they locate. The records are centrally released through FOIAOnline.

- NOAA's FOIA training practices, FOIA Public Outreach Roundtables, and FOIA Legal Experts Guidance are all lead-Bureau activities within DOC, and referenced in the pending Chief FOIA Officer's Report prepared for Congress.

NOAA FOIA Program Backlog and Litigation

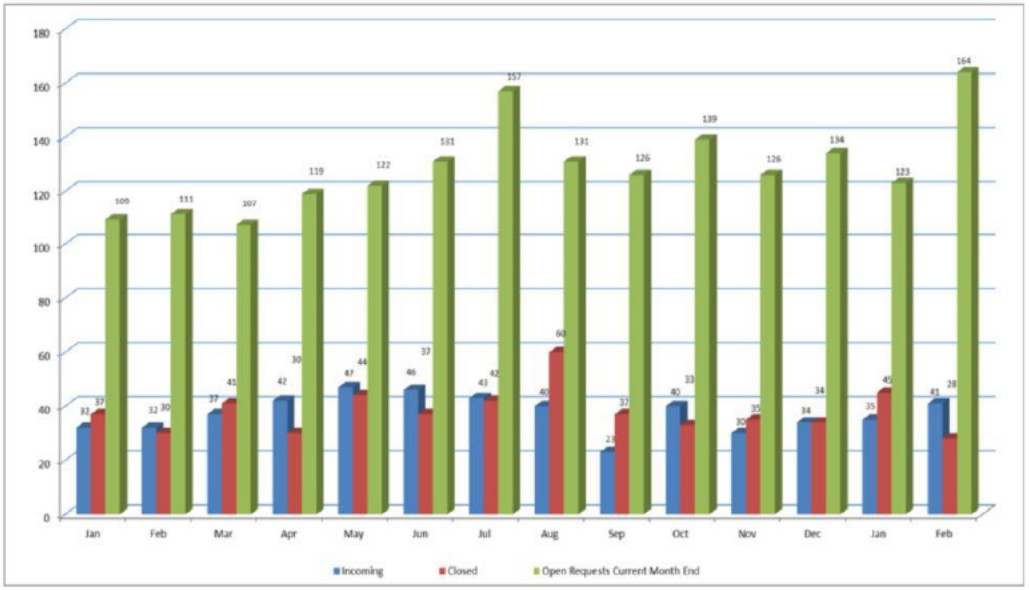
- NOAA has focused keenly on backlog reduction since the backlog peaked in 2014 at 209 requests. The current backlog, at 91 requests, represents a 56% reduction from that point.

- Despite a relatively stable, low backlog, NOAA's (and the Department's) FOIA litigation burden has spiked recently. The average filing rate for FY18 is currently 550% higher than the rate from 2013-2016. This is in line with other scientific and environmental agencies, such as EPA and DOI, who have seen 311% and 600% increases over the last FY respectively.

Background Data
FOIA Processing

Organization	Open Requests Previous Month End	Incoming Requests	Closed Requests	Open Requests Current Month End	Backlog 21-120 days	Backlog 121-364 days	Backlog 365 or more days	Total Backlog
AGO	10	6	2	19	5	1	1	7
CAO	6	1	1	6	3	1	0	4
CFO	0	0	0	0	0	0	0	0
CIO	0	1	0	1	0	0	0	0
CIO/FOIA	2	7	6	6	1	0	0	1
GC	4	0	1	2	1	1	0	2
IA	0	0	0	0	0	0	0	0
LA	1	0	0	2	1	0	0	1
NESDIS	1	1	1	1	0	0	0	0
NMFS	54	16	13	71	15	20	3	38
NOS	10	2	2	15	8	0	0	8
NWS	5	3	1	8	3	2	0	5
OAR	15	1	1	15	9	2	0	11
OMAO	1	1	0	3	1	0	0	1
OC	3	0	0	3	1	2	0	3
PPI	0	0	0	0	0	0	0	0
USEC	6	0	0	6	6	0	0	6
WFMO	5	2	0	6	4	0	0	4
NOAA Totals	**123**	**41**	**28**	**164**	**58**	**29**	**4**	**91**

Background Data
FOIA Processing



NOAA Privacy Program

Privacy Governance

- Within the last 2 years, NOAA is following Governance within the Department related to Privacy, including:
  - Execution of the NOAA's first Bureau-wide Privacy Policy.
  - Implementation of the Data Loss Prevention Solution.
  - Implementation of the Unmanned Aircraft Privacy Policy, and publication of the UAS System of Records Notice for Department-wide use.

NOAA Privacy Program

A-130 and E-Government Act Compliance

- On May 30, 2017, NOAA issued its first Bureau-wide Privacy policy, becoming one of the leading Bureaus to address issues such as cookie use, third party social media links, and mobile applications in their policy.

- NOAA has no pending allegations of a Privacy Act Violation or challenges to the collection, use, or sharing of PII.

- NOAA Currently has 88 Systems, of which, 57 currently collect Personally Identifiable Information (PII). As such, those systems require a Privacy risk review approved by DOC in the form of a Privacy Impact Assessment (PIA). When Sensitive PII is present, additional controls are necessary in this review.

NOAA Data Loss Prevention (DLP)

DLP Rollout

NOAA is one of the DOC Bureaus that has independently rolled out a Data Loss Prevention (DLP) Solution to actively prevent Privacy Incidents.

NOAA has continued to roll out the DLP Solution to mitigate SSN transmission and loss. One way to mitigate SSN transmission is to reduce SSN collection in forms. NOAA is leading the DOC initiative to remove SSNs from the internal use of the forms, including the SF-182.

Unmanned Aircraft Systems System of Records Notice

- NOAA issued the Unmanned Aircraft Privacy Policy, and submitted the UAS System of Records Notice for Department-wide use

  -This was largely driven by the need for the ability to track, in real time, storm damage assessment and incident response using UAS technology.

  -The new A-130 Expedited OMB approval process was sought by DOC to address rising issues highlighted by the 2017 hurricane season.

Contacts

Zachary Goldstein, NOAA CIO: 301-713-9600
zachary.goldstein@noaa.gov

Rob Swisher, Director, Governance and Portfolio Division: 301-628-5755
robert.swisher@noaa.gov

Mark Graff, FOIA Officer/Bureau Chief Privacy Officer: 301-628-5658
mark.graff@noaa.gov

Background Data NOAA Systems of Record Notices

NOAA-1, Applicants for the NOAA Corps
NOAA-3, NOAA Corps Officer Official Personnel Folders
NOAA-5, Fisheries Law Enforcement Case Files
NOAA-6, Fishermen's Statistical Data
NOAA-10, NOAA Diving Program File
NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission
NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Authorizations Applicants
NOAA-13, Personnel, Payroll, Travel, and Attendance Records of the Regional Fishery Management Councils
NOAA-14, Dr. Nancy Foster Scholarship Program; Office of Education, Educational Partnership Program (EPP); Ernest F. Hollings Undergraduate Scholarship Program and National Marine Fisheries Service Recruitment, Training, and Research Program
NOAA-15, Monitoring of National Marine Fisheries Service Observers
NOAA-16, Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska
NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
NOAA-20, Search and Rescue Satellite Aided Tracking (SARSAT) 406 MHz Emergency Beacon Registration Database
NOAA-21, Financial Services Division
NOAA-22, NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)
NOAA-23, Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

Background Data DOC Systems of Record Notices

DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons
DEPT-2, Accounts Receivable
DEPT-3, Conflict of Interest Records, Appointed Officials
DEPT-4, Congressional Files
DEPT-5, Freedom of Information Act and Privacy Act Request Records
DEPT-6, Visitor Logs and Permits for Facilities Under Department Control
DEPT-7, Employee Accident Reports
DEPT-8, Employee Applications for Motor Vehicle Operator's Card
DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons
DEPT-10, Executive Correspondence Files
DEPT-11, Candidates for Membership, Members, and Former Members of Department of Commerce Advisory Committees
DEPT-12, OIG Investigative Records
DEPT-14, Litigation, Claims, and Administrative Proceeding Records
DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
DEPT-25, Access Control and Identity Management System
DEPT-27, Investigation and Threat Management Records
DEPT-29, Unmanned Aircraft Systems

DO NOT RELEASE

NOAA'S ACTIVE FOIA LITIGATION AS OF MARCH 21, 2018

[redacted]

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Tuesday, April 3, 2018 12:32 PM
To:	Gioffre, Kathy (Federal); CPO; Toland, Michael; Gitelman, Steve (Contractor)
Cc:	Mark Graff NOAA Federal; John D. Parker; Russell Worman; John Kaperick
Subject:	NOAA6702 revised PTA and PIA per CRB
Attachments:	NOAA6702_PIA_032918 per CRB.pdf; NOAA6702(20180329Final_NOAA response.docx; NOAA6702 PTA 032918 per CRB.pdf

All, attached are the minutes with our responses, the revised PTA and revised PIA.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Privacy Impact Assessment (PIA) Compliance Review Board (CRB) Meeting Minutes
NOAA Office of Response and Restoration Products System (ORRPS) (NOAA6702)
March 29, 2018

Attendees:

Privacy Team
Catrina Purvis
Kathy Gioffre
Steve Gitelman
Dorrie Ferguson
Eric Cline (OCIO)

NOAA
Mark Graff
Sarah Brabson
John Kaperick
Marie Murphy
Russell Worman
John Parker

Results/Conclusion:

Upon review of NOAA Office of Response and Restoration Products System (ORRPS) (NOAA6702), Senior Agency Official for Privacy (SAOP) provides concurrence for renewal of the Authorization to Operate (ATO) effective today upon receipt of revised PIA with inclusion of System of Record Notice (SORN). The Office of the Chief Information Officer (OCIO) has provided concurrence on the NIST 853 Appendix J privacy controls.

Action Items:

Version Number: 01-2015

U.S. Department of Commerce

National Oceanic and Atmospheric Administration (NOAA)
National Ocean Services (NOS)
Office of Response and Restoration (OR&R)

Privacy Impact Assessment
For the
Office of Response and Restoration Products System (ORRPS)
NOAA6702

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Oceanic and Atmospheric Administration (NOAA)
Office of Response and Restoration Products System (ORRPS)

Unique Project Identifier: NOAA6702 (OMB Exhibit 300 ID Number: 006-000351103 00-48-02-00-02-00)

Introduction: System Description

The National Oceanic and Atmospheric Administration (NOAA), National Ocean Service (NOS), Office of Response and Restoration (OR&R) is the focal point in NOAA for preventing, planning for, and responding to oil spills, releases of hazardous substances, and hazardous waste sites in coastal environments and restoring affected resources. OR&R protects and restores coastal resources through the application of science and technology. On behalf of the public, OR&R addresses environmental threats from catastrophic emergencies such as the oil spills of the ship, Exxon Valdez or the oil drilling rig of the Deep Water Horizon; chronic releases from contaminated sediments such as the Hudson River Superfund site; and vessel groundings in sanctuaries such as coral reefs in the Florida Keys. By working in partnerships, OR&R empowers communities and decision makers to be coastal stewards by transferring the results of its experience through training, guidance, and decision-making tools that emphasize actions to take to improve coastal health.

NOS OR&R operates the Office of Response and Restoration Products System (ORRPS), NOAA6702. ORRPS is comprised of products developed and published by the Divisions within OR&R - Assessment and Restoration Division (ARD), the Emergency Response Division (ERD), Disaster Response Center (DRC) and Marine Debris Program (MDP). The ORRPS incorporates the product systems from these divisions. ORRPS is currently located in the Amazon Web Services (AWS) East/West FedRAMP cloud. The system is a cloud based solution operating the Environmental Response Management Application (ERMA®) subsystem, the Data Integration, Visualization, Exploration, and Reporting (DIVER) subsystem, the Marine Debris website, NOAA Response Asset Directory (NRAD) website, NOAA's Damage Assessment Remediation and Restoration Program (DARRP) website, Response and Restoration website, and the OR&R Intranet website. NOAA6702 has user identification requirements and applications that support assessment and restoration of natural resources, which may require the collection of PII or BII.

(a) a general description of the information in the system

NOAA6702, ORRPS contains Personally Identifiable Information (PII) that consists of the information needed to establish accounts for non-public users. The PII is non-sensitive in that it contains information provided by the user to obtain an account that includes the user's name, email address, and telephone number and is provided to the account manager through an email request.

NOAA6702 ORRPS contains Business Identifiable Information (BII) that is primarily obtained during an event, such as an oil spill, that is often part of the litigation, and not released to the public until it has completed the OR&R process to validate the information and review the sensitivity of the information, which may require the coordination with Office of General Counsel. Within the Office of General Counsel, the Natural Resources Section provides legal advice to the National Marine Fisheries Service and the National Ocean Service. The purpose of the DARRP Program is to seek restoration from responsible parties for injuries caused to our Nation's natural resources by releases of hazardous substances from thousands of waste sites, numerous oil spills, and physical impacts (e.g., vessel groundings) to unique resources located in National Marine Sanctuaries. Sharing of any PII/BII data with an outside entity would be pursuant a court order.

For Deepwater Horizon (DWH) OR&R provided a separate site from (2012-2016) for BP to access the information collected by DIVER/ERMA to do their own analysis in preparation for the court action. The datasets (9,000) from NOAA, federal, state, and Non-Governmental Organization (NGO) partners to support these tasks to respond to environmental incidents had restricted access, which required an ERMA/DIVER account to view. In the case of Deepwater Horizon (DWH), the DIVER and ERMA applications maintained a separate database for the information generated during this event. The data has been migrated to NOAA's National Centers for Environmental Information (NCEI) in accordance with OR&R and NOAA's data management and data stewardship policies. NOAA's ERMA and DIVER applications will continue to make NRDA (and other environmental data) available for mapping, query and download from these applications, and will build linkages to the archived data packages for reference and citation.

ORRPS supports Natural Resource Damage Assessment and Restoration cases and projects.

Environmental Response Management Application (ERMA):

ERMA is an online mapping tool designed to aid in spill preparedness and planning, assist in coordinating emergency response efforts and situational awareness for human and natural disasters and support the Natural Resource Damage Assessment (NRDA) process.

The case data may contain BII (oil spill evidence identifying the source of the spill) and PII (contact information for those requesting an account).

Data Integration, Visualization, Exploration, and Reporting (DIVER):
The National DIVER Portal is a login website that encompasses the DIVER Data Warehouse, which contains environmental data, activity data, and restoration project data.

The case data, when a case is active, may contain BII (oil spill evidence identifying the source of the spill; project restoration identifying information) and PII (contact information for those who collected the information and are accessing information).

(b) any information sharing conducted by the system

ERMA:

Homeland Security Infrastructure Program (HSIP)

HSIP map services or shapefile data come from the HSIP Gold. "It is a compilation of over 560 geospatial datasets, characterizing domestic infrastructure and base map features, which have been assembled from a variety of Federal agencies, commercial vendors, and State mission partners. HSIP Gold 2015, in its entirety, is unclassified; it is subject to the handling and distribution rules for "Unclassified For Official Use Only" due to licensing and sharing restrictions set forth by the data source entities.

Case data: In the case of Deepwater Horizon (DWH), the information collected was later used for litigation support. This information, which may include BII, is shared with other agencies, viewable from ERMA when a case is active. While the case data is archived at NCEI, historical data is still viewable by the public.

Ship positions: Nationwide Automatic Identification System (NAIS). Source Coast Guard

In ERMA, the user can search the Nationwide Automatic Identification System (NAIS) for an Automatic Identification System (AIS) enabled ship by name or MMSI number to determine the last known or reported location of the ship.

DIVER:

Case data: In the case of Deepwater Horizon (DWH), and other cases, information collected, which may include BII, is used for litigation support. This information is shared with other agencies, viewable from DIVER when a case is active. While the case data is archived at NCEI, historical data is still viewable by the public.

If there is a security or privacy breach, information will be shared within the bureau, with the Department and with other federal agencies as applicable.

(c) a citation of the legal authority to collect PII and/or BII

- U.S. DOC/NOAA NRDA Regulations (OPA) NRDA Regulations 15 C.F.R. 990; Oil Pollution Act of 1990. Establishes legal authorities for NRDA
- U.S. DOC/NOAA Guidance Documents
    - Preassessment Phase: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996
    - Injury Assessment: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996
    - Specifications for Use of NRDAM/CME Version 2.4 to Generate Compensation Formulas: Guidance Document for Natural Resource Damage Assessment Under the

Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996
    - Primary Restoration: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment and Restoration Program, NOAA, August 1996
    - Restoration Planning: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment and Restoration Program, NOAA, August 1996.
    - Other relevant Guidance Documents may be accessed at the NOAA DARRP Website.
- Authorities from NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.
- Authorities from DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
- Authorities from DEPT-18: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system

FIPS 199 Security Categorization: **Moderate** (M, M, M)

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

NOAA6702 addresses OR&R applications, such as ERMA and DIVER applications in its boundary.

__ _ This is a new information system.

____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

___X__ This is an existing system for which a Privacy Impact Assessment had not been done, and for which there are privacy risks.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):NOAA6702 underwent initial Assessment and Authorization (A&A) in 2017 and after ISSO/ITSO review of the system data types -and documentation it					

was determined that the system required a PIA.

____ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

NOAA6702 contains **PII** that is work-related and system administration information. **BII** is contained in the case data collected for a NRDA incident, when a case is active.
NOAA6702 data is encrypted at rest and in transit.
In DIVER, descriptive fields such as the project's name, phase, location, type (i.e., planning or project), and the activity under which the project is being undertaken are associated with the Project ID (BII information is data contained within the project, not the Project/File ID).
The DIVER application also imports data from an external DOI application. The connection to the DOI application encrypts the data while in transit.

2.1 Indicate what personally identifiable information (PII) / business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): In NOAA6702, descriptive fields such as the project's name, phase, location, type (i.e., planning or project), and the activity under which the project is being undertaken are associated with the Project or File/Case ID.					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	

c. Work Address		f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	
g. Other system administration/audit data (specify): User ID is logged in NOAA6702 (ERMA and DIVER) when files are uploaded. Displayed as user name on the screen.					

Other Information (specify)
NOAA6702 ORRPS supports Natural Resource Damage Assessment and Restoration cases and projects. ERMA is an online mapping tool designed to aid in spill preparedness and planning, assist in coordinating emergency response efforts and situational awareness for human and natural disasters and support the Natural Resource Damage Assessment (NRDA) process. The case data, when a case is active, may contain BII (oil spill evidence identifying the source of the spill) and PII (contact information for those who collected the information).
The National DIVER Portal is a login website that encompasses the DIVER Data Warehouse, which contains environmental data, activity data, and restoration project data. The case data, when a case is active, may contain BII (oil spill evidence identifying the source of the spill; project restoration identifying information) and PII (contact information for account users, including those who collected the information).

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email	X		
Other (specify): Name, phone number, and email from account request form from users that require an account. Public users do not require an account.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify Case data: NRDA activities					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	

Third Party Website or Application			
Other (specify):			

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

User name, phone number, and work email addresses are collected during the account request process. The username given is the root of the user's email address, and the email address must be a work email account. Email address is used for correspondence about planned system outages, etc., and for password reset requests. This PII is collected from federal employees and contractors, and academia (researchers who are participating in data collection and analysis for response and or restoration efforts) users who request an account on the system and are approved for a valid business need.

Administrative information is used to designate the role for access to information and the decision to allow modification to the information based on the role assigned.

Last successful login time is used to gauge automatic account deactivation.

Information sharing is an initiative to provide information, which may include PII/BII, for organizations that need it for litigation actions pursuant a court order. Interagency data flows: USCG and NOAA HSPO among others use DIVER/ERMA for responses to spills and responses. However, there is currently no such data in the system; projects that were completed are archived in NCEI.

OR&R provides information requested by other agencies from information collected during NRDA in support of their missions. BII collected is based on the target of the assessment and response activities and how the damage is litigated.

ERMA is used by the NOAA Homeland Security Program Office (HSPO) as a tool to provide their Common Operating Picture. HSPO uses the maps and data layer information from ERMA for agency situational awareness and response related to an event impacting NOAA, People, Mission and Infrastructure.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X*		X
DOC bureaus	X*		X
Federal agencies	X*		X
State, local, tribal gov't agencies			X
Public			
Private sector	X**		
Foreign governments	X**		
Foreign entities			
Other (specify):			

*In case of breach. **The PII/BII in the system will not be shared except pursuant to a court order.

	The PII and BII will not be shared.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: For active case data that is held locally in ERMA, Access Control, Encryption, Virtual Private Network, Amazon Web Services (AWS) Cloud Environment, Homeland Security Infrastructure Program (HSIP) data comes from a Department of Homeland Security (DHS) mapped server (mapping system similar to ERMA). Receives ship location information from Nationwide Automatic Identification System (NAIS) from the Coast Guard's secure server. Encryption of data in transit is used for system connections (PII/BII information). **(Response) Specific**: Department of interior (DOI) provides DIVER with public data that it collects for the Response. DOI maintains the administrative record in their websites, but DIVER uses the data from DOI after it is transformed into the DIVER schema and then provides the data to view in the DIVER application. DOI information provides information specific to the Response case data that DOI collected. The DIVER Explorer application integrates data from multiple sources. Most data are ingested directly through the DIVER application. One exception to that is the DOI Response Database. DOI provides a complete dump of their Response-related assessment data warehouse and the DIVER team manually integrates this into the warehouse. The DIVER connects to a DOI database using an Extract, Transform, Load (ETL) process that reformats the data to conform to the DIVER schema, using encryption in transit to pull sample and visual observation data. NOAA6702 doesn't share data or directly connect the systems. . The DOI dataset includes URL links to associated files and photographs which are made available through the DIVER Explorer user interface. These associated files are not generally publicly available. However, they are surfaced through DIVER Explorer to authorized users of the DIVER application. This is facilitated by a trust relationship between the DOI Response Database and NOAA DIVER application.

	The DIVER application data flow is managed by data managers on a workspace and record level basis.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://oceanservice.noaa.gov/privacy.html https://response.restoration.noaa.gov/privacy-act-statement https://portal.diver.orr.noaa.gov/web/national/request-user-account https://erma.noaa.gov/ERMA/RequestAccount?sitename=atlantic .	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the user account sites.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Users can choose to not request an account. Organizations provide BII based on an agreement with the agency in place (ERMA currently has an informal agreement with USGS; a formal agreement is in process)
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to	Specify how: Email address, phone number, and name are required

	consent to particular uses of their PII/BII.	for account maintenance and communication. Individuals cannot create an account without consent to these uses. Individuals may not consent, in the form of an incomplete account request, but this results in an account not being created. The draft USCG agreement for NAIS data does not specify BII, but does say that sensitive information is for official use only and should be protected as such. The NAIS data is restricted from public access which is limited to federal government users. Other BII collected, such as in response to a spill, is done under one of the citations in paragraph c.) such as the Oil Pollution Act of 1990 where a responsible party agrees to provide data to the federal gov't.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users reach account administrators through the "Contact" link in the site footer. Email
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: All account modification issues are logged and monitored
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 31 March 2017 This is a new system. The A&A package was approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.

	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Names of account holders and their respective phone numbers and email addresses are accessible only through a role-based security system where only account administrators of ERMA and DIVER can view.

The ERMA and DIVER software is designed to restrict access to data based on specifically granted permissions. These permissions may be granted at several levels:

- Restricted by source system IP address in combination with an authentication "token"/key.
- Restricted to authenticated users with a specific level of granted access.
- ERMA and DIVER designate most data with specific sets (datasets) of "contexts", using an event name, privilege level, and visibility level. In order to view a resource, users must be granted access to all three applicable contexts for a resource. For DIVER it's a workspace, privilege level, and sharing status.
- Low-level access to data (the database and related files) is restricted to the core application, and is not accessible from outside of the application, except by system administrators.
- All underlying system files are encrypted, ensuring that drives taken out of service are not accessible.
- Other system resource data are accessible to only ERMA designated system administrators; and System Administrators, Program Administrators, and Data Managers for DIVER.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission.

	DEPT-13, Investigative and Security Records. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the federal government. The underlying paper records relating to employees are covered by GRS 1, Civilian Personnel Records. In accordance with GRS 20, item 3, electronic versions of records scheduled for disposal under other records schedules may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later. Guidance for these records in the NOAA Records Schedules refers disposition to GRS 20. NOAA Records Schedules Chapter 100 General Chapter 200 Administrative and Housekeeping Chapter 1600 National Ocean Service (NOS) Functional Files describes records created and maintained in the National Ocean Service (NOS) on the ocean and coastal zone management services and information products that support national needs arising from increasing uses and opportunities of the oceans and estuaries. 1605 Office of Response and Restoration Records relating to the prevention and mitigation of risks to coastal resources and restoration of habitats from oil and hazardous materials; support for the cleanup of spills occurring in U.S. coastal and navigable waters; training and outreach programs; and software for spill responders and planners and coastal management decision making. 1605-01 - Incident Response and Waste Site Financial Records. 1605-02 - Query Manager Databases (QM). 1605-03 - Coastal Resource Coordinator Records. 1605-04 - HAZMAT Response Records. 1605-05 - Electronic Copies-All Offices. 1605-06 - Defunct.

	1605-07 Defunct. 1605-08 Defunct. 1605-09 - NRDA Administration Record Files - Pre Settlement. 1605-10 - NRDA Pre-Settlement Case Files. 1605-11 - NRDA Pre-Settlement Working Files. 1605-12 - Infant and Orphan Case Files. 1605-13 - Multi-case Evidence Tracking Records. 1605-14 - Cost Accounting and Documentation Files. 1605-15 - Rulemaking Administrative Record. 1605-16 - Rulemaking Working Files consolidated into 1605-15. • U.S. DOC/NOAA NRDA Regulations (OPA) NRDA Regulations 15 C.F.R. 990 • U.S. DOC/NOAA Guidance Documents • Preassessment Phase: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996 • Injury Assessment: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996 • Specifications for Use of NRDAM/CME Version 2.4 to Generate Compensation Formulas: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment Remediation and Restoration Program, NOAA, August 1996 • Primary Restoration: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment and Restoration Program, NOAA, August 1996 • Restoration Planning: Guidance Document for Natural Resource Damage Assessment Under the Oil Pollution Act of 1990, the Damage Assessment and Restoration Program, NOAA, August 1996. • Other relevant Guidance Documents may be accessed at the NOAA DARRP Website.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule. The information is retained by ERMA and DIVER as part of the legal process for supporting litigation actions.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing	X	Deleting	
Other (specify): Information is not deleted, but all information is archived or made inactive. Hard drives containing information that are no longer serviceable are overwritten and degaussed.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

ERMA and DIVER designate most data with specific sets (refers to datasets and user roles of access (event name, privilege level, and visibility level) of "contexts", using an event name, privilege level, and visibility level. In order to view a resource, users must be granted access to all three applicable contexts for a resource. For DIVER it's a workspace, privilege level, and sharing status.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Only name, phone number, and work email are recorded for accounts requiring login access.
X	Quantity of PII	Provide explanation: Only name, phone number, and work email are recorded for Government, State, Trustees, Contractors, and Academia accounts requiring login access. These accounts number less than 500.
X	Data Field Sensitivity	Provide explanation: User name, phone number, and email address are provided by the user to obtain an account voluntarily. Primarily used for account management. The information is non-sensitive PII.

X	Context of Use	Provide explanation: Only name, phone number, and work email are recorded for account user ID. Used to contact user for account set up and notifications for outages.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Only account administrators can see the PII. Concept of least privilege; secure network and database; encrypted storage and transmission. Information is stored in AWS as a FedRAMP approved site.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Addition of privacy act statements.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner (Acting) Name: Nancy Wallace Office: NOAA/NOS/ OR&R Phone: (240)-533-0412 Email: nancy.wallace@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: WALLACE.NANCY.E.1382920305 Digitally signed by WALLACE.NANCY.E.1382920305 Date: 2018.03.13 11:53:19 -04'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: NOAA/NOS Phone: 240-533-0832 Email: John.D.Parker@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.13 20:41:58 -04'00' Date signed: 3/13/18
Authorizing Official Name: Dave Westerholm Office: NOAA/NOS OR&R Phone: (240) 533-0385 Email: dave.westerholm@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Date signed: 3/13/2018	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.20 15:58:54 -04'00' Date signed: 3/13/18

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.14 07:57:57 04'00'

Zachary Goldstein - NOAA Federal

From:	Zachary Goldstein NOAA Federal
Sent:	Tuesday, April 3, 2018 1:15 PM
To:	Anthony Vandegrift NOAA Federal
Cc:	Sarah Brabson NOAA Federal; Beckie Koonge NOAA Federal; Mark Graff NOAA Federal; Andrew Browne NOAA Federal; Ben Kyger NOAA Federal; Ann Rivers
Subject:	Re: NOAA8865 Tsunami Warning System Privacy Threshold Analysis
Attachments:	NOAA8865 PTA 03202018_av2.pdf

Anthony,

Attached is subject PTA with my digital signature.

Regards,
Zach

On Tue, Apr 3, 2018 at 11:22 AM, Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov> wrote:

> All,
> Still awaiting signatures from Zach and Beckie before Mark can review and sign.
> Please review and sign at your earliest convenience.
>
> I've converted it to PDF as it seems to be faster to sign PDFs.
>
> Thanks,
> Anthony
>
> On Tue, Mar 20, 2018 at 2:50 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Thanks, Anthony. Zach or Ann, please return to me for Mark's signature.
> >
> > This will be our last system that was lacking a PIA (which Mark is reviewing now).
> >
> > thx Sarah
> >
> > Zach
> >
> > On Tue, Mar 20, 2018 at 2:38 PM, Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov> wrote:
> >
> > > All,
> > > Attached is the PTA for NOAA8865. It was identified earlier this year that previous PIA/PTAs were unsatisfactory as they failed to capture information about employee information stored on the IS as well as point of contact information from Seismic network points of contacts and emergency managers that we maintain email, phone, and fax information for.
> > > Please review and sign at your convenience and reattach to this email string until the relevent parties have signed:

Beckie Koonge or Andrew Browne, NWS ITSO
Zachery Goldstein, NOAA8865 AO
Mark Graff, Bureau Privacy Officer

CCed is Ben Kyger, NOAA8865 SO for his visibility.

Anthony Vandegrift
Information System Security Officer
National Tsunami Warning Center
NOAA/NWS/NCEP/NTWS
910 S Felton Street
Palmer, AK 99645
Phone: 907-861-4225
Govt. Cel (b)(6)
anthony.vandegrift@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Anthony Vandegrift
Information System Security Officer
National Tsunami Warning System
NOAA/NWS/NCEP/NTWS
910 S Felton Street
Palmer, AK 99645
Phone: 907-861-4225
Govt. Cel (b)(6)
anthony.vandegrift@noaa.gov

Zachary G. Goldstein
Chief Information Officer and Director, High Performance Computing and Communications
National Oceanic and Atmospheric Administration

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Tuesday, April 3, 2018 1:19 PM
To:	Mark Graff NOAA Federal
Subject:	Fwd: NOAA8865 Tsunami Warning System Privacy Threshold Analysis
Attachments:	NOAA8865 PTA 03202018_av2.pdf

Here you go, a record signature from Zach!

Forwarded message
From: **Zachary Goldstein - NOAA Federal** <zachary.goldstein@noaa.gov>
Date: Tue, Apr 3, 2018 at 1:14 PM
Subject: Re: NOAA8865 Tsunami Warning System Privacy Threshold Analysis
To: Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov>
Cc: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Beckie Koonge NOAA Federal <beckie.koonge@noaa.gov>, Mark Graff NOAA Federal <mark.graff@noaa.gov>, Andrew Browne NOAA Federal <andrew.browne@noaa.gov>, Ben Kyger NOAA Federal <ben.kyger@noaa.gov>, Ann Rivers <Ann.Madden@noaa.gov>

Anthony,

Attached is subject PTA with my digital signature.

Regards,
Zach

On Tue, Apr 3, 2018 at 11:22 AM, Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov> wrote:

> All,
> Still awaiting signatures from Zach and Beckie before Mark can review and sign.
> Please review and sign at your earliest convenience.
>
> I've converted it to PDF as it seems to be faster to sign PDFs.
>
> Thanks,
> Anthony
>
> On Tue, Mar 20, 2018 at 2:50 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Thanks, Anthony. Zach or Ann, please return to me for Mark's signature.
> >
> > This will be our last system that was lacking a PIA (which Mark is reviewing now).
> >
> > thx Sarah

Zach

On Tue, Mar 20, 2018 at 2:38 PM, Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov> wrote:

> All,
> Attached is the PTA for NOAA8865. It was identified earlier this year that previous PIA/PTAs were unsatisfactory as they failed to capture information about employee information stored on the IS as well as point of contact information from Seismic network points of contacts and emergency managers that we maintain email, phone, and fax information for.
> Please review and sign at your convenience and reattach to this email string until the relevent parties have signed:
> Beckie Koonge or Andrew Browne, NWS ITSO
> Zachery Goldstein, NOAA8865 AO
> Mark Graff, Bureau Privacy Officer
>
> CCed is Ben Kyger, NOAA8865 SO for his visibility.

Anthony Vandegrift
Information System Security Officer
National Tsunami Warning Center
NOAA/NWS/NCEP/NTWS
910 S Felton Street
Palmer, AK 99645
Phone: 907-861-4225
Govt. Cel (b)(6)
anthony.vandegrift@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Anthony Vandegrift
Information System Security Officer
National Tsunami Warning System
NOAA/NWS/NCEP/NTWS
910 S Felton Street
Palmer, AK 99645
Phone: 907-861-4225
Govt. Cel (b)(6)
anthony.vandegrift@noaa.gov

Zachary G. Goldstein
Chief Information Officer and Director, High Performance Computing and Communications
National Oceanic and Atmospheric Administration

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Tuesday, April 3, 2018 1:27 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA8865 Tsunami Warning System Privacy Threshold Analysis
Attachments:	NOAA8865 PTA 03202018_av2 mhg.pdf

Back atcha. Again, though I can't tell from this document or the PIA what the "alteration in character of data" is that's referenced in Sec. 1? Where this is the first PIA for this system, it seems the response to Sec. 1 should be that this is an existing system, with no changes, and there is not an SAOP approved PIA.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Tue, Apr 3, 2018 at 1:19 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Here you go, a record signature from Zach!
>
> Forwarded message
> From: **Zachary Goldstein - NOAA Federal** <zachary.goldstein@noaa.gov>
> Date: Tue, Apr 3, 2018 at 1:14 PM
> Subject: Re: NOAA8865 Tsunami Warning System Privacy Threshold Analysis
> To: Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov>
> Cc: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Beckie Koonge NOAA Federal <beckie.koonge@noaa.gov>, Mark Graff NOAA Federal <mark.graff@noaa.gov>, Andrew Browne NOAA Federal <andrew.browne@noaa.gov>, Ben Kyger NOAA Federal <ben.kyger@noaa.gov>, Ann Rivers <Ann.Madden@noaa.gov>
>
> Anthony,
>
> Attached is subject PTA with my digital signature.
>
> Regards,
> Zach
>
> On Tue, Apr 3, 2018 at 11:22 AM, Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov> wrote:
>
> > All,

Still awaiting signatures from Zach and Beckie before Mark can review and sign.
Please review and sign at your earliest convenience.

I've converted it to PDF as it seems to be faster to sign PDFs.

Thanks,
Anthony

On Tue, Mar 20, 2018 at 2:50 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Thanks, Anthony. Zach or Ann, please return to me for Mark's signature.
>
> This will be our last system that was lacking a PIA (which Mark is reviewing now).
>
> thx Sarah
>
> Zach
>
> On Tue, Mar 20, 2018 at 2:38 PM, Anthony Vandegrift NOAA Federal <anthony.vandegrift@noaa.gov> wrote:
>
> > All,
> > Attached is the PTA for NOAA8865. It was identified earlier this year that previous PIA/PTAs were unsatisfactory as they failed to capture information about employee information stored on the IS as well as point of contact information from Seismic network points of contacts and emergency managers that we maintain email, phone, and fax information for.
> > Please review and sign at your convenience and reattach to this email string until the relevent parties have signed:
> > Beckie Koonge or Andrew Browne, NWS ITSO
> > Zachery Goldstein, NOAA8865 AO
> > Mark Graff, Bureau Privacy Officer
> >
> > CCed is Ben Kyger, NOAA8865 SO for his visibility.
> >
> >
> >
> > **Anthony Vandegrift**
> > Information System Security Officer
> > National Tsunami Warning Center
> > NOAA/NWS/NCEP/NTWS
> > 910 S Felton Street
> > Palmer, AK 99645
> > Phone: 907-861-4225
> > Govt. Cel (b)(6) [redacted]
> > anthony.vandegrift@noaa.gov

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Anthony Vandegrift
Information System Security Officer
National Tsunami Warning System
NOAA/NWS/NCEP/NTWS
910 S Felton Street
Palmer, AK 99645
Phone: 907-861-4225
Govt. Cel (b)(6)
anthony.vandegrift@noaa.gov

Zachary G. Goldstein
Chief Information Officer and Director, High Performance Computing and Communications
National Oceanic and Atmospheric Administration

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA8865 – National Tsunami Warning System

U.S. Department of Commerce Privacy Threshold Analysis

NOAA 8865 –NTWS

Unique Project Identifier: NOAA 8865

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) The NOAA National Tsunami Warning System is a general support system that acts to evaluate seismic data and determine possible tsunami hazards. The system then notifies parties responsible for emergency management.
b) The system is split between two centers on at the Inouye Regional Center in Honolulu, Hawaii (Pacific Tsunami Warning Center) and one in Palmer, Alaska (National Tsunami Warning Center).
c) This system is supported via the National Centers for Environmental Prediction (NCEP) for it's routing/firewall/and enterprise support as well as Alaska Region Headquarters and the Inouye Regional Center for building support. Outside of NOAA the system collects seismic data from international and domestic partners for evaluating events and warning messages are disseminated through email, phone, fax, EMWIN, social media, and the web.
d) The system serves to issue tsunami warnings to emergency managers, media, and the public via evaluating information received from seismic partners and ran through models.
e) The system receives seismic data from partners around the world. After detecting an earth quake its properties are evaluated to determine if there is a tsunami risk. It is ran through a model to determine possible impact. Emergency managers that supply their contact info are notified, messages are also sent via numerous NOAA emergency notification systems, social media, and our web site.
f) Seismic data is collected by the system, evaluated and appropriate warning/watch/statement is issued/modified/retracted. Titles, names, phone numbers, emails, and fax numbers are collected for seismic data points of contacts and necessary parties that need to be notified in the event of a tsunami related message. Personnel information is acquired for supervisory tasks related to employment at NOAA.

g) Only NTWS employees have access to the information system and hard copies of the points of contacts for warnings and seismic entities. Only managers and the employee for which the information is about has any kind of access to personnel information.

h) Point of contact information is kept in a database that can be looked up on the information system. Emails and faxes are sent to email lists maintained with ISC International that we create, manage, and remove entries for. Personnel information can be requested for the person the documents are about.

i) Emails and faxes are sent to points of contacts from ISC International once it receives an email from us. For certain locations phone calls may be necessary to ensure proper parties have been notified. For personnel files the information follows the policies set forth by NOAA personnel management.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__ X__ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	X
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

__X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X___ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

__X__ DOC employees
___X_ Contractors working on behalf of DOC
__X__ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NTWS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):
_____Anthony Vandegrift_____

3/20/2018

X VANDEGRIFT.ANTHONY.WAYNE.1147676855 Digitally signed by VANDEGRIFT.ANTHONY.WAYNE.1147676855 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=VANDEGRIFT.ANTHONY.WAYNE.1147676855 Date: 2018.04.03 11:20:35 -04'00'

Signature of ISSO or SO:

Name of Information Technology Security Officer (ITSO): _Beckie Koonge__

X

NWS ITSO

Signature of ITSO:

Name of Authorizing Official (AO): _____Zachery Goldstein_____

X GOLDSTEIN.ZACHARY.G.1228698985 Digitally signed by GOLDSTEIN.ZACHARY.G.1228698985 Date: 2018.04.03 13:11:08 04'00'

Zachary Goldstein
NOAA8865 Authorizing Official

Signature of AO:

Name of Bureau Chief Privacy Officer (BCPO): _____Mark Graff_____

X GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.04.03 13:22:55 04'00'

Mark Graff
Bureau Chief Privacy Officer

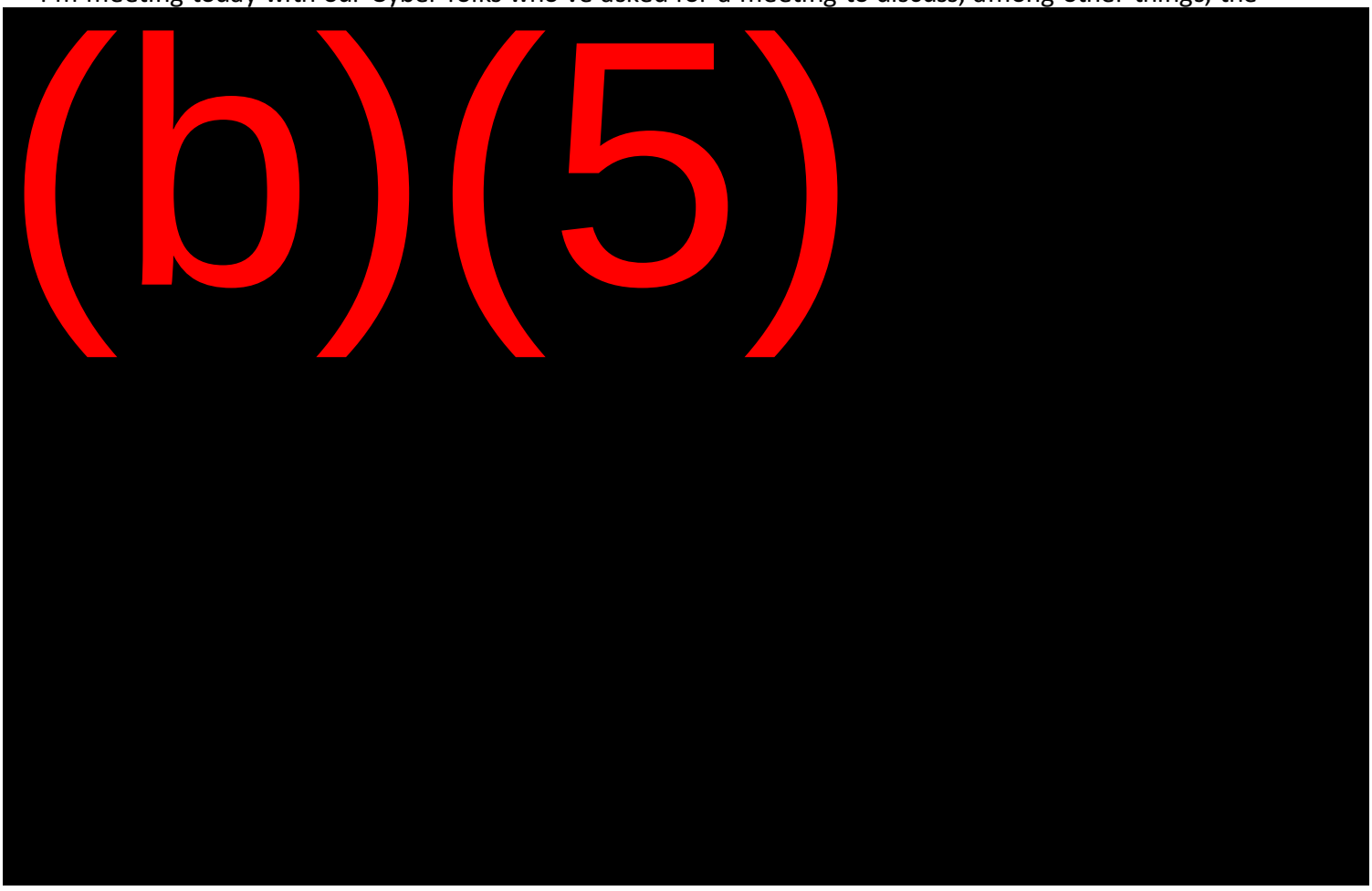
Signature of BCPO:

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, April 4, 2018 9:30 AM
To:	Bogomolny, Michael (Federal)
Cc:	Robert Hogan
Subject:	User Rules of Conduct Discussion
Attachments:	NOAA IT Security Manual.pdf; Office of Investigations Scope.pdf; Examples in Congressional Testimony from EPA OIG.pdf

Hi Bogo,

I'm meeting today with our Cyber folks who've asked for a meeting to discuss, among other things, the



Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

OIG Investigations of Employee Misconduct at the U.S. Environmental Protection Agency

Statement of Patrick Sullivan
Assistant Inspector General for Investigations

Before the Committee on Oversight and Government Reform
U.S. House of Representatives

May 18, 2016

Statement of
Patrick Sullivan
Assistant Inspector General for Investigations
Office of Inspector General
U.S. Environmental Protection Agency
Before the
Committee on Oversight and Government Reform
U.S. House of Representatives
May 18, 2016

Good morning, Chairman Chaffetz, Ranking Member Cummings and members of the committee. I am Patrick Sullivan, Assistant Inspector General for Investigations for both the U.S. Environmental Protection Agency (EPA) and the U.S. Chemical Safety and Hazard Investigation Board (CSB). I am pleased to appear before you today to discuss specific Office of Inspector General (OIG) investigations of employee misconduct issues at the EPA.

Employee Misconduct at the EPA

The EPA OIG is charged with conducting investigations and audits related to programs and operations at the EPA and CSB. The OIG remains committed to its statutory role of detecting waste, fraud and abuse, as well as promoting the effectiveness and efficiency of government operations. We operate with a separate budget and decision-making authority, and neither EPA nor CSB senior leaders may prohibit, prevent or obstruct us from conducting our work. Our independence from the agencies over which we have oversight ensures enhanced transparency and accountability in the OIG's investigations of alleged employee misconduct.

This committee specifically has asked about a number of OIG investigative cases that we previously reported on in summary fashion, and has sent the OIG a formal written request to obtain the Reports of Investigation regarding many of those, which we have provided to the committee. My testimony will provide an overview of several cases of EPA employees who viewed and downloaded pornography on government-issued computers, as well as other types of misconduct, some of which resulted in criminal prosecution. It is important to note that most of the alleged misconduct occurred at least 2 years ago.

I am happy to report that since I last testified before this committee to discuss misconduct by EPA employees, in April 2015, the agency's internal adjudication process has dramatically improved. At the suggestion of both Chairman Chaffetz and Ranking Member Cummings, the OIG, the EPA's Office of General Counsel, and the EPA's Office of Administration and Resources Management (which includes a Labor and Employee Relations section) now meet biweekly about pending misconduct cases and their adjudication by the agency. Misconduct cases are now being addressed faster and more consistently by EPA management. This increased efficiency is a result of the coordination and communication between the OIG and the agency to create a streamlined process to address employee misconduct issues. I believe that this process can serve as a "best practices" model for the federal government.

In addition, I note that while many allegations lodged against EPA employees are investigated by the OIG, some are ultimately determined to be unfounded or unsupported. In other words, OIG investigations often clear an individual. Our job is to collect and present the facts in a fair and unbiased manner. We are just as proud of our work in the cases that clear an employee as we are when our work leads to a criminal conviction or the removal of an employee who engaged in serious misconduct.

Now, I would like to summarize two of our more significant misconduct investigations that will be cited in our next Employee Integrity Cases report that will be posted to our website over the next weeks. Then I will highlight seven significant cases from our last three Employee Integrity Cases reports.

OIG Investigation of a Contractor in the EPA's Western Ecology Division

In May 2014, the OIG Seattle Field Office received a complaint from the EPA's Office of Environmental Information that a government computer assigned to an EPA contractor who was working in the EPA Western Ecology Division, Office of Research and Development, in Corvallis, Oregon had logged over 700 denials to blocked pornography, gaming and gambling sites on two occasions.

OIG special agents interviewed the EPA contractor, who stated that he was an information technology specialist who had provided support for the past 20 years. Stating he was "addicted" to pornography, he admitted to viewing pornography on his government-issued computer for the last 18 years. In the past year, he had watched pornography at least one to two hours per day. According to the contractor, he avoided detection for many years because he used commercial software to scrub/wipe his government computer. The contractor accessed pornographic sites using search engines hosted in foreign nations, including one located in Russia. He said that traditional search engines, such as Google and Yahoo, lead to pornographic sites blocked by the EPA.

Shortly after the OIG's interview, the EPA contractor was fired by his company. In addition, the OIG was successful in recovering $22,088 in repayments to the EPA by the company for the amount of time the contractor had viewed pornography during the prior year. Furthermore, the OIG made the EPA's Office of Environmental Information aware of EPA network vulnerabilities that had enabled the contractor to avoid detection for 18 years.

OIG Investigation of a GS-13 Special Agent in the EPA's Criminal Investigations Division

In February 2013, the OIG Office of Professional Responsibility was notified by the U.S. Attorney's Office (USAO) District of Connecticut, that a GS-13 special agent assigned to the EPA's Criminal Investigations Division (CID) in New Haven, Connecticut may have been engaged in criminal activity in connection with a Ponzi scheme. The special agent's name had surfaced during the prosecution of the ringleaders of a four-level pyramid scheme involving "gifting tables." New participants in this scheme would pay a $5,000 "gift" to the person occupying the top level.

Shortly after the OIG opened its investigation, the USAO District of Connecticut recused itself from the case because the EPA CID special agent was well known to the local Assistant U.S. Attorneys. The special agent had participated in numerous environmental crimes prosecutions by that office. The U.S. Department of Justice then assigned the case to the USAO District of Massachusetts.

The OIG investigation determined that the EPA CID special agent had made a false statement on a required Office of Government Ethics financial disclosure form in January 2012, wherein she concealed the fact that she had received $2,500 cash from her participation in the pyramid scheme.

In January 2015, the special agent retired from the EPA. In March 2015, she pleaded guilty to one felony count of 18 U.S.C. 1001, False Statements. In July 2015, she was sentenced to 1 year of probation and ordered to pay $7,500 in restitution, as well as a fine of $500.

OIG Investigation of a GS-14 Employee in Dallas (Case 5: April 1, 2015, to September 30, 2015)

In January 2012, the OIG Dallas Field Office received information alleging that a GS-14 program manager in EPA Region 6, Dallas, Texas, who was responsible for managing grants for the Border Environment Cooperation Commission, was using grant money for purposes not related to the grant.

The OIG investigation determined that the EPA program manager misused her position to divert agency grant funds, resulting in several improper payments by Border Environment Cooperation Commission officials totaling $5,195.

The USAO Northern District of Texas declined to prosecute the EPA program manager for potential violation of various federal statutes, including 18 U.S.C. 641 (theft of government funds) and 18 U.S.C. 666 (theft or bribery concerning programs receiving federal funds). The USAO declined to prosecute primarily because the program manager did not personally benefit from the diversion of the grant funds.

In July 2014, although termination was proposed in lieu of this, the EPA Region 6 Director of Multimedia Planning and Permitting Division agreed to let the program manager enter into an Abeyance/Last Chance Agreement. The terms of the agreement included the following:

- The effective date of the program manager's removal from employment would be held in abeyance in return for her compliance with the terms of this agreement.
- Within 2 years of signing this agreement, she would pay back $5,195 to the federal government based on a process determined by the agency.
- She would be demoted to a position chosen by the agency at the pay rate of GS-12, Step 10.

OIG Investigation of a GS-13 Employee in EPA's Office of Pollution Prevention and Toxics (Case 17: April 1, 2015, to September 30, 2015)

In March 2012, the OIG Washington Field Office received a complaint from the EPA's Office of Environmental Information alleging that a GS-13 biologist who worked in the EPA's Office of Pollution Prevention and Toxics downloaded pornographic images to an EPA shared file. During the course of the investigation, the employee admitted that he viewed and downloaded videos, movies and photographs, including those of pornographic nature, onto his EPA-issued computer.

The OIG reviewed the pornographic material on the employee's EPA-issued computer through a forensic examination, and found approximately 500 pornographic images. Additionally, the OIG determined that more than 2,560 videos and 435 music files were accessed and/or downloaded by the employee. The review also discovered sexually explicit videos on the employee's EPA-issued computer.

In 2014, the employee was barred from EPA facilities and placed on paid administrative leave pending a decision on the matter. In March 2015, a notice of proposal for removal for the misuse of government equipment for other than official purpose was provided to the employee. In May 2015, the employee's retirement after receiving a written notice for the proposal of removal went into effect.

OIG Investigation of a GS-12 Employee in Atlanta (Case 8: October 1, 2014, to March 31, 2015)

In October 2013, an OIG special agent in the Atlanta Field Office proactively checked a list of EPA property reportedly lost or stolen from EPA Region 4 in Atlanta through a law enforcement database. This search resulted in a "hit" on an EPA digital camera pawned at a store in Decatur, Georgia, in July 2012. The person who pawned the camera had the same name as an EPA Region 4 employee a GS-12 public affairs specialist in the Office of External Affairs. The camera was assigned to the Office of External Affairs.

The subsequent OIG investigation revealed that, on seven occasions between July and September 2012, the EPA employee pawned EPA digital cameras and camcorders at the same pawn shop. She failed to reclaim EPA property on five occasions, and the property was then sold by the pawn shop, resulting in a loss to the government of $3,117. The USAO Northern District of Georgia declined prosecution for violation of 18 U.S.C. 641 (theft of government property). However, the District Attorney's Office in Fulton County, Georgia, accepted the case for local prosecution.

In January 2014, the EPA Region 4 Director of the Office of External Affairs issued a memorandum that proposed the suspension of the employee for 120 days. Following an appeal by the employee, the Deputy Regional Administrator issued, in May 2014, a memorandum detailing the final decision to suspend the employee for 30 days.

In October 2014, the EPA employee pleaded guilty to theft, in violation of Georgia Code, Title 16, Section 16-8-2, in Superior Court of Fulton County. She was sentenced to 3 years of probation, and ordered to pay restitution in the amount of $3,117, as well as a fine of $1,000.

The OIG investigation further revealed that the EPA Region 4 property custodian falsely certified her physical property inventories in fiscal years 2012 and 2013. The property custodian signed and certified that she conducted an inventory of all of the property items assigned to her inventory for that period. It was determined that two of the items allegedly inventoried by the property custodian were previously pawned by the GS-12 public affairs specialist and not returned. Therefore, these items were not physically present within Region 4, and could not have been inventoried. In June 2014, the Director of the Office of External Affairs issued the property custodian a letter of warning in reference to her false certifications of inventories.

OIG Investigation of a GS-12 Employee in the Office of Administration and Resources Management in Research Triangle Park (Case 9: October 1, 2014 to March 31, 2015)

In August 2013, the OIG Research Triangle Park (RTP), North Carolina, Field Office was notified that a GS-12 employee, who was working as a Contracting Officer's Representative at the Facilities Support Branch, Office of Administration and Resources Management, in RTP, was suspected of having a financial interest in a company doing business with the EPA.

The OIG's investigation determined that the EPA employee did have a financial interest in a company doing business with the EPA, which is a potential violation of 18 U.S.C. 208 (acts effecting a personal financial interest). The USAO Middle District of North Carolina declined prosecution and referred the matter back to the EPA for administrative action.

In July 2014, the OIG submitted a Report of Investigation to the Office of Administration and Resources Management senior management official at RTP, in which allegations of misconduct were supported. The OIG's investigation determined that the EPA employee had not reported that she had a financial interest in a company doing business with the EPA. Further, she used EPA computers for conducting personal business. She also provided false information when interviewed by OIG special agents.

In August 2014, EPA rescinded the EPA employee's authority to act as a Contracting Officer's Representative. In September 2014, the employee resigned. At the time of her resignation, the EPA was considering a proposal to remove her from federal service. However, she had not yet been served with termination papers.

OIG Investigation of a GS-13 Employee in Dallas (Case 17: October 1, 2014, to March 31, 2015)

In March 2006, the OIG Dallas Field Office was informed that a GS-13 EPA Enforcement Officer was cited by the Dallas Police Department for the improper use of emergency lights on his personal vehicle while also being a registered sex offender. He previously had been convicted, in April 1997, on a deferred adjudication for indecent acts with a minor. (Note: An EPA Enforcement Officer is NOT a federal law enforcement officer (LEO), but rather an administrative enforcement officer. Unlike a federal LEO who carries a gun and badge and is authorized to execute arrest and search warrants, an EPA enforcement officer is not armed and cannot make arrests). The EPA employee also possessed a make-shift badge which accompanied his administrative EPA

Enforcement Officer credentials, which were displayed by the employee to the police officer. This led the police officer to believe that the employee was an EPA law enforcement officer. The EPA employee also used emergency lights affixed to his personal vehicle at an accident scene. The police officer checked the employee's vehicle license plate and determined that he was a registered sex offender.

The subsequent OIG investigation disclosed that the EPA employee had designed and purchased 20 similar badges. He also possessed a bullet-proof vest and installed emergency lights on his personal vehicle, which was a violation of his probation for a sex offender charge. (Note: In March 1999, the same employee had been counseled by EPA Region 6 officials for using emergency lights on his personal vehicle. He was then told to remove all law enforcement equipment from his personal vehicle.)

In April 2006, the USAO Northern District of Texas declined to prosecute the EPA employee for violation of 18 U.S.C. 912 (false personation) and 18 U.S.C. 701 (counterfeit badges). EPA Region 6 then imposed discipline in the form of a 60-day suspension, and the EPA employee was removed from his position as an EPA Enforcement Officer. He was reassigned to an administrative position within the office.

In August 2013, the Dallas Police Department Sex Offender Unit requested assistance from the OIG in arresting the same EPA employee for violation of probation. He was arrested on the probation violation charge. As a result of this arrest, the OIG developed information that the employee may have viewed and possessed child pornography on his EPA-issued computer. A subsequent OIG forensic examination of his computer revealed no evidence of child pornography or any pornography on his EPA computer.

Following the employee's arrest for probation violation, EPA Region 6 indefinitely suspended him. In January 2014, the employee was terminated from his employment with the EPA.

Subsequently, the Merit Systems Protection Board overturned the employee's termination and ordered that he be re-hired by the EPA. In September 2014, the employee returned to work at the EPA. In January 2015, the employee entered into a Settlement Agreement, which was overseen by Merit Systems Protection Board, in which he agreed to resign from the EPA in exchange for certain considerations.

OIG Investigation of SES-Level Director in EPA's Office of Administration and Resources Management (Case 3: April 1, 2014 to September 30, 2014)

In January 2014, while conducting an investigation into an unrelated misconduct case, an OIG special agent in the Washington Field Office discovered that an Senior Executive Service (SES)-level EPA employee, who was the Director of the Office of Administration and Resources Management's Facilities Management and Services Division, incurred $22,315 in international roaming charges on her EPA-issued mobile device between December 2010 and October 2012. The EPA Director had no authorized international travel on behalf of EPA. The OIG investigation ultimately supported the following charges in which the EPA Director:

1. Improperly used her EPA issued mobile device while overseas on personal travel and incurred over $22,000 in charges.
2. Made false statements on the SF-86, Questionnaire for National Security Positions when she failed to disclose five trips to Israel and one trip to Germany.
3. Made false statements on the same SF-86 when she failed to disclose that she wired $90,000 to a foreign national in Jericho, Palestine.
4. Claimed approximately 24 hours of regular work time while on personal travel to Israel, when she should have claimed annual leave.

The USAO District of Columbia declined to prosecute for violations of 18 U.S.C. 1001 (false statements) and 18 U.S.C. 641 (theft of government funds).

In May 2014, the OIG provided the EPA with a report of investigation; however, shortly thereafter, and prior to the agency taking administrative action, the EPA Director resigned her position. Subsequently, the agency conducted an initial review and was unable to determine what portion of the employee's charges were due to personal activity versus work activity. In April 2016, the EPA informed the OIG that the matter was being reviewed. The agency is now considering issuing a debt notice to the EPA Director for the charges incurred.

OIG Investigation of a GS-14 Employee in Kansas City (Case 10: April 1, 2014 to September 30, 2014)

In August 2010, the EPA Regional Administrator, Region 7, Kansas City, Kansas, made a formal referral to the OIG based upon a complaint filed in the U.S. District Court, District of Nebraska by the Union Pacific Railroad Company. The referral alleged that the EPA violated the Freedom of Information Act and other statutes in connection with the Omaha Lead Superfund Site. It was alleged that the agency destroyed emails and other records.

In 2012, the OIG opened a criminal investigation, in concert with the FBI, after developing preliminary information indicating that a GS-14 EPA environmental engineer assigned to Region 7 destroyed emails concerning the Omaha Lead Superfund Site and encouraged other agency employees to do the same. Because of a potential conflict of interest, the USAO District of Nebraska recused itself from the criminal investigation. The U.S. Department of Justice assigned the case to the USAO District of Kansas. Ultimately, the USAO declined to prosecute the EPA employee for violation of 18 U.S.C. 1519 (destruction or alteration of records in federal investigations and bankruptcy) or other statutes due to a lack of provable criminal intent.

In November 2013, the OIG submitted to the Region 7 Regional Administrator a Report of Investigation in which administrative misconduct by the employee was supported. The OIG investigation revealed through the use of computer forensics, and the results of interviews, affidavits and depositions that the employee deleted emails and directed and/or instructed other EPA employees to delete emails pertaining to the Omaha Lead Superfund Site.

In May 2014, the OIG was informed that a notice of proposed removal was served on the employee, but the employee retired from federal service before the termination became effective.

Additional EPA Employee Integrity Cases

The OIG posts to its publicly-accessible Investigations web page reports summarizing the closed EPA employee integrity cases. The following, available in those posted reports, describe a number of additional OIG investigations that were closed within the previous three reporting periods (April 1, 2014, to September 30, 2014; October 1, 2014, to March 31, 2015; and April 1, 2015, to September 30, 2015). The OIG intends to publish its next report on employee integrity cases (October 1, 2015, to March 31, 2016) in late May or early June 2016.

List of Selected Closed Employee Integrity Cases: April 1, 2015, to September 30, 2015

CASE 1: An SES-level supervisor allegedly engaged in inappropriate behavior, hiring, promotions and management of programs. Also, the supervisor allegedly compromised his ability to be objective in his conduct at work and in his management of senior staff. The supervisor admitted involvement in an inappropriate romantic relationship with a subordinate, GS-15-level, employee. Additionally, evidence showed that the supervisor attempted to influence other EPA employees in an effort to promote the subordinate employee. The supervisor retired from the EPA before a report of investigation could be presented to the agency.

CASE 6: Potential conflicts of interest were alleged to have resulted from the appointment of an EPA attorney as Chairman of an environmental quality board. The allegation noted that the employee claimed to speak for or represent the EPA in meetings with the local regulated community, and may have misused the dual positions for private gain. In addition, according to the allegation, the EPA employee may have sponsored and organized a fundraising event, and required board employees to make donations and attend the event for the re-election campaign of a governor. The investigation was unable to substantiate that the employee had used the EPA position for private gain or that the employee had made board employees contribute to a fundraising event. The employee resigned from the EPA during the investigation. This case was presented to the U.S. Office of Special Counsel and the USAO; both declined advancing the matter.

CASE 9: An EPA employee allegedly was cited for attempting to bring approximately three grams of marijuana and two marijuana pipes through the security checkpoint at an Internal Revenue Service facility in Denver, Colorado, and arrested on an active warrant for failure to appear. The investigation confirmed that the employee had appeared in the U.S. District Court for the District of Colorado and was found guilty of one count of possession of marijuana on federal property. The employee was sentenced to a 3-day suspended sentence, 12 months' unsupervised probation and 20 hours of community service, and was ordered to pay a $2,500 fine. The employee was suspended from the EPA for 21 days.

CASE 10: An EPA employee allegedly failed to disclose criminal and financial indebtedness when completing form OF-306, *Declaration for Federal Employment*, and form SF-85P, *Questionnaire for Public Trust Positions*. The investigation revealed that, during an employment suitability background investigation of the EPA employee conducted by the Office of Personnel

Management, criminal and financial indebtedness information surfaced that previously had not been divulged on forms OF-306 and SF-85P. The EPA's Personnel Security Branch requested from the employee documentation of the paying down of accumulated debts. The documentation tendered did not appear authentic and was determined to be fraudulent. The employee provided false information to the EPA concerning criminal history and failed to pay accrued personal debts, which included an EPA travel card balance of $10,226. The EPA presented the employee with a letter of proposed removal; however, the employee retired from the EPA prior to removal.

CASE 11: An EPA employee allegedly misused an EPA-issued travel credit card for personal expenses. During an interview, the employee admitted using the EPA-issued travel credit card for personal charges totaling $625. The employee stated a belief that there was no loss to the government as the expenses were subsequently paid for with cash. The employee had not been candid with supervisors and the OIG when initially questioned about the personal charges. The employee was issued a 14-day suspension.

CASE 16: An EPA employee may have violated conflict of interest laws by representing two nonprofit organizations back to the federal government. The investigation did not substantiate the allegation but uncovered evidence of other violations. The employee had misused EPA resources, such as EPA email and an EPA-issued computer, to conduct business on behalf of the two nonprofit organizations. The employee had neglected to disclose involvement with the nonprofit organizations on the *Confidential Financial Disclosure Report* (OGE Form 450). The employee also had allowed biographical information to be posted on one nonprofit organization's website, and the biography gave more prominence to the employee's EPA position than to other details. After this discovery, the biography was removed from the organization's website. Additionally, the employee was acting in a "leader" capacity at the same nonprofit and previously had been a board member there (while concurrently working for the EPA). A report of investigation was presented to the EPA, which later notified the OIG that the employee was suspended for two days.

List of Selected Closed Employee Integrity Cases: October 1, 2014, to March 31, 2015

CASE 5: An EPA employee was alleged to have potential conflicts of interest and ethical violations. The investigation found that the employee had violated the Code of Federal Regulations and the EPA ethics code by submitting a letter of support to the EPA on EPA letterhead, resulting in a potential unfair competitive advantage to a prospective grant recipient and disqualification of the grantee's proposal from further consideration. The employee was issued a warning letter for assisting the prospective grant recipient with a proposal.

CASE 13: An EPA employee allegedly misused the employee's position by allowing two nonprofit organizations to use an EPA leased trailer and surrounding property to conduct non EPA related activities without authorization. The investigation supported and the employee admitted to allowing two nonprofit organizations unauthorized use of the trailer, free of charge, for non project related activities. The employee was suspended for five days.

CASE 18: An EPA employee was arrested on felony charges of marijuana possession after local police discovered a marijuana growing operation in her residence. The employee was placed on

paid administrative leave in March 2014, and the employee signed a separation agreement in May 2014. She remained on paid administrative leave until her retirement on October 30, 2014. In as much as there was no violation of federal law, this case was not presented to the USAO.

List of Selected Closed Employee Integrity Cases: April 1, 2014, to September 30, 2014

CASE 8: An EPA employee allegedly misused an EPA-issued mobile device by placing personal international calls. The investigation disclosed that the employee had incurred more than $4,500 in international roaming charges when the mobile device was used in a foreign country while the employee was on leave. The employee and all division staff were counseled by management on the appropriate use of EPA-issued mobile devices. The USAO-District of Columbia declined prosecution for violation of 18 USC 641 (theft of government funds).

CASE 11: A GS-15-level employee viewed pornographic material on an EPA-issued computer while in duty status. The employee admitted to the allegation, and a forensic analysis of the hard drive substantiated that the employee had watched pornography regularly at work for the past several years. The employee was suspended for 5 working days, is no longer allowed to telework, and is not allowed to attach any unauthorized external drive devices to a government computer.

CASE 13: There was an alleged conflict of interest between an EPA employee and a contractor when the employee became involved with an initial contract task order. The investigation substantiated the allegation, but the case was declined for criminal prosecution by the U.S. Attorney's office. The EPA's administrative proposal recommended removal of the employee, but the employee retired before the proposal was finalized.

CASE 15: An EPA employee allegedly misused his EPA-issued travel card for services unrelated to government travel and attempted to mislead EPA officials regarding how the travel card had been used. Management initiated removal of the employee; however, the employee resigned prior to being formally served with a notice of proposed removal. The USAO-Northern District of California, declined prosecution for violation of 18 USC 1001 (false statements). There was no dollar loss to the government.

CASE 16: An EPA employee and a contractor allegedly exchanged emails containing procurement-sensitive information relative to the EPA's Central Data Exchange support contract valued at $220 million. The emails allegedly constituted a violation of the Procurement Integrity Act, which prohibits the disclosure of contractor bid or proposal information and source selection information. The investigation confirmed that the employee had engaged in conversation, via email, with the contractor, revealing sensitive procurement information. The email exchange took place during the open procurement period for the contract. The allegation regarding violation of the act was proven. The EPA issued a warning to and counseled the employee concerning improper communications. The employee was relieved of the role of Contracting Officer's Technical Representative and instructed to take interpersonal skills training.

CASE 17: An EPA employee allegedly used an office purchase card to pay off a personal debt to a university in the amount of $1,678. This case was prosecuted by the USAO-District of

Columbia. The employee pleaded guilty to one count of first degree fraud misdemeanor and entered into a deferred sentencing agreement. The conditions of the agreement were for the employee to perform 48 hours of community service and not be rearrested in the next 6 months with any incident where probable cause could be established. No restitution was ordered by the court. The employee resigned following her conviction.

CASE 18: An EPA employee allegedly incurred improper international roaming charges on an EPA-issued mobile device. The employee agreed to pay back $1,725. The employee also was orally reprimanded and counseled on the appropriate use of government-issued equipment and the EPA's international travel policies. The employee's manager indicated that all staff would be made aware of the EPA's policy on government equipment and international travel.

Conclusion

The OIG takes very seriously its overall responsibility for investigations into allegations of employee misconduct at the EPA. To that end, we will continue to work closely with the agency, U.S. Department of Justice, our law enforcement partners and Congress to ensure that allegations of employee misconduct are quickly and properly addressed. We appreciate your continued interest in the work of the OIG.

Mr. Chairman, this concludes my prepared statement. I will be happy to answer any questions that you, the Ranking Member and the committee members may have.

Biography of Assistant Inspector General for Investigations
Patrick Sullivan

Patrick Sullivan is the Assistant Inspector General for Investigations, Office of the Inspector General of the U.S. Environmental Protection Agency (EPA). He supervises the OIG's criminal investigative activities, including allegations of grant fraud, contract fraud, employee misconduct, threats directed against EPA officials and facilities, and other violations of federal law within the OIG's jurisdiction. He has more than 30 years of service in federal law enforcement with significant supervisory, administrative, intelligence, counter-terrorism and criminal investigative experience.

Prior to his appointment at the EPA-OIG, Mr. Sullivan served as a Deputy Assistant Director with the Transportation Security Administration's (TSA's) Federal Air Marshal Service. He supervised TSA's participation in the Joint Terrorism Task Force program, the Federal Air Marshals' intelligence program and the imbedding of Federal Air Marshals with the Federal Bureau of Investigation, the Central Intelligence Agency, Immigration and Customs Enforcement, and Customs and Border Protection. He also was responsible for supervising TSA's domestic and foreign law enforcement liaison activity.

Previously, Mr. Sullivan was an Assistant Director with the Government Accountability Office, Office of Special Investigations, where he worked on cases involving allegations of misconduct by high-level government officials as well as special investigations requested by congressional committees.

He spent more than 20 years in the U.S. Secret Service, where his last assignment was the worldwide supervision of counterfeiting investigations. He also was assigned to the U.S. Department of Justice, Organized Crime Strike Force, in Brooklyn, NY, where he worked cases targeting the traditional mafia crime families in New York City. Furthermore, he spent four years assigned to the Presidential Protection Division under Presidents Ronald Reagan and George H.W. Bush.

Early in his career, Mr. Sullivan worked for the FBI as an Investigative Assistant assigned to the surveillance of foreign intelligence officers engaged in suspected espionage and other intelligence activities directed against the United States.

He is a graduate of the John Jay College of Criminal Justice with a B.S. degree in Police Science and Criminal Justice. He is also a graduate of the Naval Postgraduate School, Center for Homeland Defense and Security, Executive Leadership Program and a member of the federal Senior Executive Service.

Department of Commerce • National Oceanic & Atmospheric Administration

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

IT SECURITY MANUAL 212-1301

Effective Date: September 01, 2016

Management, Operational, and Technical Controls

NOTICE: This publication is available at: NOAA IT Security Web Site

Date of Issuance: May 25, 2016

Version 5.6

This page is intentionally blank.

Changes/Revisions:

Modifications made to this document are recorded in the Change/Revision Record below. This record shall be maintained throughout the life of the document.

Change / Revision Record				
Date	**Version**	**Section**	**Description of Change**	**Author**
2007-05-15	3.3	All	Initial Version	L. Reed
2008-02-04	4.0		Added Revision History	L. Reed
2008-02-04	4.0		Aligned control selections with NIST SP 800-53 rev2 CP-4 changed from Not Selected to CP-4 for Low Baseline	L. Reed
2008-02-04	4.0		Corrected alignment with SP 800-53 rev2 AU-8 changed from Not Selected to AU-8 for Low Baseline MP-3 changed from MP-3 to Not Selected for Moderate Baseline AC-18 changed from Not Selected to AC-18 for Low Baseline SI-3 added enhancement 2 for Moderate Baseline SI-4 added enhancement 4 for Moderate Baseline	L. Reed
2008-02-04	4.0	All	Added Section numbers	L. Reed
2008-02-04	4.0	RA-5	Added requirements for remediation and reporting	L. Reed
2008-02-04	4.0	IR-1	Clarified N-CIRT role during incident (suspected incident) response	L. Reed
2008-02-25	4.0	RA-1,RA-5, IR-1, AT-2, AT-3, PL-1	Changed to address ITSC comments	L. Reed
2008-02-28	4.1	RA-5	Grammar correction	L. Reed

Change / Revision Record				
Date	**Version**	**Section**	**Description of Change**	**Author**
2008-02-28	4.1	CA-1.B	Changed Certification Official to Certification Agent. Clarified "recommendation" to CA recommendation.	L. Reed
2008-02-28	4.1	CA-6	Removed reference to National Critical systems	L. Reed
2008-02-28	4.1	MP-1.k	Removed moderate systems to align with SP 800-53	L. Reed
2008-02-28	4.1	SC-11	Grammar correction	L. Reed
2008-03-10	4.1	IR-1	Added escalation requirement	L. Reed
2008-03-11	4.2	IR-1	Clarifications	L. Reed
2013-06-30	5.0	All	Addressed requirements for NIST SP 800-53, Rev.4	Team Ambit
2015-01-23	5.1	All	Draft updates per ITSC reviews	Team Ambit
2015-03-24	5.2	Sections 2, 3 and Appendices	Updates per CSD and LO ITSO reviews	D. Stevens
2015-05-12	5.3	All	Updates per CSD and LO ITSO reviews	D. Stevens
2015-06-17	5.4	All	Updates per CSD and LO ITSO reviews	D. Stevens
2016-4-29	5.5	All	Updated cover page/removed Water marks, corrected contents table.	H. Burgos
2016-5-11	5.6	Cover Page/Sect. 1.3	Effective Date updated	H. Burgos

This page is intentionally blank.

Contents

SECTION 1: INTRODUCTION

This page is intentionally blank.

1 INTRODUCTION

The U.S. Department of Commerce National Oceanic and Atmospheric Administration (NOAA) have adopted a set of security controls to protect sensitive information and information systems. The Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, specifies the minimum security requirements for federal information and information systems. NOAA is responsible for ensuring that all information systems meet the minimum security requirements defined in FIPS 200 through the use of the security controls provided in the NOAA System Security Plan (SSP) which includes updates from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. NOAA developed the security policies and procedures to ensure security controls are properly implemented and maintained.

The development of sound policies provides both direction and management support. The NOAA Information Technology Security Manual (ITSM) sets the NOAA-wide direction for protecting NOAA information and information systems. This ITSM defines the key roles and responsibilities for carrying out information security program activities at NOAA. The ITSM also establishes the "NOAA-defined" parameters for identified NIST SP 800-53 Revision 4 security controls and additional security policies.

These policies and procedures are established to ensure all NOAA users adhere to the following three security objectives:

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Confidentiality ensures that NOAA information is protected from all unauthorized disclosure.

Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Information integrity ensures that NOAA information is protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:

- **Authenticity –** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- **Non-repudiation –** Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
- **Accountability** The property that enables the tracing of system activities to their sources who may then be held responsible for such activities. Auditing is a primary means of monitoring accountability.

Availability - Ensuring timely and reliable access to and use of information. Availability ensures that NOAA information resources (system or data) are accessible on a timely basis to meet mission requirements or to avoid substantial losses. Information availability also includes ensuring resources are used only for intended purposes.

1.1 PURPOSE

The purpose of this ITSM is to define the requirements necessary for all of NOAA systems to meet the fundamental security and privacy objectives of system and data confidentiality, integrity, and availability.

1.2 SCOPE AND APPLICABILITY

The policies and procedures in this document, and its attachments, apply to all NOAA information resources. NOAA information includes data that is owned, sent, received, or processed by NOAA or third parties on behalf of NOAA and includes information in either physical or digital form. NOAA information resources include NOAA hardware, software, media, and facilities.

Finally, this policy applies to other Agencies' systems as delineated in Memorandums of Understanding (MOU) and Interconnection Security Agreements (ISA) with NOAA.

Everyone who uses, manages, operates, maintains, or develops NOAA applications or data wherever the applications or data reside must comply with the ITSM, unless a specific waiver is obtained from the NOAA Chief Information Officer (CIO) or the NOAA Senior Agency Information Security Officer (SAISO), following the process specified in section 1.4 below.

1.3 COMPLIANCE AND ENFORCEMENT

Compliance: NOAA ITSM is mandatory for all NOAA employees and contractors. All users must adhere to all policies detailed in this manual by its effective date of **1 September 2016.**

Enforcement: Under authority outlined in the NOAA Administrative Order (NAO) 212-13, the NOAA CIO is responsible for continually reviewing the status of NOAA's

Information Security Programs by monitoring:

- The effectiveness of security and privacy control measures;
- Compliance with existing policies, procedures, standards, and guidelines; and
- User awareness of information security and privacy.

Violations of the policies contained in the ITSM including any related NOAA Information Technology Policies may result in the loss of, or limitation of, access to NOAA information systems and information. Anyone in NOAA who violates the policy may face administrative action ranging from counseling to removal from the NOAA, as well as, criminal penalties or financial liability, depending on the severity of the misuse.

NOAA employees and contractors are subject to penalties established by the Privacy Act of 1974. Certain penalties apply to the misuse or unauthorized disclosure of personally identifiable information. The Act (5 U.S.C. 552a (g)) provides for civil remedies for injured parties, including actual damages, attorney fees, and litigation costs.

A policy violation is an infringement or nonobservance of NOAA policy. If policy violation is suspected, NOAA employees shall report it to their NOAA supervisor, manager, and Staff and Line Office ITSO, as appropriate. Contractors shall report suspected violations to their contracting officer's technical representative and the System Owner. The following preemptive

actions must be taken to isolate the suspected violators and systems to prevent additional risk to NOAA:

- The suspected violator's group lead shall notify the NOAA Cyber Security Division for additional guidance;
- Management shall be responsible for any disciplinary actions;
- The NOAA CIO or respective ACIO shall be responsible for any technical actions; and
- The NOAA CIO or respective ACIO shall restrict access to NOAA information systems until the violator proves, to the satisfaction of the CIO or respective ACIO, that the issue is resolved and there is no future risk.

1.4 ADOPTION OF THE INFORMATION SECURITY AND PRIVACY POLICY REQUIREMENTS

NOAA users are responsible for using the current official version of the ITSM posted on the NOAA intranet (https://sites.google.com/a/noaa.gov/cio/internal-use-only). NOAA leadership will hold users responsible for adhering to the policies and standards in the current official version.

1.5 WAIVER PROCESS

Waivers are to be adjudicated by the NOAA CIO, except for controls and/or policies which explicitly require a waiver be adjudicated at the DOC CIO level. Circumstances for waivers differ from controls baseline tailoring as described in Waiver requests shall document:

1. Explanation of unique circumstance justifying foregoing the implementation of the requirement/control (to be documented in a single waiver to cover multiple systems affected, and in the SSP for each system on which the control/policy will not be implemented must reference the single waiver.)

2. Description of compensating control(s) that provide(s) an equivalent or comparable protective value to that of the requirement/control objective not being implemented in the manner described by policy. This will be documented in a single waiver to cover multiple systems affected, and in the SSP for each system on which the control/policy is compensated must reference the single waiver.

3. Description of any residual risk introduced as a result of meeting the requirement/control objective through application of compensating controls to be documented in a single waiver to cover multiple systems affected. The Risk Assessment must reference the single waiver.

4. A written recommendation from the system's responsible Authorizing Officials (AOs) in regard to accepting the risk and approving the waiver.

5. Controls not currently being employed but which are planned to be employed must be documented in a POA&M and the POA&M referenced in the respective control section in the SSP or Risk Assessment.

6. Decision by the NOAA CIO (or DOC CIO in cases where policy requires DOC CIO approval of waivers).

Waivers shall be made available through CSAM to the DOC CISO/SAISO.

1.6 MAINTENANCE OF THE OFFICIAL VERSION

The CIO will be assisted by the IT Security Committee (ITSC) in the review of the policy at least annually from its initial distribution, and will review and update it as needed based on emerging information security policy and procedure requirements.

When document revisions are formally approved, the CIO will issue a new version or an amendment to the ITSM and post it to the NOAA Intranet (https://sites.google.com/a/noaa.gov/cio/internal-use-only).

1.7 LEGAL AUTHORITY

NOAA developed the ITSM to comply with applicable laws and directives related to information security and policies. This policy document acquires its legal authority from the NOAA Administrative Order (NAO) 212-13 and Federal Information Security Management Act (FISMA); the Privacy Act of 1974; the Computer Security Act of 1987; the Computer Fraud and Abuse Act of 1987; OMB A-130, Appendix III; the Clinger-Cohen Act of 1996; Executive Order 13011, Federal IT; and all relevant NIST standards, regulations in the Code of Federal Regulations (CFR); and the Office of Management and Budget (OMB) memorandums, circulars, and directives.

SECTION 2: ROLES AND RESPONSIBILITIES

This page is intentionally blank.

2 ROLES AND RESPONSIBILITIES

All NOAA users have information security policy and procedure responsibilities. The key roles and responsibilities for carrying out this policy are outlined below as defined in the NIST Special Publication 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems, Appendix D*.

2.1 UNDER SECRETARY OF COMMERCE FOR OCEANS AND ATMOSPHERE AND ADMINISTRATOR (Head of Agency/Chief Executive Officer)

The NOAA agency head is the Under Secretary of Commerce for Oceans and Atmosphere and Administrator. This individual has the responsibility to ensure that (i) information security management processes are integrated with strategic and operational planning processes; (ii) senior officials within the organization provide information security for the information and information systems that support the operations and assets under their control; and (iii) the organization has trained personnel sufficient to assist in complying with the information security requirements in related legislation, policies, directives, instructions, standards, and guidelines.

2.2 RISK EXECUTIVE FUNCTION

The NOAA Chief Information Officer (CIO) and Deputy CIO (DCIO) along with the NOAA Enterprise IT Risk Board, the NOAA Executive Council (NEC), the NOAA Executive Panel (NEP), the NOAA CIO Council and the NOAA Enterprise IT Risk Coordinator, are responsible for establishing the NOAA-wide approach for managing agency-wide data and system risk and help ensure that: (i) risk-related considerations for individual information systems, to include authorization decisions, are understood at an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and integrates IT security risk with the DOC Enterprise Risk Management process. The risk executive (function) coordinates with the senior leadership of an organization to:

- Provide a comprehensive, NOAA-wide, holistic approach for addressing risk an approach that provides a greater understanding of the integrated operations of the organization.
- Develop a risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole.
- Facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization.
- Provide oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent and effective risk acceptance decisions.
- Ensure that authorization decisions consider all factors necessary for mission and business success.
- Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation.

- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility.
- Ensure that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities; and
- Identify the organizational risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

2.3 NOAA CHIEF INFORMATION OFFICER

The NOAA Chief Information Officer (CIO) has oversight responsibility for the NOAA IT Security Program. The Security Program is implemented and maintained through interaction with NOAA's Line Office Assistant CIOs (ACIOS) and the LO Senior Agency Information Security Officers (SAISOs) or IT Security Officers (ITSOs). The NOAA CIO:

- Acts as the Authorizing Official (AO) for the authorization of all NOAA IT systems. This authority of the NOAA CIO may be delegated in writing to the Assistant CIOs of the involved Staff or Line Office or their Deputy. The NOAA CIO serves as Co-AO for all NOAA high systems. The Line Office Assistant CIOs will be the Co-AO for Low and Moderate systems.
- Ensures the appointment and/or designation of AOs and co-AOs as appropriate and in writing
- Ensures AOs and co-AOs, as applicable, authorize all systems and ensuring compliance with the Federal Information Security Management Act (FISMA), as well as DOC and NOAA policy requirements.
- Approves and enforces information security policies, procedures, and control techniques to address all applicable requirements.
- Oversees offices, groups, teams, or other organizations that are responsible for providing generic IT services identified in the NOAA-level IT Service Catalog, including personnel with significant responsibilities for information security; and ensures that the personnel are adequately trained.
- Assists other senior organizational officials concerning their security responsibilities
- In coordination with other senior officials, reports annually to the NOAA Administrator on the overall effectiveness of the organization's information security program, including progress of remedial actions.
- Provides advice and assistance to the NOAA Administrator and other senior Agency personnel to ensure NOAA IT security goals, priorities, and requirements are effectively and efficiently addressed to protect NOAA's investments in IT.
- Ensures sufficient funds are requested and allocated to sustain the NOAA wide IT security programs.

2.4 NOAA ASSISTANT CHIEF INFORMATION OFFICER

The Assistant Chief Information Officer (ACIO) will:

- Ensure that an IT Security Program is developed and implemented for their Staff or Line Office.
- Designate in writing a Senior Agency Information Security Officer (SAISO)/Cyber Security Program Manager (CSPM) to oversee and execute the Staff or Line Office Cyber Security Program and ensure that the SAISO/PM has the staff and resources necessary to carry out the program in accordance with FISMA.
- Act as the Co-Authorizing Official (AO) for the authorization of all low and moderate Line Office IT systems, and the AO for all low and moderate systems under their direct ownership authority. This authority may be delegated only to the Deputy ACIO. The Line Office ACIO will hold the Line Office AOs accountable for authorizing all systems to operate and ensuring compliance with the FISMA, the Line Office relevant policies, as well as DOC and NOAA policy requirements.
- Ensures the appointment and/or designation of AOs and co-AOs as appropriate and in writing
- Ensure that an adequate and appropriate IT security safeguards are in place for all Staff and Line Office systems.
- Ensure that the Staff and Line Office IT Security Program integrates fully into the Staff and Line Office's enterprise architecture and capital planning and investment control processes.

2.5 INFORMATION OWNER/STEWARD

See DOC Information Technology Security Program Policy, Section 3.3.3, IT Security Roles and Responsibilities.

2.6 PRIVACY ACT OFFICER/FREEDOM OF INFORMATION ACT (FOIA) OFFICER

The NOAA Bureau Chief Privacy Officer (BCPO) works with the DOC Office of Privacy and Open Government's (OPOG) and the Director of OPOG for the development and maintenance of privacy policies, procedures, and guidance essential to safeguarding the collection, access, use, dissemination, and storage of personally identifiable information (PII) and Privacy Act information in accordance with the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Management Act (FISMA), and policy and guidance issued by the President and Office of Management and Budget (OMB), and for the conduct of Privacy Impact Assessments on Information Technology that collects, maintains, or disseminates information in an identifiable form.

NOAA FOIA Officer in addition to responsibilities in NOAA FOIA Office below:

a. approves or denies fee waiver and expedited processing requests; and

b. act as Denial Official, as listed in Appendix B, 15 CFR Part 4 (http://www.corporateservices.noaa.gov/foia/title_15_commerce_and_foreign_trade/appendix-b.html)

NOAA FOIA Office will:

a. review and update FOIA policies, procedures, and guidance in coordination with the Department of Commerce (DOC) FOIA Office and NOAA Office of General Counsel (NOAA GC);

b. offer guidance, advice, and training to NOAA managers, program personnel, and FOIA Liaisons who respond to FOIA requests and provide basic training on NOAA FOIA procedures to all employees;

c. prepare and submit the NOAA contribution of the FOIA Annual Report to Department of Justice and Chief FOIA Officer report, and coordinate the submission of all other FOIA reports requested of NOAA;

d. maintain the NOAA FOIA home page;

e. retain copies of all FOIA requests and files in FOIAonline unless there is a documented strong business need to maintain outside of the web-based tool. Original copies of responsive records, whether released or not, are kept by the FOIA SO/LO Liaison or Action Office;

f. review all FOIA requests received by NOAA, including referrals from DOC and other federal agencies, and assign them to the appropriate FOIA Liaison whose office may have records responsive to the request and, when appropriate, suggest adding a task to additional office(s) at the time of assignment;

g. serve as agency lead for responding to all FOIA requests referred to NOAA from DOC;

h. maintain a list of all NOAA appeals and work with FOIA Liaisons to facilitate the appeals process;

i. function as the primary liaison between NOAA and DOC in resolving any FOIA issues; and

j. read each FOIA response to review metadata for completeness and mark as closed in FOIAonline.

2.7 SENIOR AGENCY INFORMATION SECURITY OFFICER (DIRECTOR, NOAA CYBER SECURITY DIVISION)

The NOAA Senior Agency Information Security Officer (SAISO) is the official responsible for carrying out the NOAA CIO's responsibility under FISMA. The NOAA SAISO shall:

- Issue through the NOAA CIO Council, NOAA-wide IT security policies, architectures, standards, best practices, and guidance that establish a framework for the IT Security program and ensures compliance with applicable federal statutes, regulations, policies and guidance.
- Designate in writing a NOAA OCIO IT Security Officer (ITSO) for the systems directly under the NOAA CIO as the primary AO.

- Serve as the principal advisor to the NOAA CIO on all matters (technical and otherwise) involving the security of the operating unit's IT systems.
- Maintain an accurate inventory of NOAA FISMA Systems.
- Monitor and evaluate the status of NOAA IT Security by overseeing Staff and Line Office security programs and system Authorizations to Operate.
- Track and report on NOAA-wide security posture including but not limited to weaknesses and POA&Ms to implement corrective actions.
- Ensure that all Staff and Line Office ACIOs appoint a Senior Agency Information Security Officer (SAISO)/Cyber Security Program Manager (CSPM) to establish, oversee, and execute the Staff or Line Office Cyber Security Program
- Ensure that the SAISO/PM has the staff and resources necessary to carry out the program in accordance with FISMA.
- Develop, implement, and maintain a computer incident response team within NOAA to ensure that NOAA has the expertise to manage security incidents.
- Maintain a security professional certification in accordance with the current DOC CITR.
- Ensure that an IT Security Awareness Training Program is developed, implemented, and managed, including procedures for all NOAA employees, contractors, and temporary personnel.
- Ensure that a risk management framework program is in place that provides support to authorization process for all NOAA IT systems.
- Ensure that NOAA systems are protected against malicious software through the acquisition and implementation of a NOAA-wide solution(s).
- Serve as the Chair of the NOAA IT Security Committee (ITSC) and hold regularly scheduled meetings to disseminate current information to Staff and Line Office ITSOs on issues relating to Federal, DOC/NOAA IT security law, policies, regulations, guidelines, or concerns.
- Coordinate with the DOC IT Security Program Manager and Critical Infrastructure Program Manager (CIPM), as well as the Office of Security (OSY),Office of the Inspector General (OIG) and NOAA Homeland Security, as appropriate, to address incidents, potential threats, and other IT security concerns.
- Maintain the Cyber Security Division Program web site.

2.8 NOAA IT SECURITY OFFICER

The assigned NOAA IT Security Officer (ITSO) will serve as backup to the Director, NOAA Cyber Security Division, function as the IT security liaison/focal point for Staff and Line Office ITSOs, and perform those duties assigned by the Director in support of the IT Security Program. In the absence of the NOAA ITSO the alternate NOAA ITSO will serve as the NOAA ITSO. The NOAA ITSO will:

- Serve as the central point of contact for the NOAA Cyber Security Division (CSD) and for NOAA security incidents.

- Implement NOAA wide IT security policies, architectures, standards, best practices, and guidance that establish a framework for the IT Security program and ensure compliance with applicable federal statutes, regulations, policies and guidance.
- Ensure all NOAA systems have in place effective and current security documentation, annual assessments, current and tested contingency plans, and current Assessments and Authorizations (A&As); via Staff and Line Office SAISOs/ITSOs
- Ensure the development of IT security policies, architectures, standards, best practices, and guidance which contributes to open, standard, scalable, interoperable, yet secure IT environments at the appropriate levels.
- Ensure 100% organizational participation in the NOAA IT Security Awareness Course (SAC). Review and monitor Staff and Line Office role-based security training programs to ensure compliance to the current DOC CITR.
- Ensure an inventory of FISMA systems in CSAM is maintained and coordinated with DOC to track compliance with DOC/NOAA IT Security Program requirements and provide updated inventories to the Director, NOAA Cyber Security Division as required.
- Advise NOAA SAISO of technological advances in IT security which can be used on an organizational scale and provide reduced cost for security efforts.
- Develop and track entity level remedial actions to mitigate risks in accordance with the DOC policies and procedures (e.g.: DOC CITR for plans of actions and milestone (POA&Ms) management).
- Recommend and adjudicate IT Security policy questions and requests for interpretation. Provide IT security guidance and technical assistance to the organizational IT security community.
- Disseminate information concerning potential security threats to NOAA IT information Staff and Line Office SAISOs and ITSOs, Network/System Administrator (N/SA) and IT Security community.
- Serve as directed on various committee and working groups and attend regularly scheduled meetings to disseminate current information on issues relating to federal, DOC/NOAA IT security law, policies, regulations, guidelines or concerns.
- Maintain a security professional certification in accordance with the current DOC CITR.

As appropriate, the ITSO may also take on the responsibilities of the Information System Security Engineer and Information Security Architect roles, as described in NIST SP 800-37.

Staff and Line Office ITSOs will serve similar roles, functions and responsibilities of the NOAA ITSOs within their respective offices.

2.9 LINE OFFICE SENIOR AGENCY INFORMATION SECURITY OFFICER/CYBER SECURITY PROGRAM MANAGER

The assigned Line Office Senior Agency Information Security Officer (SAISO)/Cyber Security Program Manager (CSPM) develops and oversees the LO cyber security program and manages staff of ITSOs who execute the LO cyber security program that consists of the responsibilities outlined below. In the absence of the Line Office SAISO/CSPM the Line Office ITSO will fill the role. The Line Office SAISO/CSPM will:

- Implement a risk-based security program.
- Serve as the AODR for unclassified Line Office information systems.
- Serve as the central point of contact for the Line Office IT Security program and for Line Office security incidents.
- Develop and implement Line Office IT security policies, architectures, standards, best practices, and guidance that establish a framework for the IT Security program and ensure compliance with applicable federal statutes, regulations, policies and guidance
- Ensure all Line Office systems have in place effective and current security documentation, annual assessments, current and tested contingency plans, and current Authorization to Operate (ATO).
- Develop IT security policies, architectures, standards, best practices, and guidance which contribute to open, standard, scalable, interoperable, yet secure IT environments at the appropriate levels.
- Ensure 100% participation of NOAA personnel in the NOAA IT Security Awareness Course.
- Review and monitor security training programs to ensure compliance to DOC CITR-006.
- Ensure that an inventory of FISMA systems in CSAM is maintained and coordinated with DOC to track compliance with DOC/NOAA IT Security Program requirements and provide updated inventories to the Director, NOAA Cyber Security Division as required.
- Advise appropriate levels of management of technological advances in IT security which can be used on an organizational scale and provide reduced cost for security efforts.
- Develop and track program level remedial actions to mitigate risks in accordance with the DOC CITR for plans of actions and milestone (POA&Ms) management.
- Recommend and adjudicate IT Security policy questions and requests for interpretation. Provide IT security guidance and technical assistance to the organizational IT security community.
- Ensure dissemination of information concerning potential security threats to Line Office IT information system owners, Network/System Administrator; (N/SA) and IT Security community.
- Serve as directed on various committees and working groups and attend regularly scheduled meetings to disseminate current information on issues relating to federal, DOC/NOAA IT security law, policies, regulations, guidelines or concerns.
- Maintain a security professional certification in accordance with DOC CITR-006.
- Serve as a voting member of the NOAA IT Security Committee and attend regularly scheduled meetings to obtain current information on issues relating to federal, DOC/NOAA IT security law, policies, regulations, guidelines or concerns.

As appropriate, the SAISO may also take on the responsibilities of the Information System Security Engineer and Information Security Architect roles, as described in NIST SP 800-37.

Line Office SAISOs/ITSOs will serve similar roles, functions and responsibilities of the NOAA ITSOs within their respective offices.

2.10 NOAA IT SECURITY COMMITTEE

The National Oceanic and Atmospheric Administration (NOAA) Information Technology Security Committee (ITSC) leads the NOAA wide development, implementation and maintenance of the enterprise IT Security Program. This is accomplished through the development and promulgation of policies and guidance, coordination of IT security activities, and strategic planning across all line offices. The ITSC also researches and develops recommendations to the NOAA Chief Information Officer's (CIO) Council on IT security issues.

The NOAA IT Security Committee is made up primarily of the NOAA SAISO/CSMP, Director of Cyber Security, NOAA ITSO, all Line Office SAISOs, all Line Office ITSOs, and/or their alternates.

The NOAA ITSC will:

- Provide governance for the NOAA IT Security Program.
- Recommend NOAA-wide policies to the NOAA CIO Council.
- Identify activities and specific coordination to be proposed for the DOC IT
- Facilitate an open forum for the sharing and discussion of IT security issues and concerns.
- Review enterprise-wide IT security products and services.

2.11 AUTHORIZING OFFICIAL

An Authorizing Official (AO) must be at least a senior official or executive with the authority to formally assume responsibility and risk for operating an information system and associated data at an acceptable level of risk.

Within NOAA, the NOAA CIO will serve as the Co-Authorizing Official (Co-AO) for all high systems. For all low and moderate systems, the Line Office Assistant CIO serves as Co-AO as delegated by the NOAA CIO. A Co-AO is necessary when the AO is not in the chain of command of the NOAA CIO.

The NOAA CIO delegates AO authority to the LO AA (or Deputy AA) with the privilege of delegating that authority further within the LO the LO AA (or Deputy AA) being required to notify the NOAA CIO in writing of any re-delegation. For high-impact systems, the AO must be a member of the Senior Executive Service (SES). The AO must ensure that adequate resources are allocated to A&A activities from system security categorization to post-authorization continuous monitoring.

The AO will:

- Execute the budget and business operations of the information systems within their area of responsibility.
- Collaborate with the Co-AO for an acceptable level of risk to operations, assets, or individuals by executing risk-based decision supported by an ATO. The ATO decision must be based on an annual assessment that includes the key components as outlined in NIST SP 800-37.
- Appoint a system owner (SO) for each IT system in concert with the Co-AO, as appropriate, and in writing.

- Review all A&A packages for compliance to requirements. Ensure risk acceptances are valid and justified.
- Approve the FIPS 199 security categorization, FIPS 200 Security Control Selection, documentation of security controls baseline tailoring risk acceptance, and any other Risk Acceptance documentation, including acceptance of risk, and the Authorization to Operate memoranda and all ATO supporting documentation for those systems for which they are responsible. AOs also are required to sign any external agreement such as an ISA or MOU/A. An AO may also approve the system's security plan (SSP) and other key documents, but may delegate this approval to the AO Designated Representative (AODR).
- For high impact systems, the Co-AO and AO must both approve the delegation of risk acceptance to the AODR.

2.12 CO-AUTHORIZING OFFICIAL

Within NOAA, the NOAA CIO will serve as the Co-Authorizing Official (Co-AO) for all high systems. For all low and moderate systems, the Line Office Assistant CIO serves at Co-AO as delegated by the NOAA CIO. This role provides oversight and serves to provide a consistent application of risk management and tolerance principles across NOAA and within individual Staff and Line Offices. This role is not the same as a primary AO, and is not required to be operationally involved throughout the day to day management and decision making for an IT system.

The Co-AO along with the primary AO, a Co-AO must agree and sign the following key security documents including: the FIPS 199 Security Categorization, FIPS 200 Security Control Selection and any Risk Acceptance documentation, such as an acceptance of risk, and the Authorization to Operate memoranda and all ATO supporting documentation.

2.13 COMMON CONTROL PROVIDER

The NOAA common control provider is the NOAA OCIO IT Security Office, which is responsible for the development, implementation, assessment, and monitoring of common control designations for NOAA systems. Please see Section 3.3.8 Common Control Provider in the *DOC ITSPP*, 2014.

2.14 NOAA IT RISK MANAGEMENT OFFICER

The NOAA IT Risk Management Officer (ITRMO) is appointed by the NOAA CIO.

The NOAA IT Risk Management Officer helps ensure:

I. Risk-related considerations for individual information systems, to include authorization decisions, are viewed from an NOAA-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and

II. Managing information system-related security vulnerabilities and risks is consistent across NOAA, reflects NOAA risk tolerance and is considered along with other types of risks in order to ensure mission/business success.

The ITRMO coordinates with the senior leadership of NOAA Cyber Security Division to:

- Provide a comprehensive, NOAA-wide, holistic approach for addressing IT Security risk an approach that provides a greater understanding of the integrated operations of the organization.
- Identify and manage information security risks to achieve mission objectives.
- Develop an IT Security risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole.
- Facilitate the sharing of IT Security risk-related information among authorizing officials and other senior leaders within the organization.
- Provide oversight for all IT Security risk management-related activities across the organization (e.g., security categorizations) to ensure consistent and effective risk acceptance decisions.
- Ensure authorization decisions consider all factors necessary for mission and business success.
- Provide a NOAA-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation.
- Ensure the shared responsibility for supporting NOAA mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities.
- Identify the organizational IT Security risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

2.15 NOAA COMPUTER INCIDENT RESPONSE TEAM

The Director, NOAA Cyber Security Division manages the NOAA Computer Incident Response Team (N-CIRT) that serves as the focal point for NOAA on all matters relating to any type of IT security-related incidents or violations. The N-CIRT has authority to make all decisions during the incident response process. The N-CIRT will:

- Coordinate all reported incidents with the DOC IT Security Program Manager (ITSPM), DOC Office of Inspector General (OIG), DOC Office of Security (OSY), Federal Bureau of Investigation (FBI), and Department of Homeland Security (DHS) US Computer Emergency Readiness Team (US-CERT).
- Establish procedures for reporting and receiving information regarding incidents affecting NOAA. This will include establishing a hotline for reporting, tracking, and coordinating incident data, and maintaining a database of incidents to analyze and assess overall threats.
- Provide incident response services to NOAA as defined in NIST SP 800-61, DOC policy, federal policy, and US-CERT Concept of Operations.
- Perform and coordinate organizational computer forensic information gathering as required in support of legal activities for NOAA.

- Monitor the resolution of all incidents and prescribe corrective actions pursuant to incident containment and recovery.
- Provide other organizational support services that may include (in a directed manner) provisions for the Vulnerability Monitoring and Regression Testing activity that includes an ad-hoc end-user liaison function, tools, education, auditing, consulting, product evaluation, and security testing in product evaluation.
- Provide the organizational community guidance and technical assistance on NOAA anti-virus software.
- Assist in the development of policy and guidance for N-CIRT and N/SAs.
- Participate in NOAA ITSC meetings.
- Monitor NOAA campuses for wireless networks. Wireless networks found to be in noncompliance will be reported to the Staff and Line Office ITSO, the relevant Authorizing Official (AOs), the ACIO for the Line Office, or, as appropriate, the NOAA Cyber Security Division or NOAA CIO office for action.

2.16 SECURITY OPERATION CENTER

The NOAA Security Operation Center (SOC) serves as a central clearinghouse for all reported organizational incidents. The SOC will provide appropriate security alerts, bulletins, and other security related material as well as disseminate to all NOAA IT Systems Owners and Managers prompt advisories of system threats, operating system vulnerabilities, and tracking information related to reported incidents, trends, and impacts.

2.17 CERTIFICATION AGENT/SECURITY CONTROL ASSESSOR/CERTIFIER

The Security Control Assessor (SCA) (also referred to as “Certifier” or “Certification Agent”) is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). SCAs also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. In addition to the above responsibilities, Security Control Assessors prepare the final security assessment report containing the results and findings from the assessment.

For assessments that require independence (moderate and high systems), the AO or AODR must approve the designation of the SCA. For these systems, the SCA will not be in the same chain of command as the primary SO but is in the same chain as the primary AO.. For control assessments that do not require independence (low systems), the SO may appoint the SCA.

The SCA role may be filled by a variety of methods. A Staff and Line Office may choose to contract out to a vendor to obtain the services. Or they may use a NOAA Staff and Line Office assessment team Staff and Line Office that is not within the same chain of command as the

primary AO Official of the system under assessment. The SCA lead must comply with the professional certification requirements of DOC CITR-006.

2.18 INFORMATION SYSTEM OWNER

As described in the NIST SP-800-37, Appendix D.4, the Information System Owner (SO) (System Owner/Project Manager) has many responsibilities in addition to the day-to-day operation and maintenance of their systems as well as direct oversight of the system/network administrators and operations staff. The information SO is the NOAA or Staff and Line Office manager responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system, and relies on the assistance and advice of the appropriate Staff and Line Office SAISO/ITSO and other IT staff in the implementation of the following security responsibilities. For IT systems (classified and/or unclassified) under their responsibility, System owners will:

- Ensure that security considerations are included in the systems lifecycle management.
- Develop and maintain the system's SSP and perform continuous monitoring to ensure that the system is deployed and operated at an acceptable risk level in accordance with the AO-approved security controls baseline.
- Develop and maintain specific procedures for implementing security policies and requirements for systems under their preview.
- In coordination with the information owner/steward, the SO will decide who has access to the system (and with what types of privileges or access rights) and ensure system users and support personnel receive the requisite security awareness training (e.g., instruction in rules of behavior) and role-based training.
- Based on guidance from the AO or AODR, the SO will inform appropriate organizational officials of the need to conduct the security authorization, ensure the necessary resources are available for the effort, and provides the required information system access, information, and documentation to the SCA as agreed in the Security Assessment Plan.
- Assemble the security authorization package, recommend draft POA&Ms or risk acceptance, and submit the package to the authorizing officials for approval.
- Ensure all controls are effective and operating as intended, and for those with POA&Ms, ensure actions are taken and POA&Ms are closed on schedule.
- Ensure system users, system administrators and ISSOs receive system specific security awareness training and education as appropriate and acknowledge acceptance of responsibility as required.
- Ensure personnel designated in the SSP control AT-3 as having a role with significant IT security responsibilities comply with DOC CITR-006.
- Maintain an updated list of hardware and software inventory operated/used by the system.
- Ensure that IT system security documentation such as contingency plans are maintained and tested as required.
- Routinely perform security impact analysis as part of system configuration changes ensuring the awareness of the system's security posture.

- Appoint an ISSO, and if necessary an Alternate ISSO, in writing and ensure the ISSO maintains a professional certification as required by DOC-CITR-006.
- Identify, in writing, a(n) Account Manager(s)/Network and System Administrators, responsible for the creation, deletion and change of user IDs.

2.19 INFORMATION SYSTEM SECURITY OFFICER

Each Information System Security Officer (ISSO), supported by an Alternate ISSO if appropriate, will design, implement, and maintain IT system security controls continuous monitoring program consistent with DOC/NOAA, and government-wide laws, regulations, policies, procedures, and standards. The ISSO implements controls and executes the Program as required by DOC, NOAA, and SO/LO policies. The ISSOs are appointed in writing by the SO and must implement the system-level controls and maintain system documentation. The ISSO is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information system owner. The ISSO also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The ISSO has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned by the SO the responsibility for the continuous monitoring of day-to-day security operations of a system. This responsibility may also include, but is not limited to, physical and environmental protection, personnel security, incident handling, and security training and awareness. The ISSO may be called upon to assist in the development of the security policies and procedures and to ensure compliance with those policies and procedures. In close coordination with the Information System Owner, the ISSO often plays an active role in the monitoring of a system and its environment of operation to include developing and updating the security plan, managing and controlling changes to the system, and assessing the security impact of those changes.

The ISSO will:

- Advise the System Owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e., life cycle management).
- Assist in the determination of an appropriate level of security commensurate with the level of security categorization of the system.
- Assist in the development and maintenance of security and contingency plans for all FISMA ID systems under their responsibility.
- Participate in security impact analysis for system changes and annually review the security categorization of the system, risks, and risk mitigation strategies.
- Serve as the point of contact for all security incidents within their area of responsibility and reports as appropriate to the NOAA Computer Incident Response Team (N-CIRT). Handles and investigates incidents in cooperation with and under direction of the Staff and Line Office ITSO and N-CIRT.
- Participate in vulnerability scanning and penetration testing of systems/networks.
- Not function as the network and/or systems administrator for any Moderate- or High-impact system they are assigned to as the ISSO unless a waiver with justification is

requested from the Staff and Line Office ACIO. Separation of duties dictates that an ISSO cannot be a systems administrator for the same IT system.

- Ensure that all user accounts are disabled within 24 hours of notification of user's separation from employment and immediately for individuals being separated for adverse reasons.
- Monitor and review system security policy, practices, and procedures at least annually, and update as necessary.
- Ensure the security of all interfaces between the IT system and external systems by developing, maintaining, and enforcing interconnection agreements (ISA, SLA, MOU, and MOA).
- Maintain a security professional certification as specified by DOC CITR-006.

2.20 INFORMATION SECURITY ARCHITECT

The Information Security Architect is an individual, group, or organization within a Staff or Line Office who will ensure the selection of security controls is consistent with the enterprise architecture, including reference models and segment and solution architectures. They will ensure that the information security requirements necessary to protect NOAA's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. The information security architect will serve as the liaison between the enterprise architect and the information system security engineer and also coordinate with information system owners, common control providers, and information system security officers on the allocation of security controls as system-specific, hybrid, or common controls. In addition, the information security architect, in close coordination with information system security officers, will advise authorizing officials, chief information officers, senior information security officers, and the risk executive (function), on a range of security-related issues including, for example, establishing information system boundaries, assessing the severity of weaknesses and deficiencies in the information system, plans of action and milestones, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

The ITSO/SAISO may also take on the responsibilities of the Information Security Architect.

2.21 INFORMATION SYSTEM SECURITY ENGINEER

The Information System Security Engineer is an individual, group, or organization that will conduct information system security engineering activities including:

- Provide advice on the continuous monitoring of the information system
- Provide advice on the impacts of system changes to the security of the system
- Participate in the configuration management process
- Participate in any acquisition/development activities that are required to implement a system change
- Implement approved system changes

The ITSO/SAISO may also take on the responsibilities of the Information System Security Engineer.

2.22 NETWORK/SYSTEM ADMINISTRATOR (N/SA)

Each system and or network(s) within NOAA will have administrators to perform IT security implementation through installation and configuration of IT resources. The N/SAs will:

- Take action for specific aspects of system security, such as adding and deleting user accounts as authorized by the system owner or ISSO, patching systems, implementing secure configurations as prescribed in the system security plans, and normal operations of the system in keeping with job requirements.
- Implement DOC, NOAA, and Staff and Line Office security policies, procedures, and guidelines on local systems and networks.
- Assist in the development and maintenance of security and contingency plans for FISMA ID systems under their responsibility.
- Participate in security impact analysis of system configuration changes and in the annual review of the system security categorization , risks, and mitigation strategies.
- Participate in continuous monitoring assessments of system safeguards and program elements and in annual authorization and assessment of the system.
- Evaluate proposed technical security controls to assure proper integration with other system operations.
- Identify requirements for resources needed to effectively implement technical security controls.
- Assures the integrity of technical security controls.
- Report all incidents to the system ISSO and system owner and assist in the investigation of incidents as directed.
- Develop system administration and operational procedures and manuals.
- Evaluate and develop procedures that assure proper integration of service continuity with other system operations.
- Know which systems or parts of systems for which they are directly responsible (e.g., network equipment, servers, LAN, etc.).
- Know the sensitivity of the data they handle and take appropriate measures to protect it.
- Will not function as the ISSO on any system he/she functions as the system administrator unless there has been security baseline controls tailoring to the AC-5 control requirements, with justification is requested from the Staff and AOs/Line Office ACIO.
- Maintain the system(s) baseline(s), coordinating changes with the ISSO, SO and Change Control Board (CCB) and obtaining approval for baseline deviations.

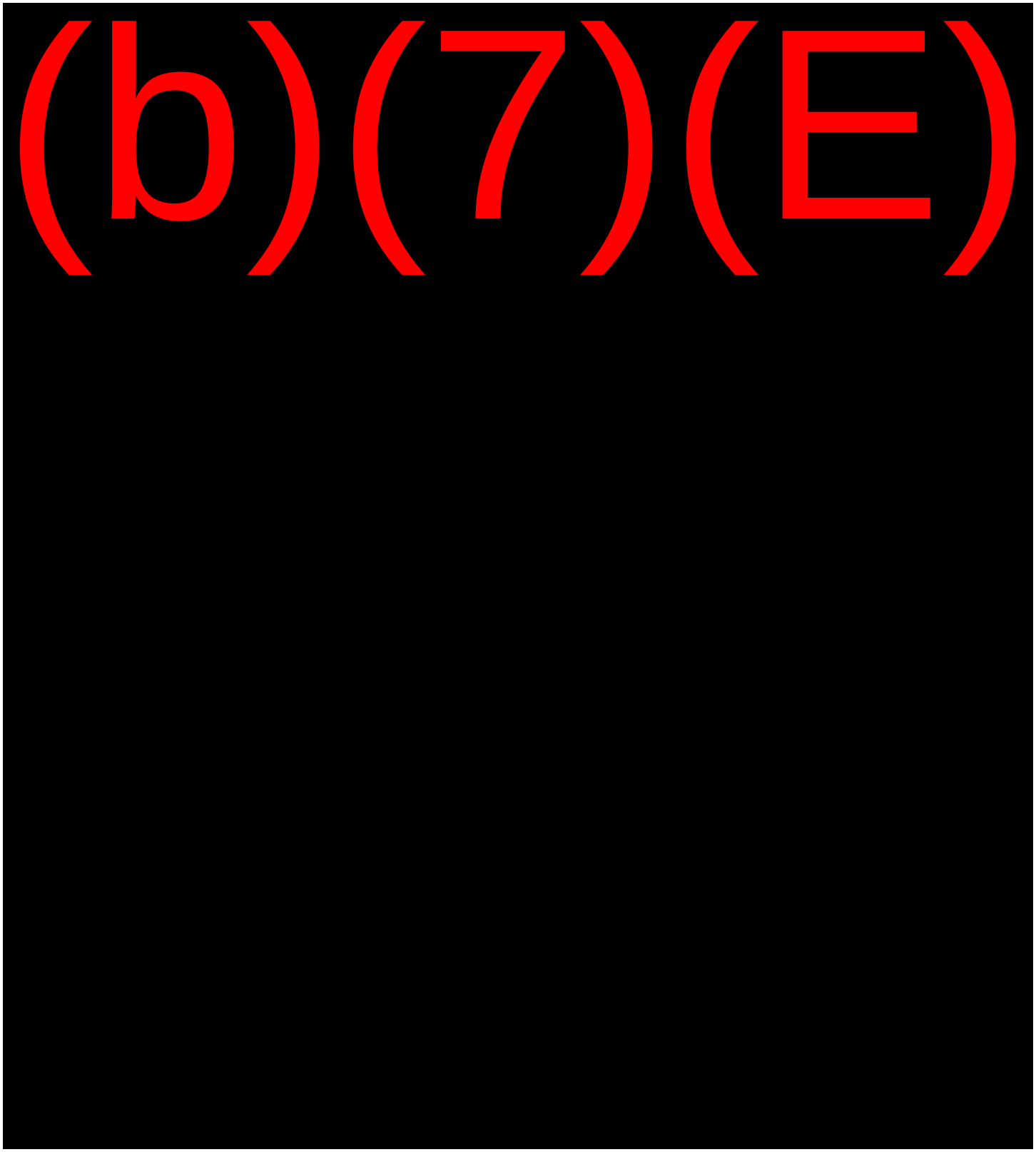
2.23 EMPLOYEES, CONTRACTORS AND TEMPORARY PERSONNEL (END USERS)

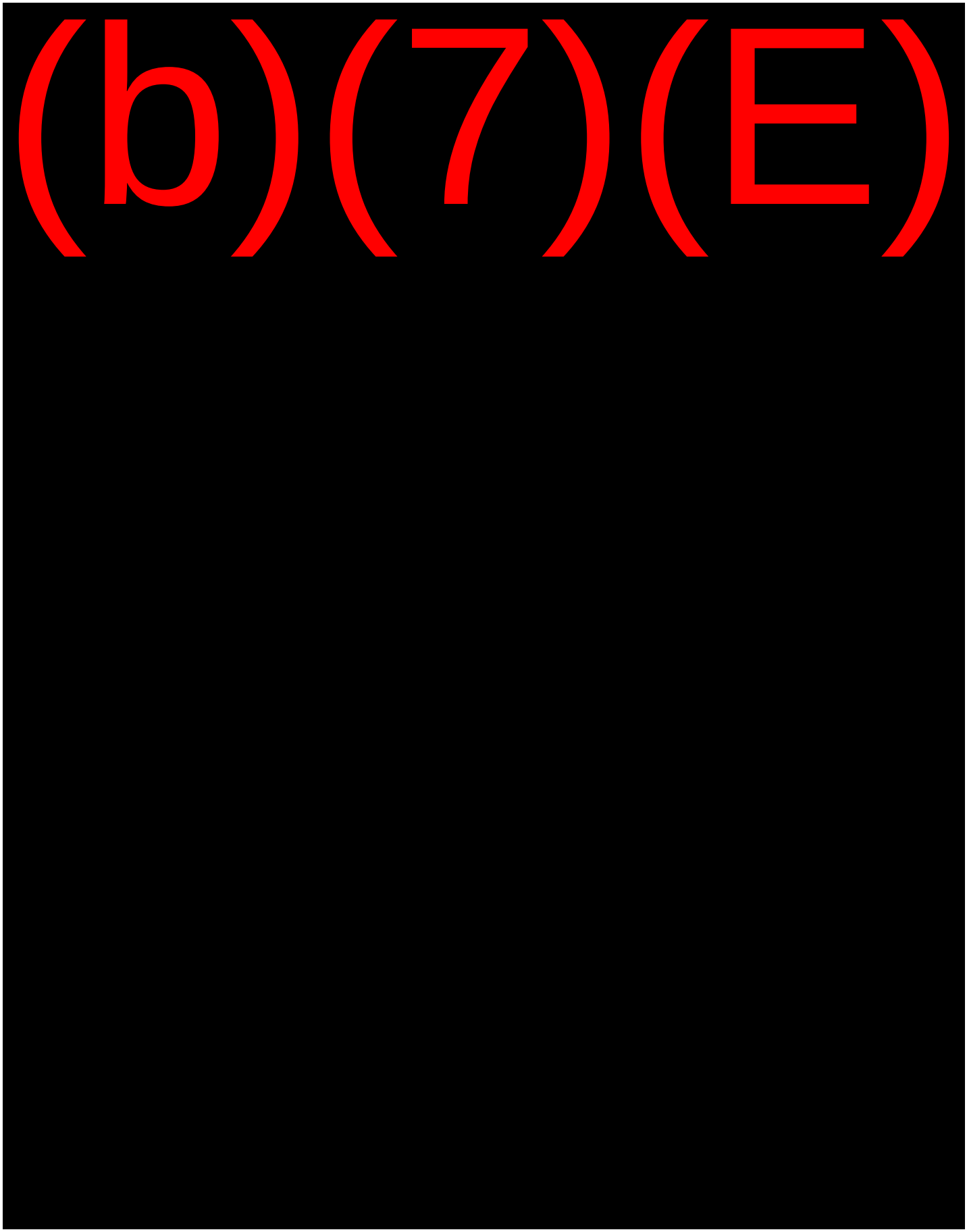
Each employee, including contractors and temporary personnel, is responsible for the adequate protection of IT resources based on the security category of the information within their control or possession, e.g., laptops, devices, passwords. End users will also be vigilant in performing necessary security procedures in order to maintain the confidentiality, integrity, and availability of the information. End users will:

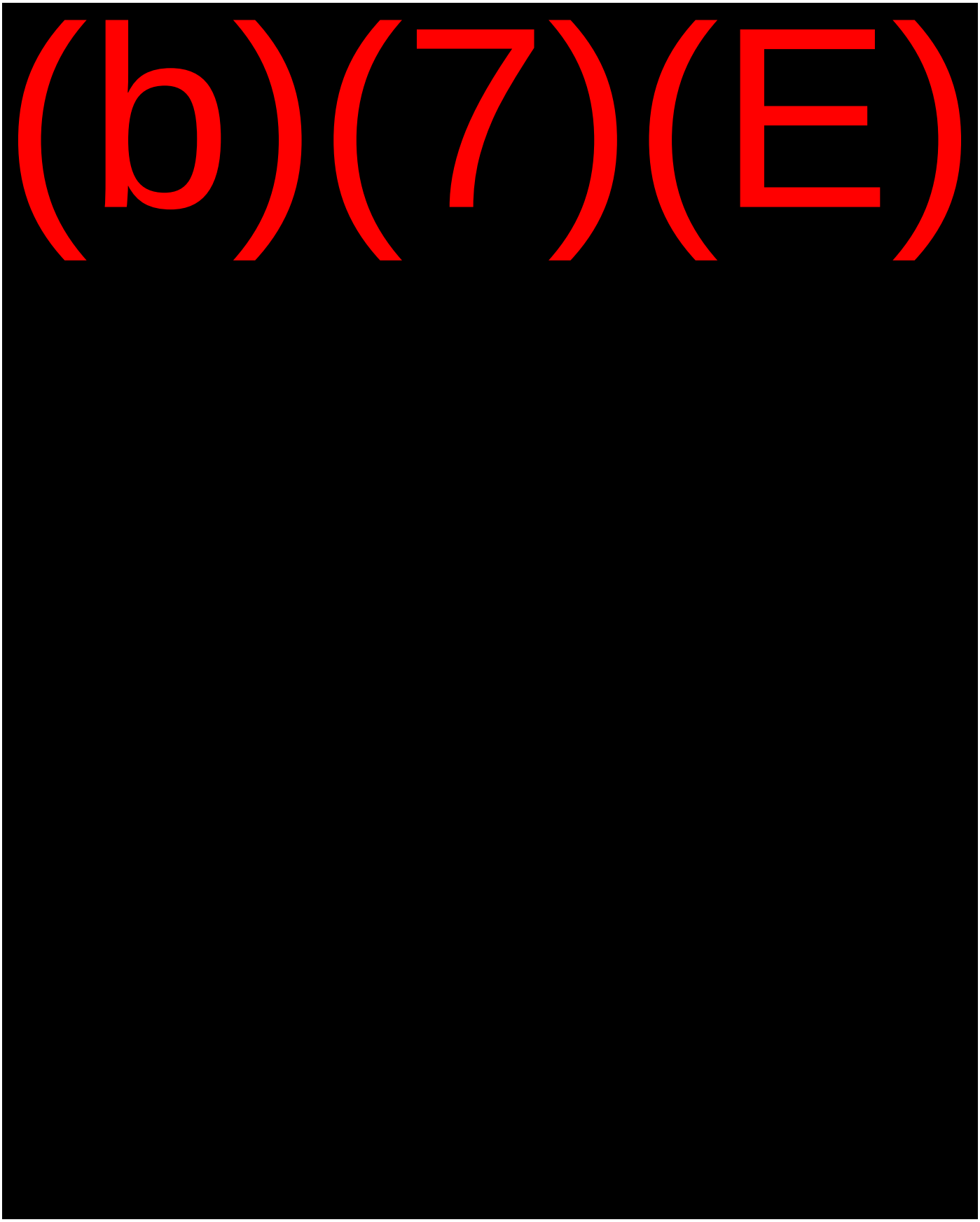
- Participate in the IT Security Awareness Program by completing the NOAA IT security awareness training annually as required;
- Follow installation procedures and requirements for the protection of information resources to which access is granted;
- Report IT security incidents according to established policies and in a timely manner to appropriate managers or supervisors and to the ISSO and cooperate in the investigation of incidents;
- Comply with all NOAA security program policy, passwords, rules of behavior, and appropriate use policy requirements regarding use or abuse of operating unit IT resources; and
- Protect sensitive information and data that resides on mobile devices and/or portable storage devices (USB drives, CD-ROMs, etc.) that are under the users control.

SECTION 3: SECURITY POLICIES

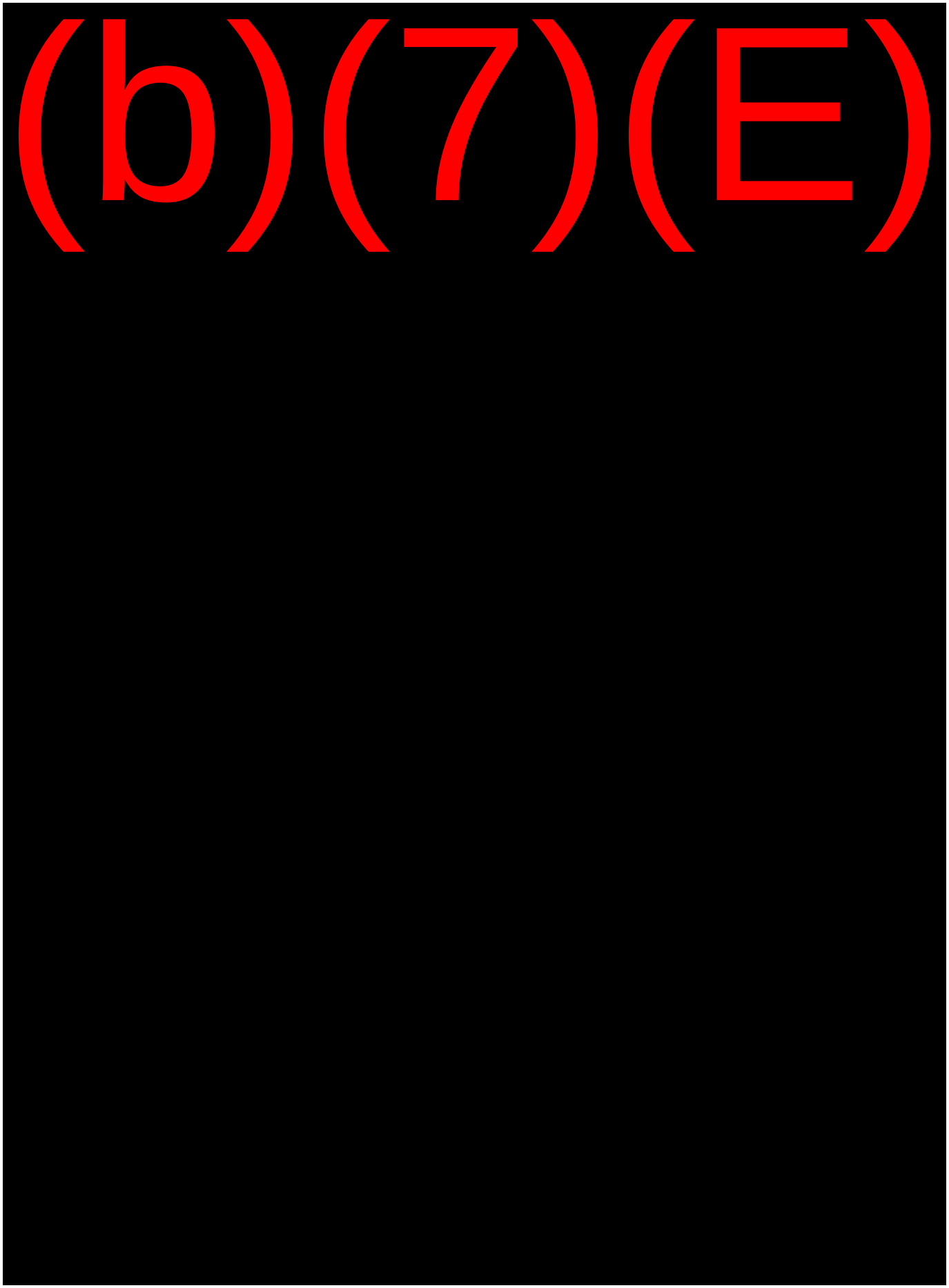
This page is intentionally blank.

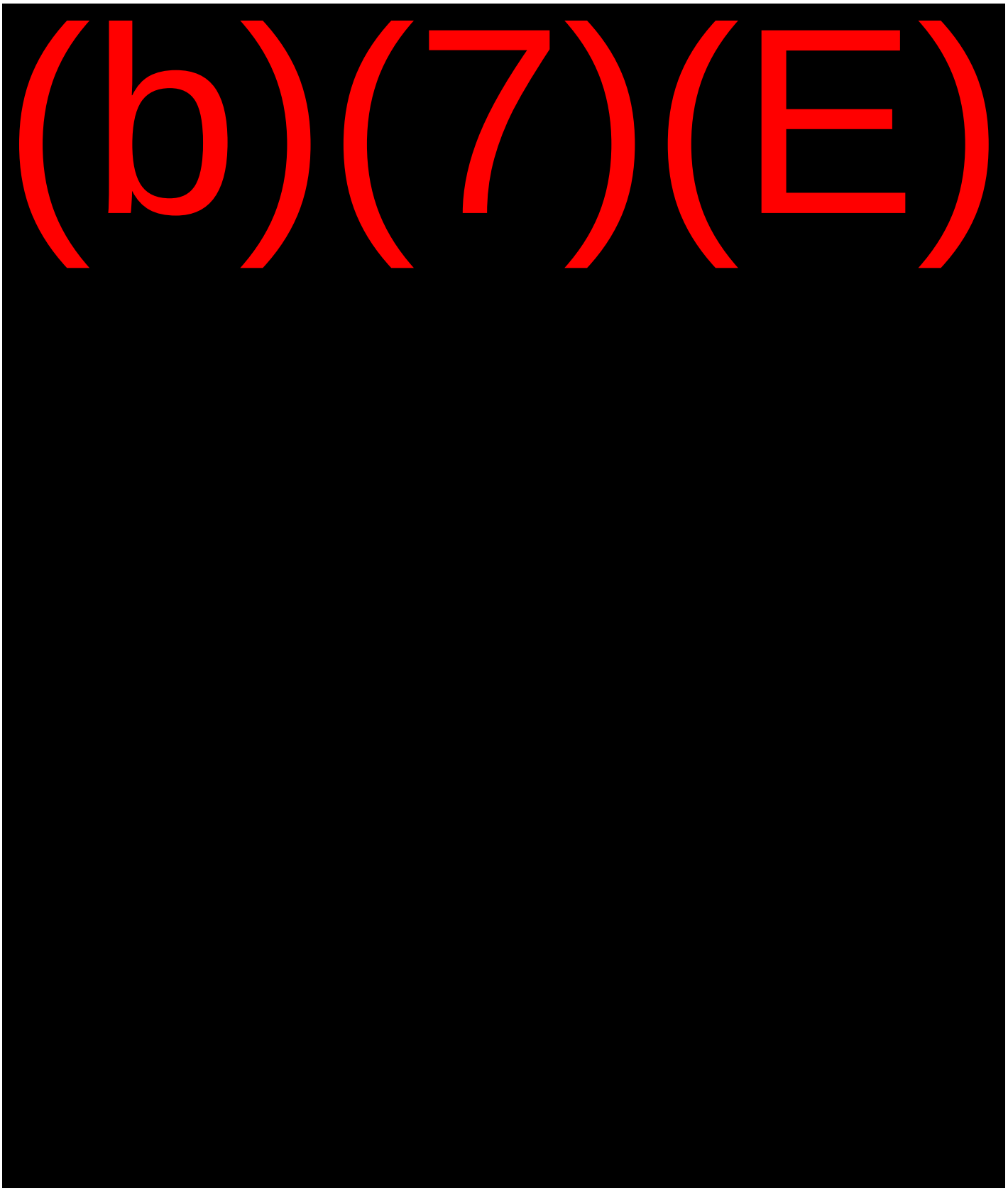

(b)(7)(E)

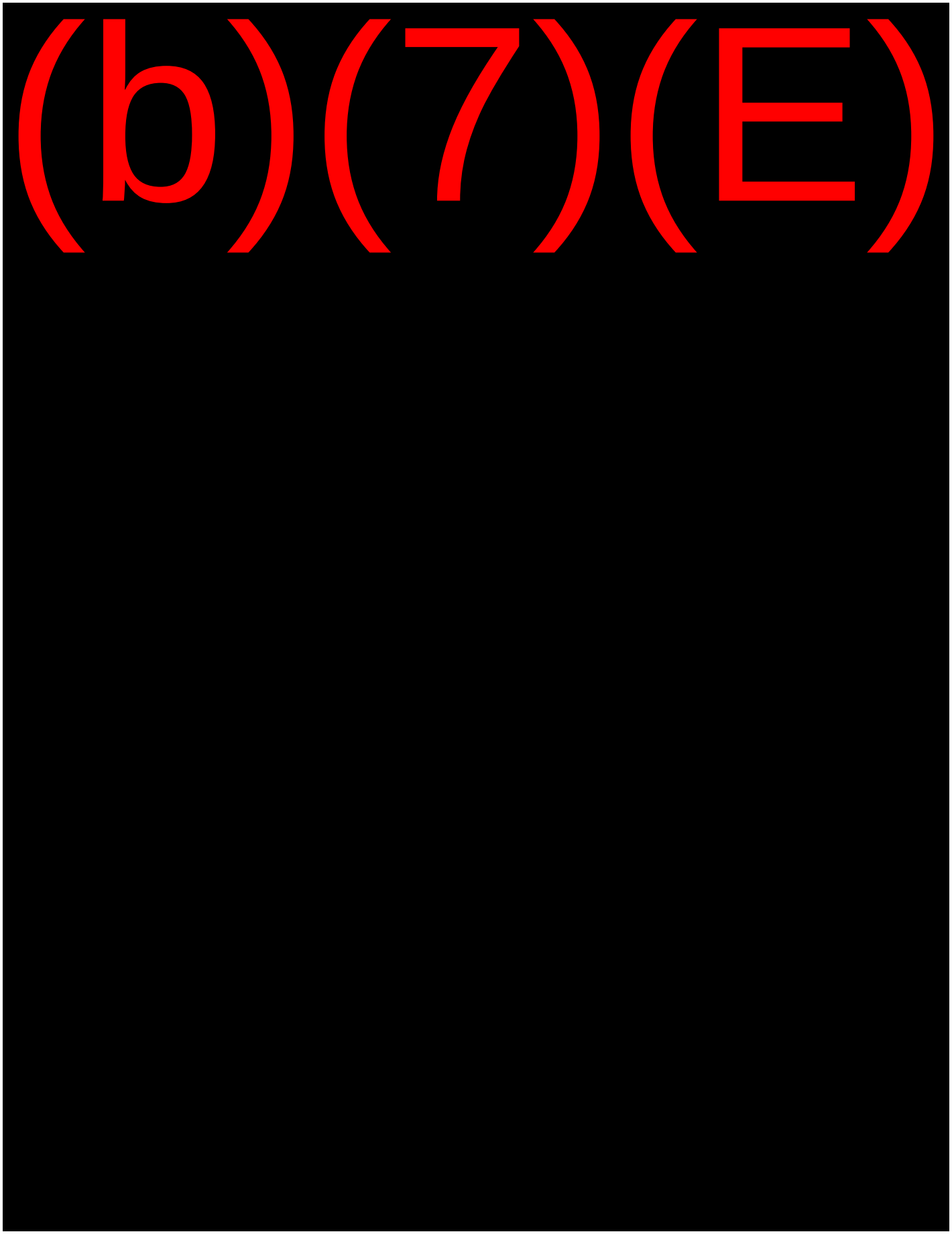

(b)(7)(E)

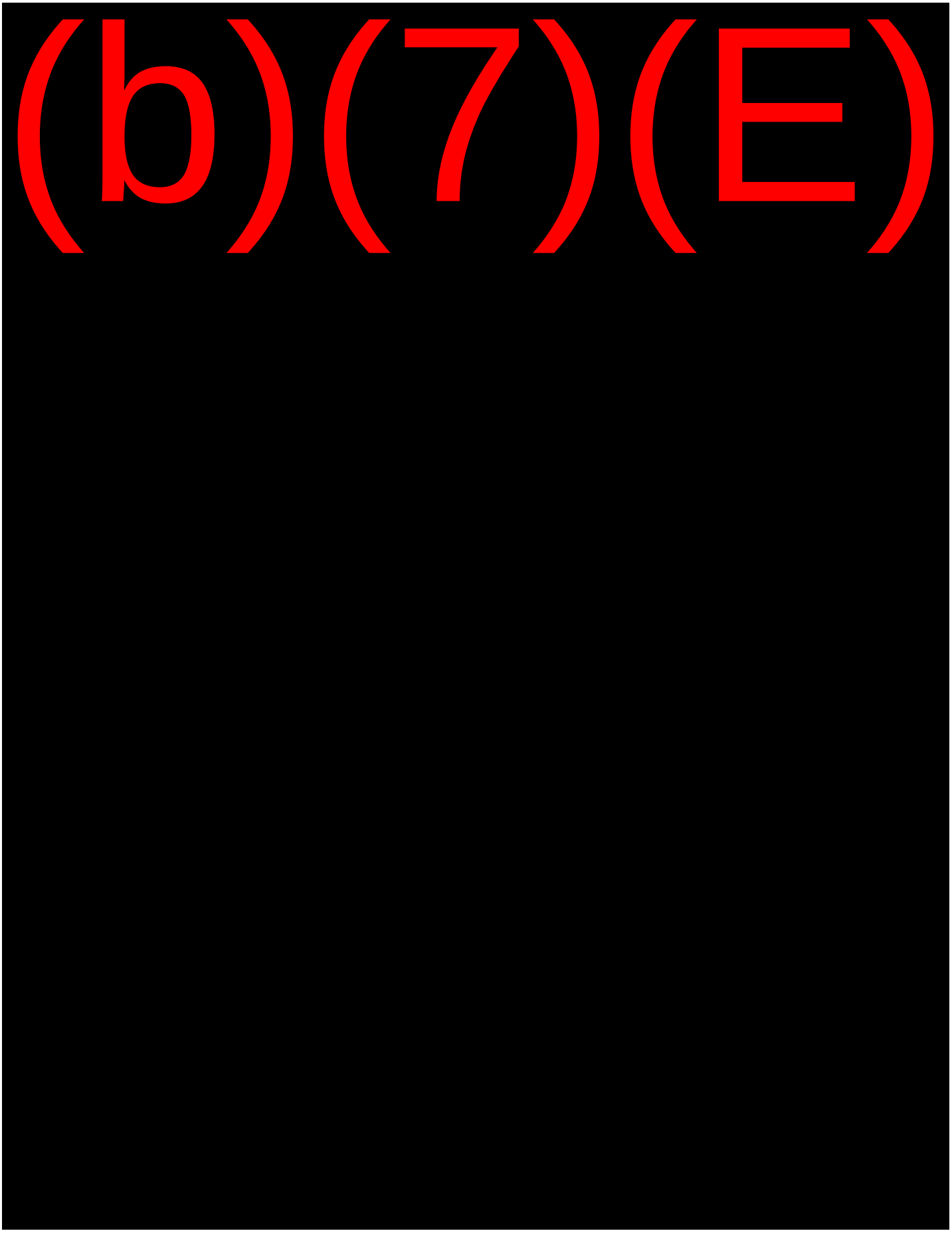

(b)(7)(E)

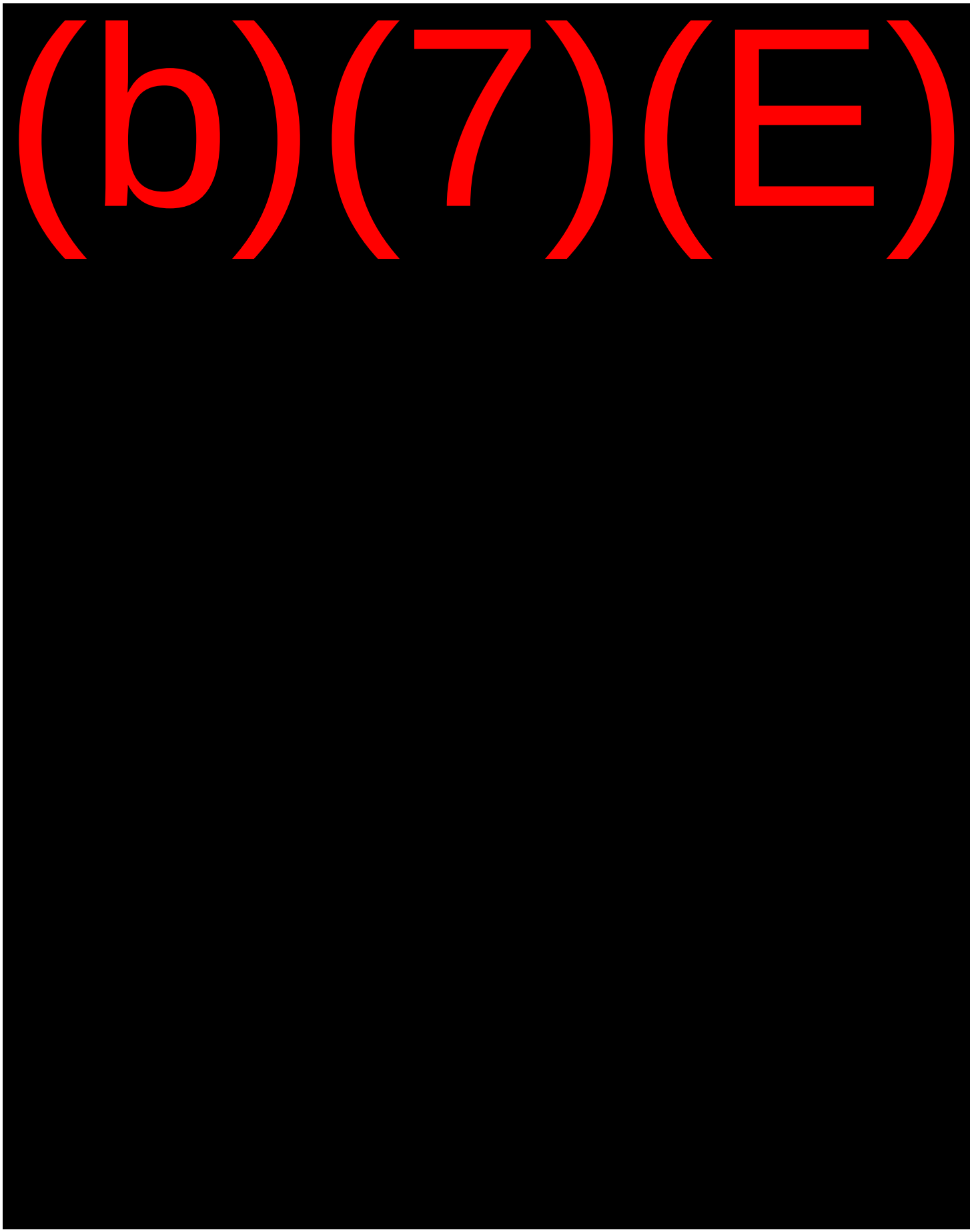

(b)(7)(E)


(b)(7)(E)

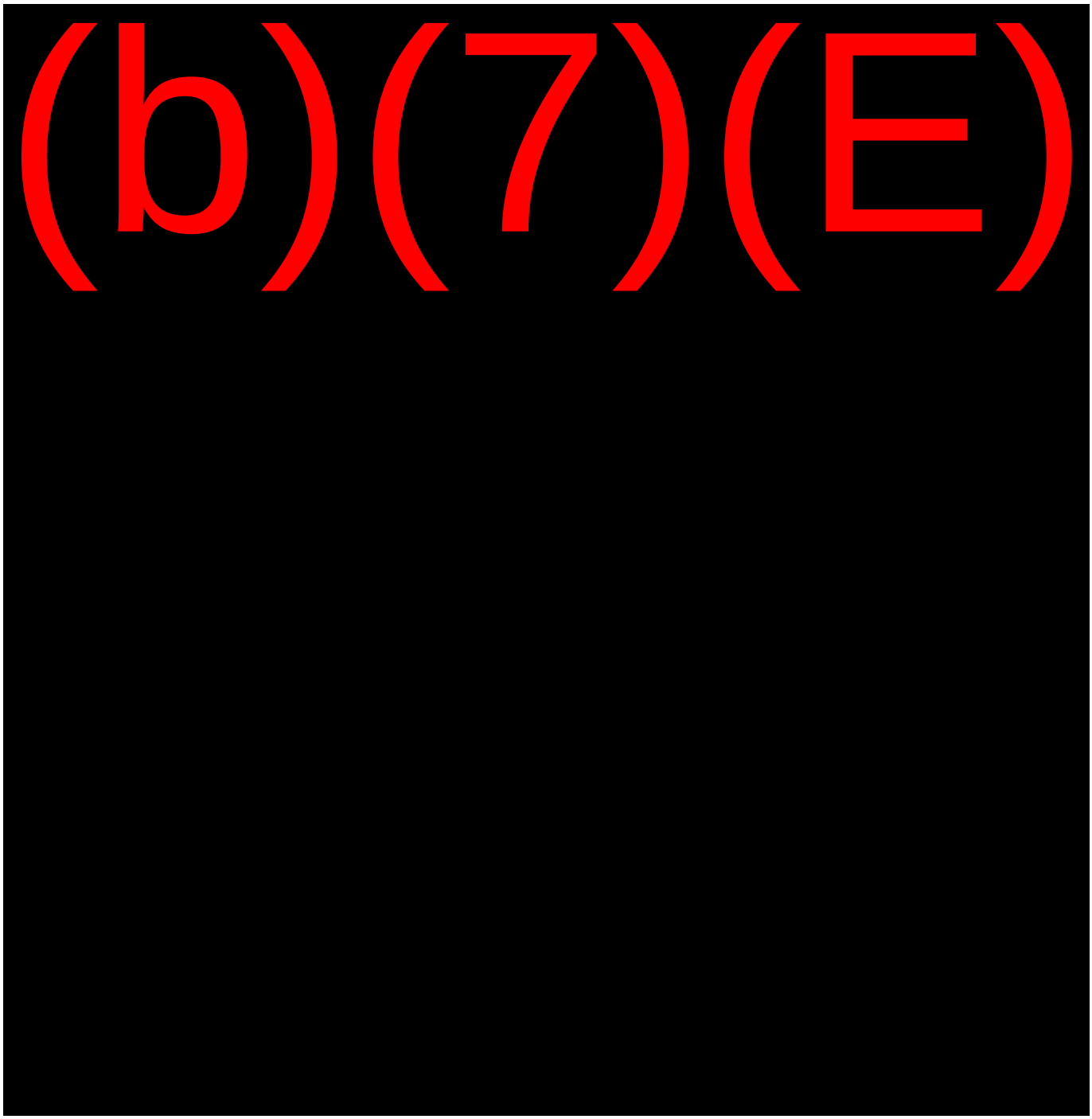

(b)(7)(E)


(b)(7)(E)

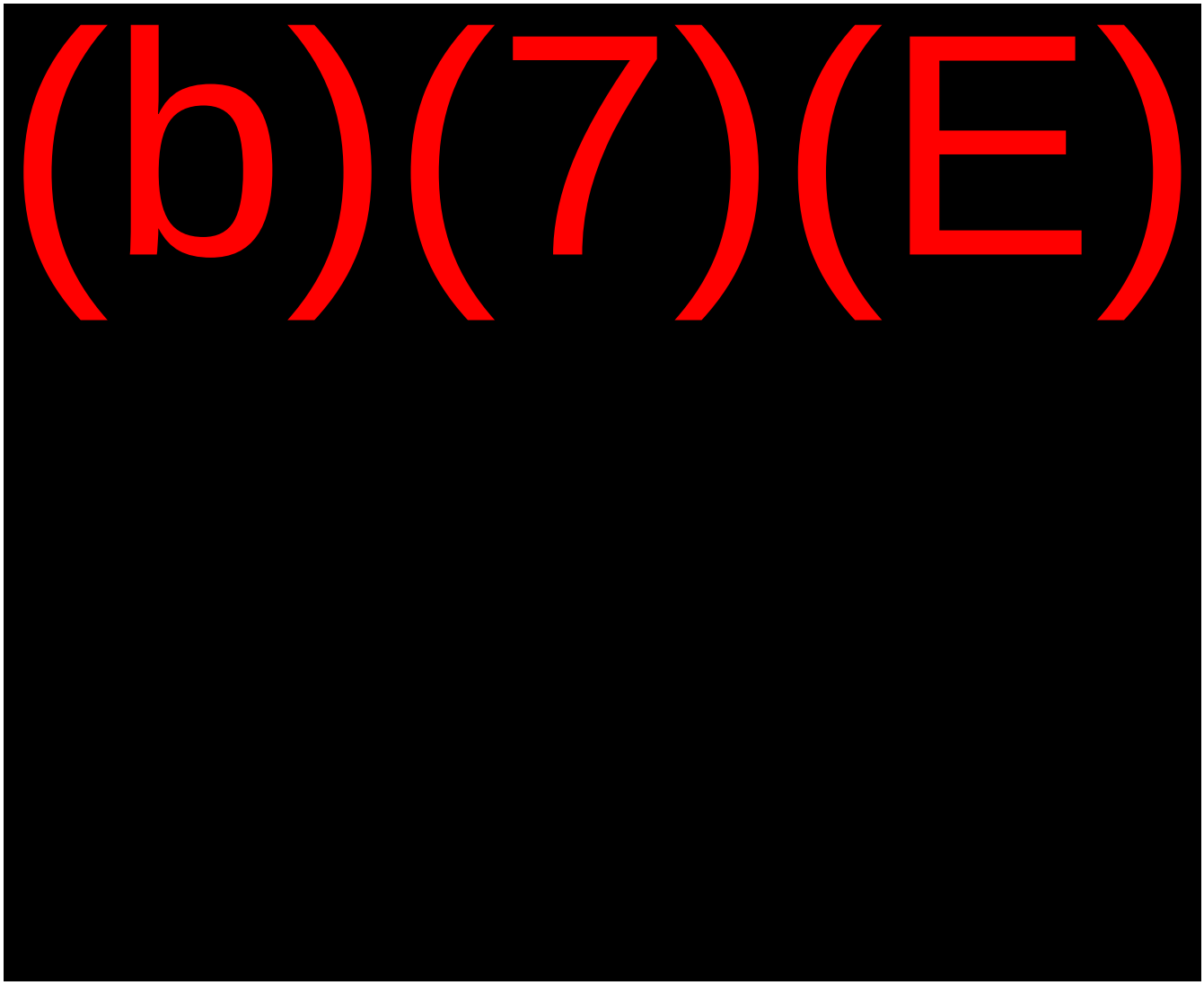

(b)(7)(E)

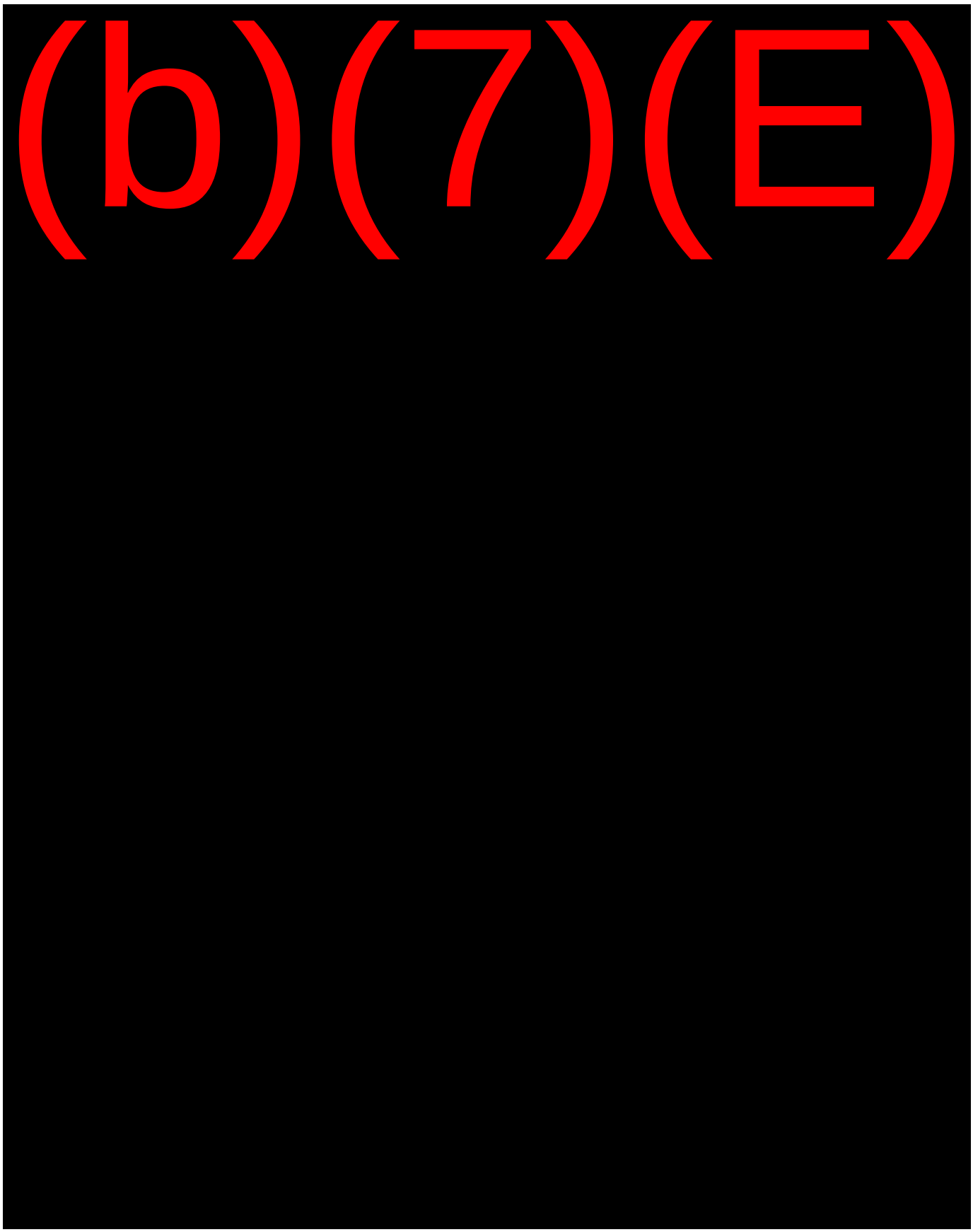

(b)(7)(E)

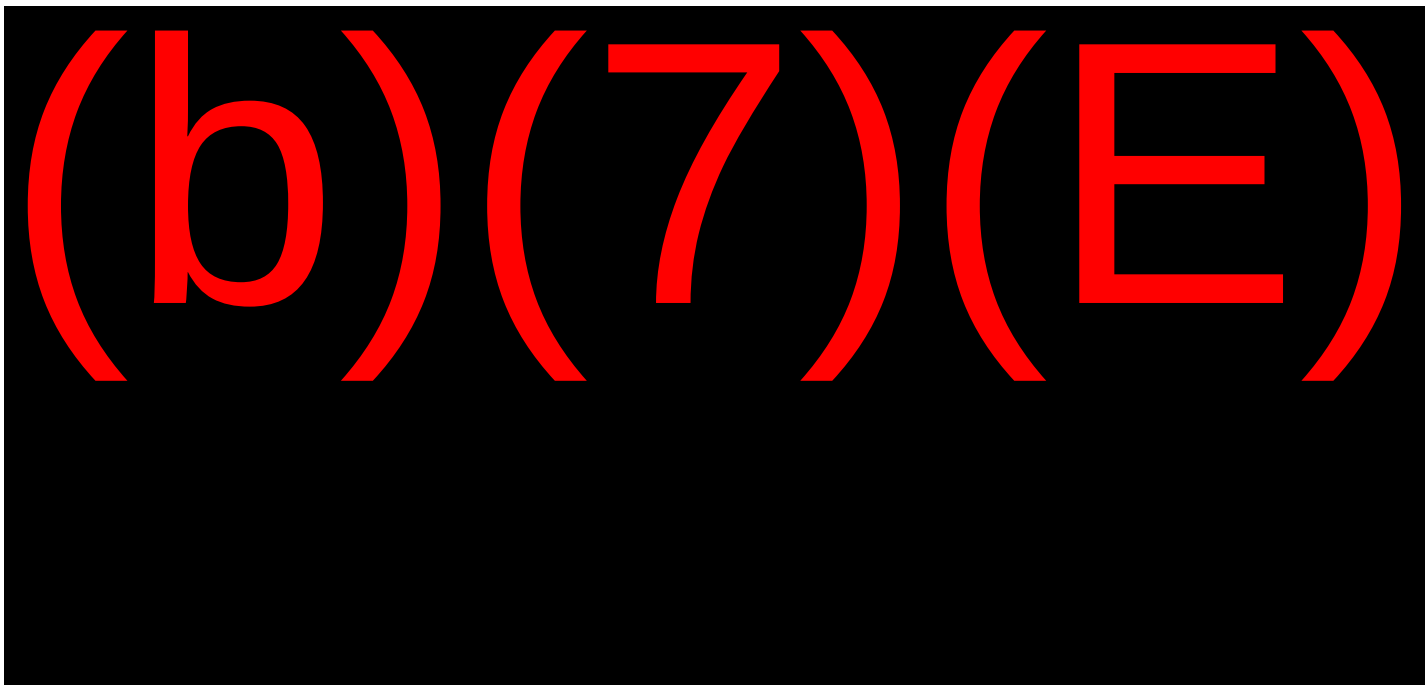

(b)(7)(E)

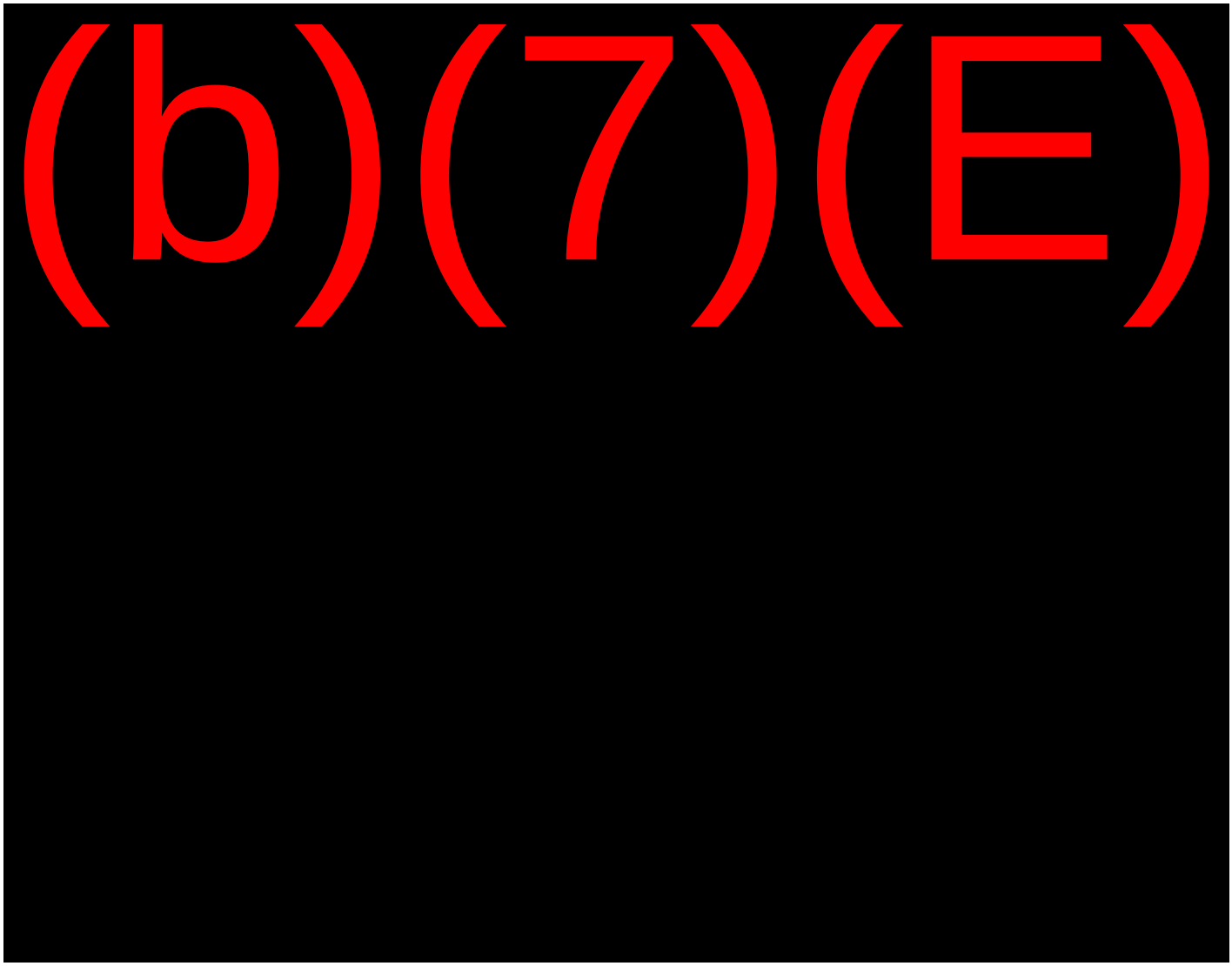

(b)(7)(E)


(b)(7)(E)

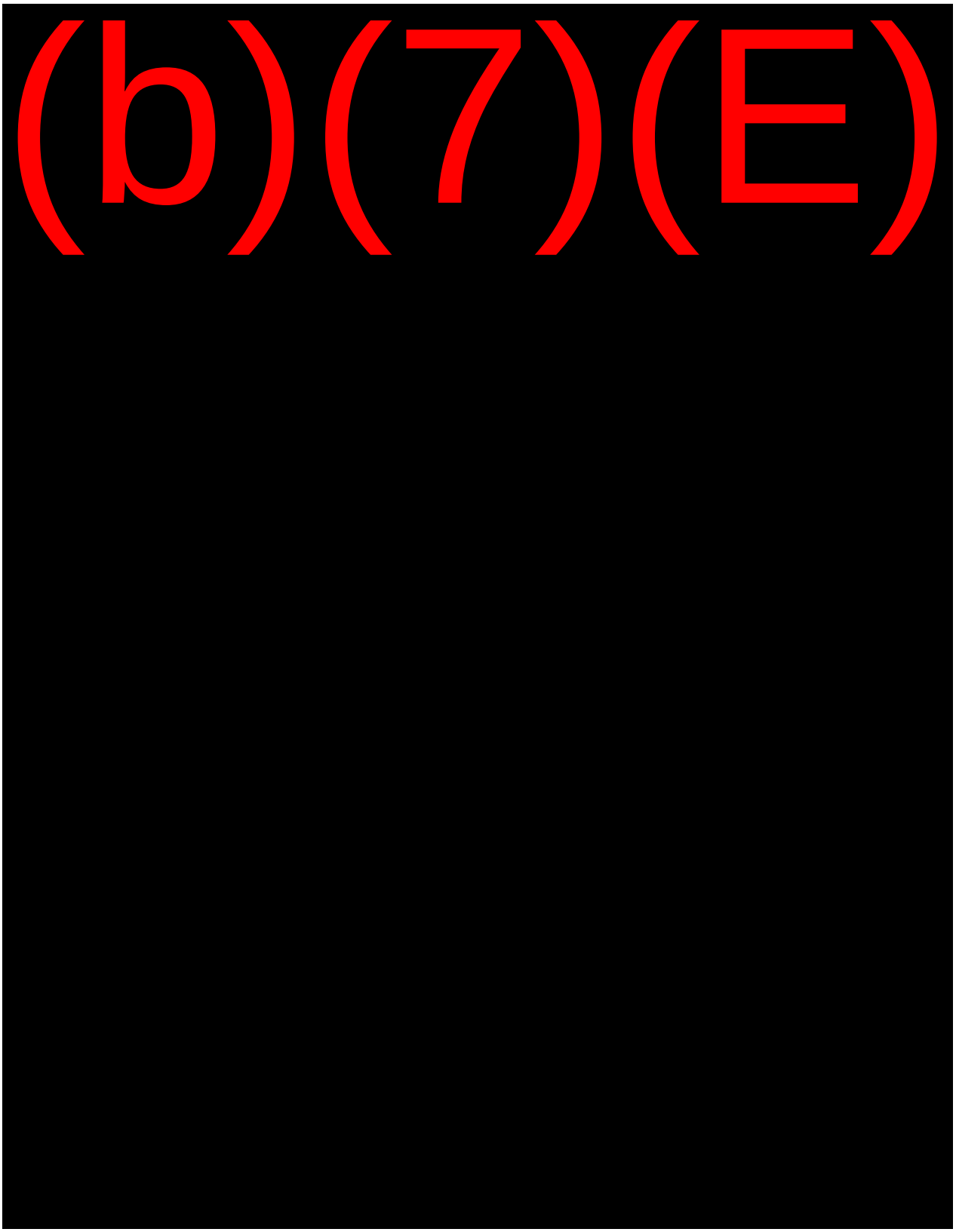

(b)(7)(E)

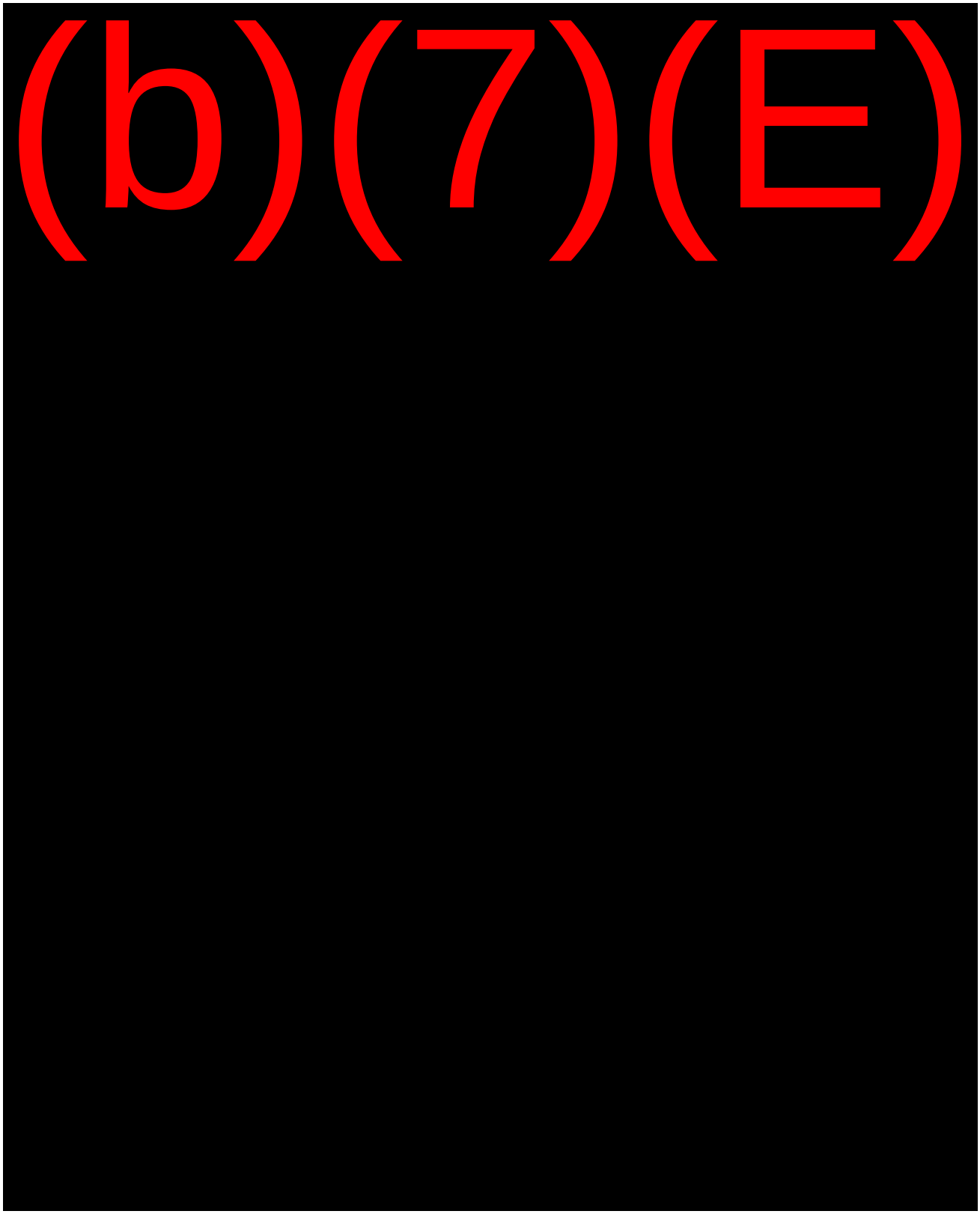

(b)(7)(E)

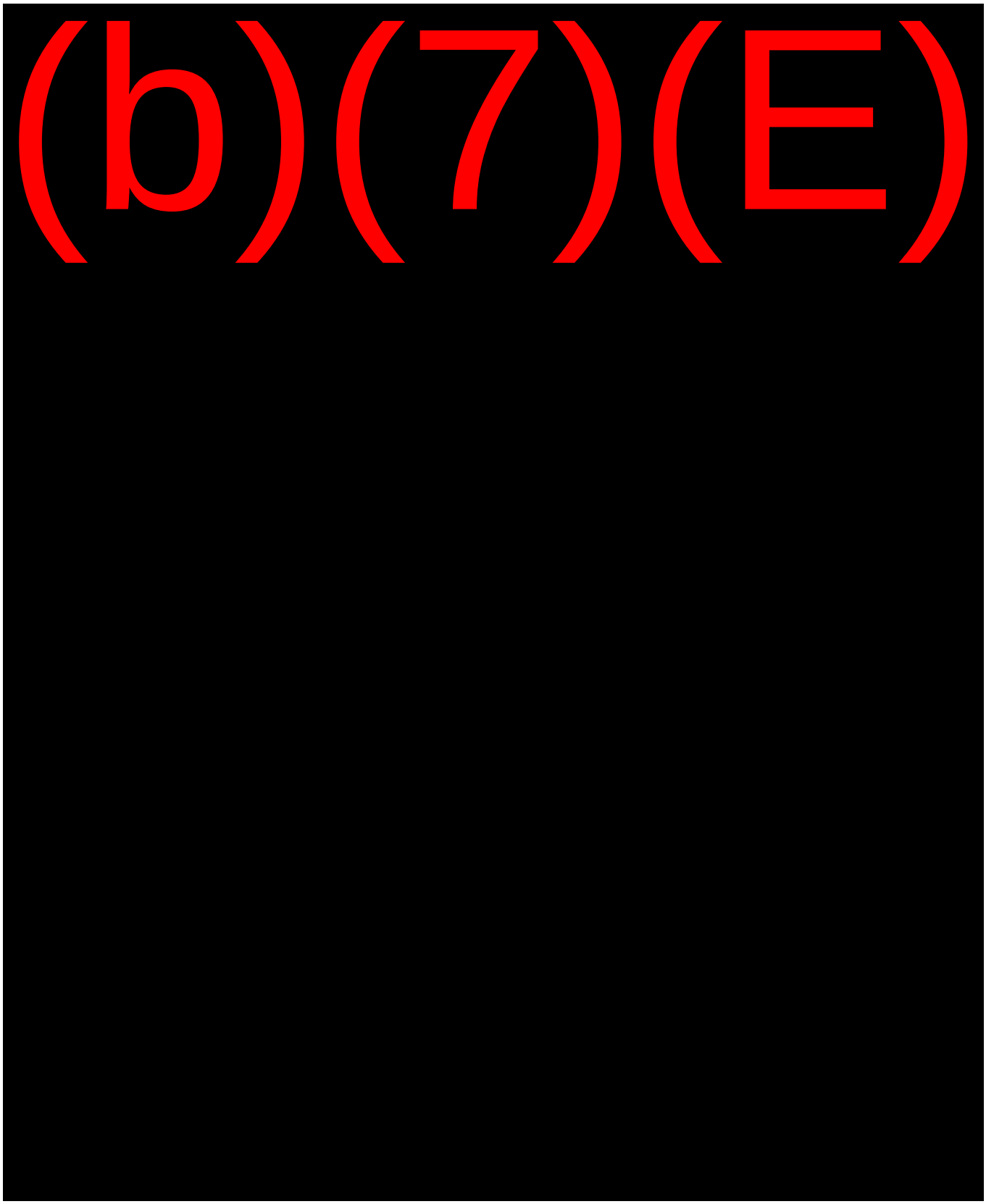

(b)(7)(E)

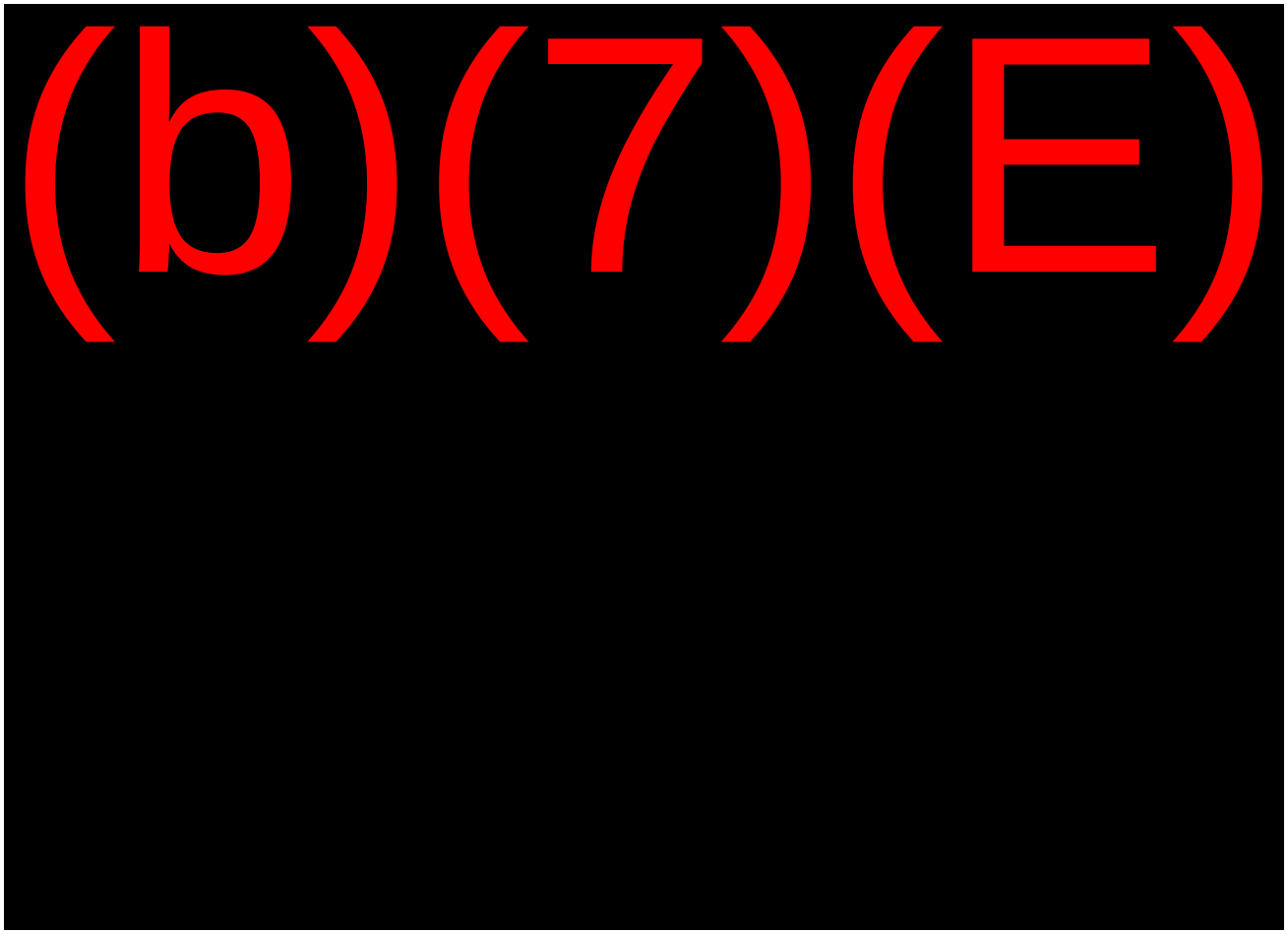

(b)(7)(E)

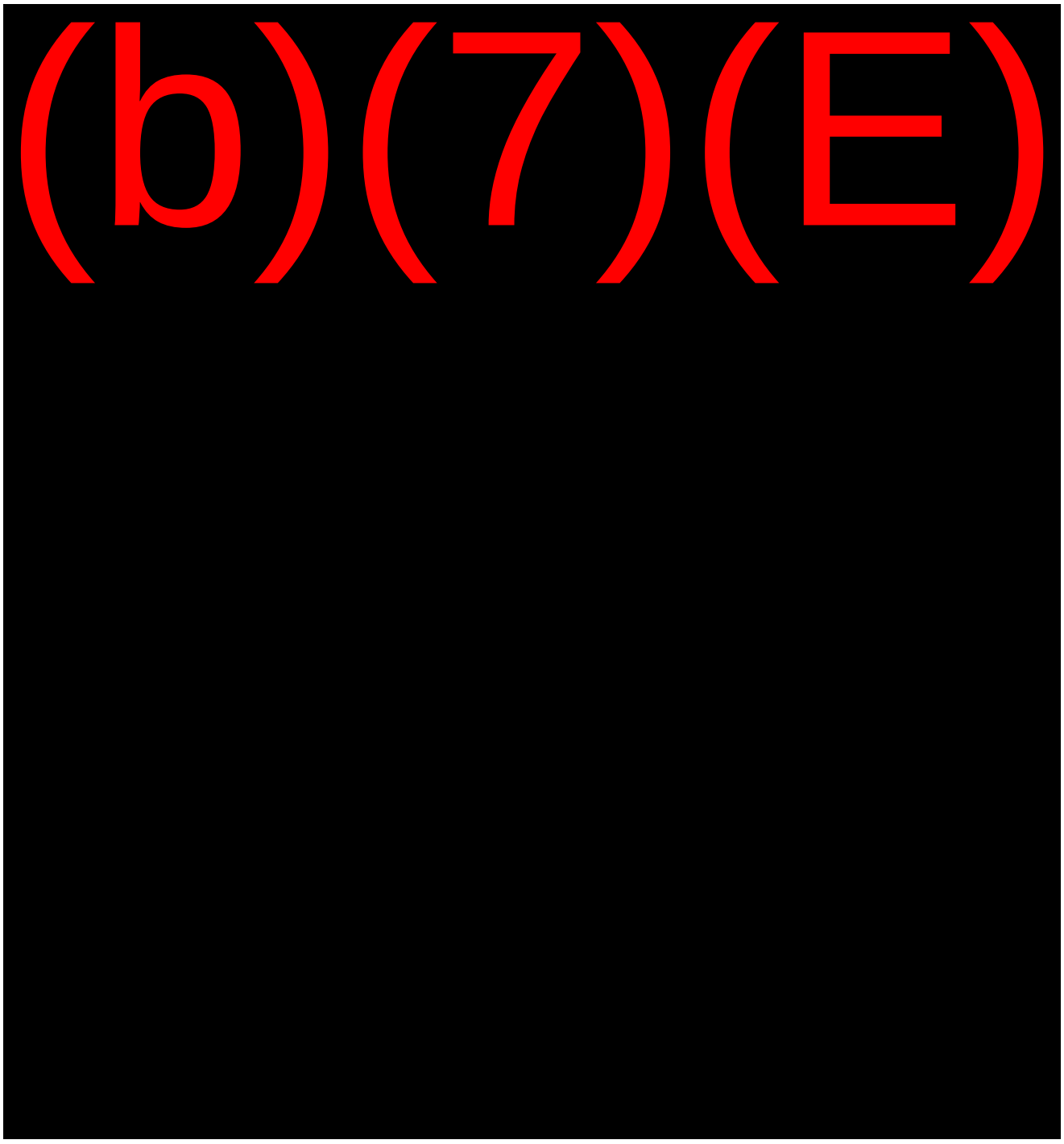

(b)(7)(E)


(b)(7)(E)

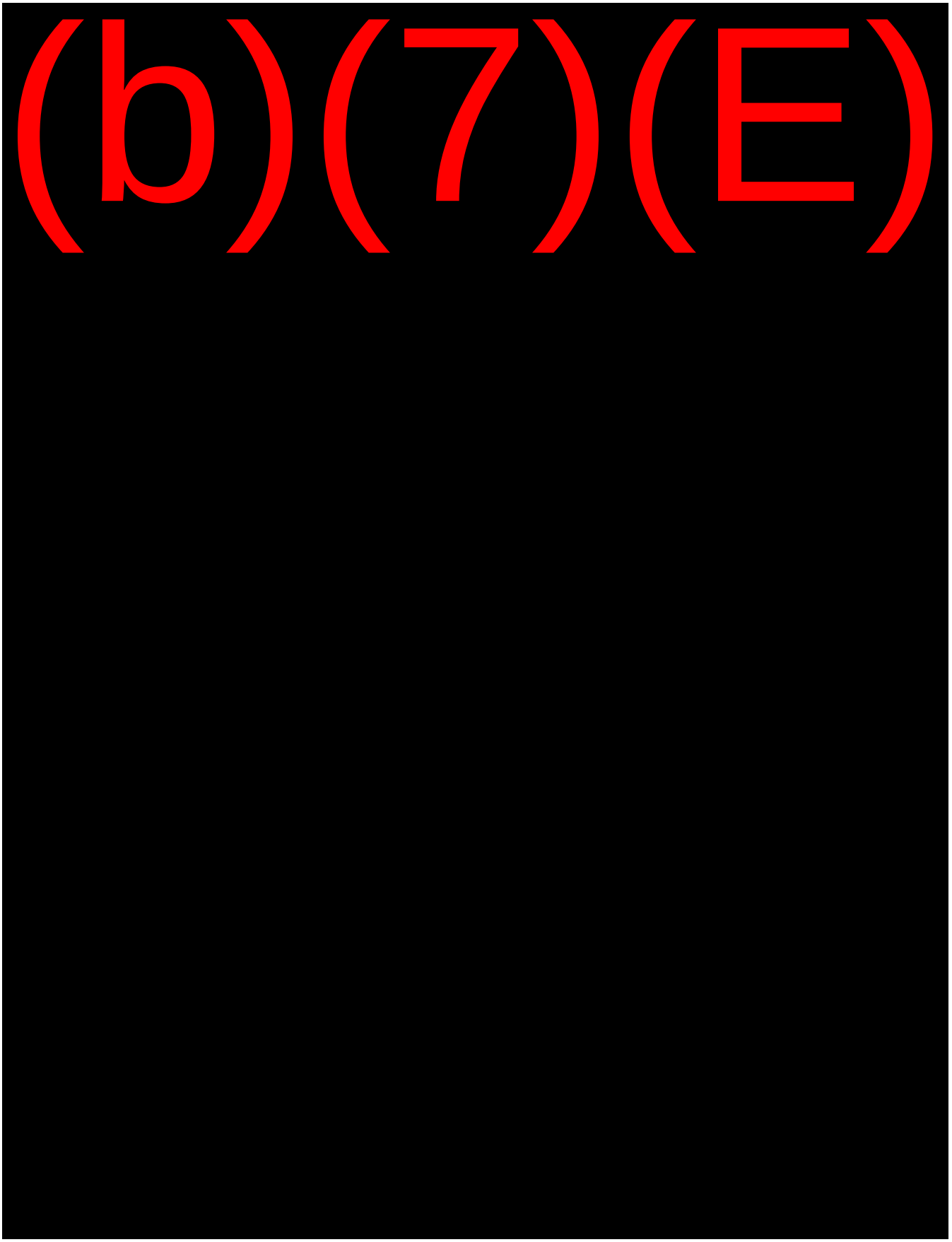

(b)(7)(E)

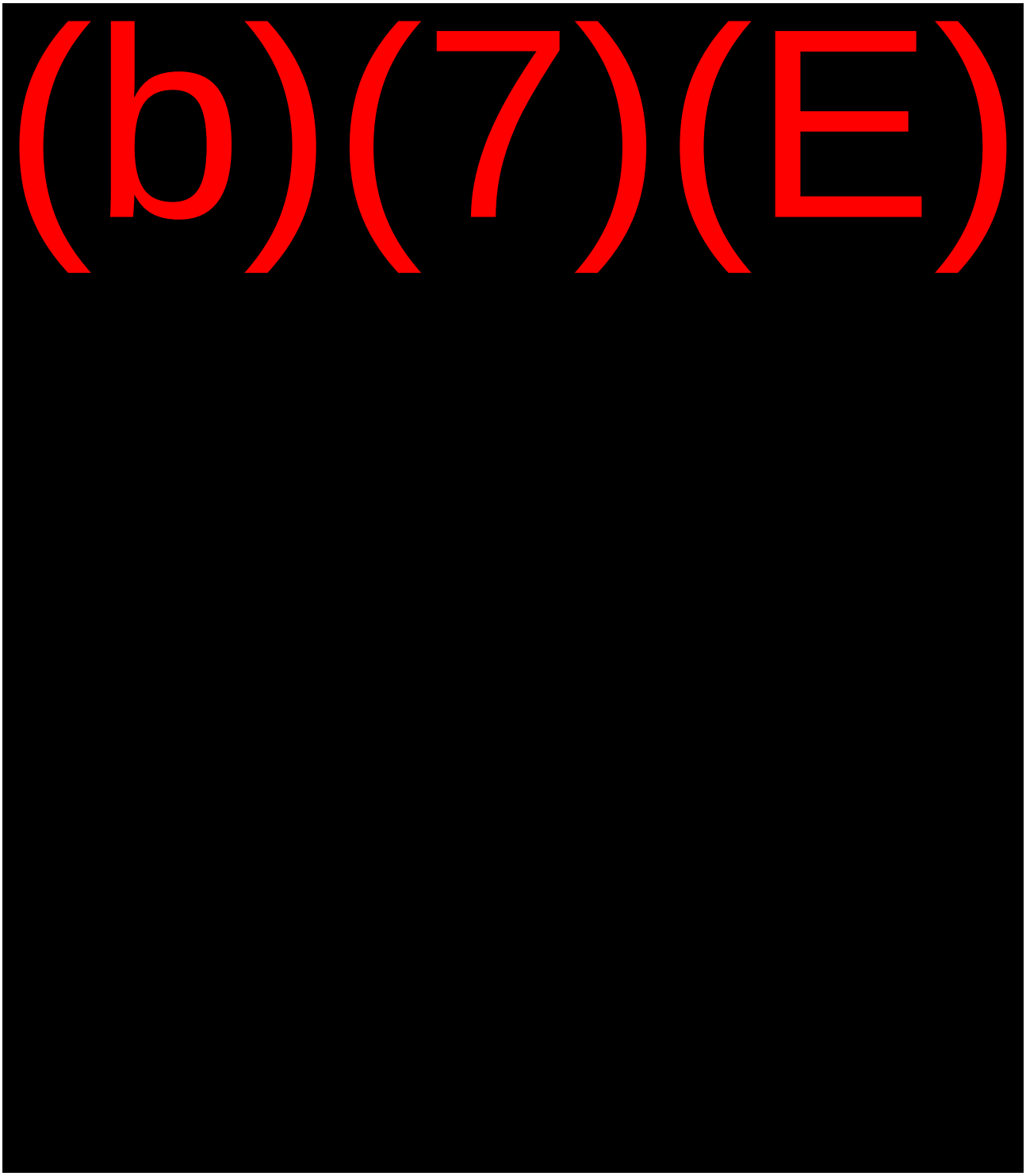

(b)(7)(E)

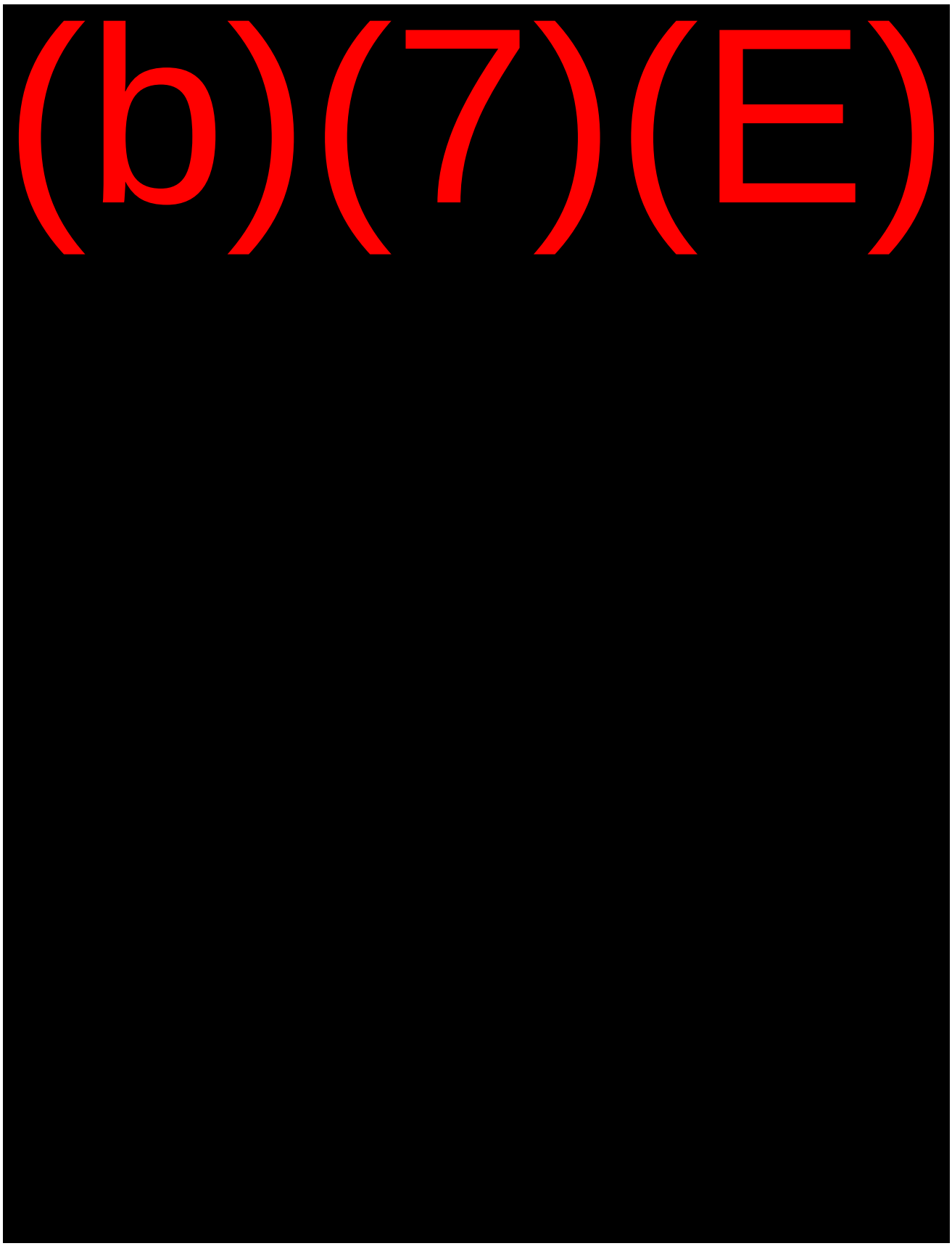

(b)(7)(E)


(b)(7)(E)

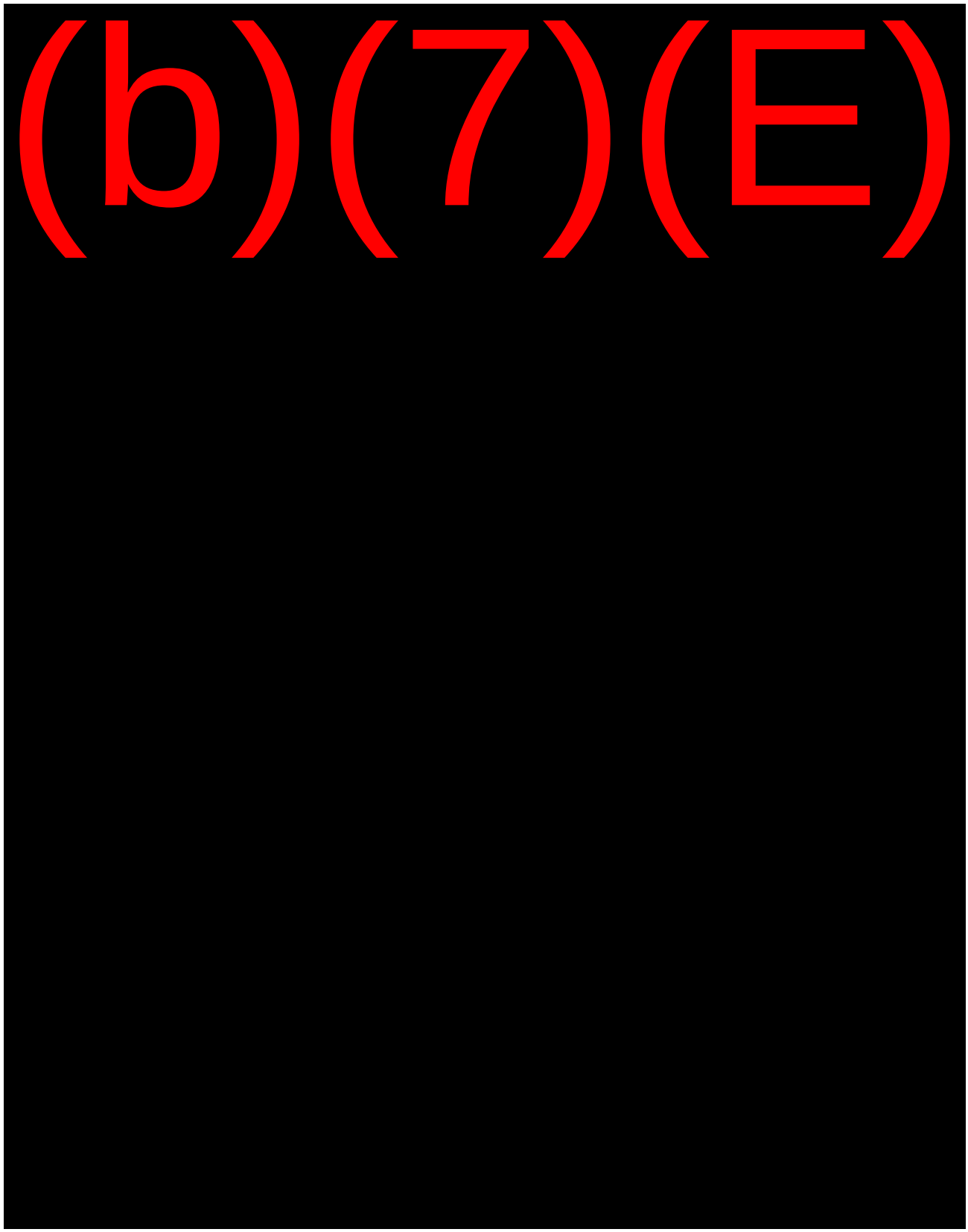

(b)(7)(E)

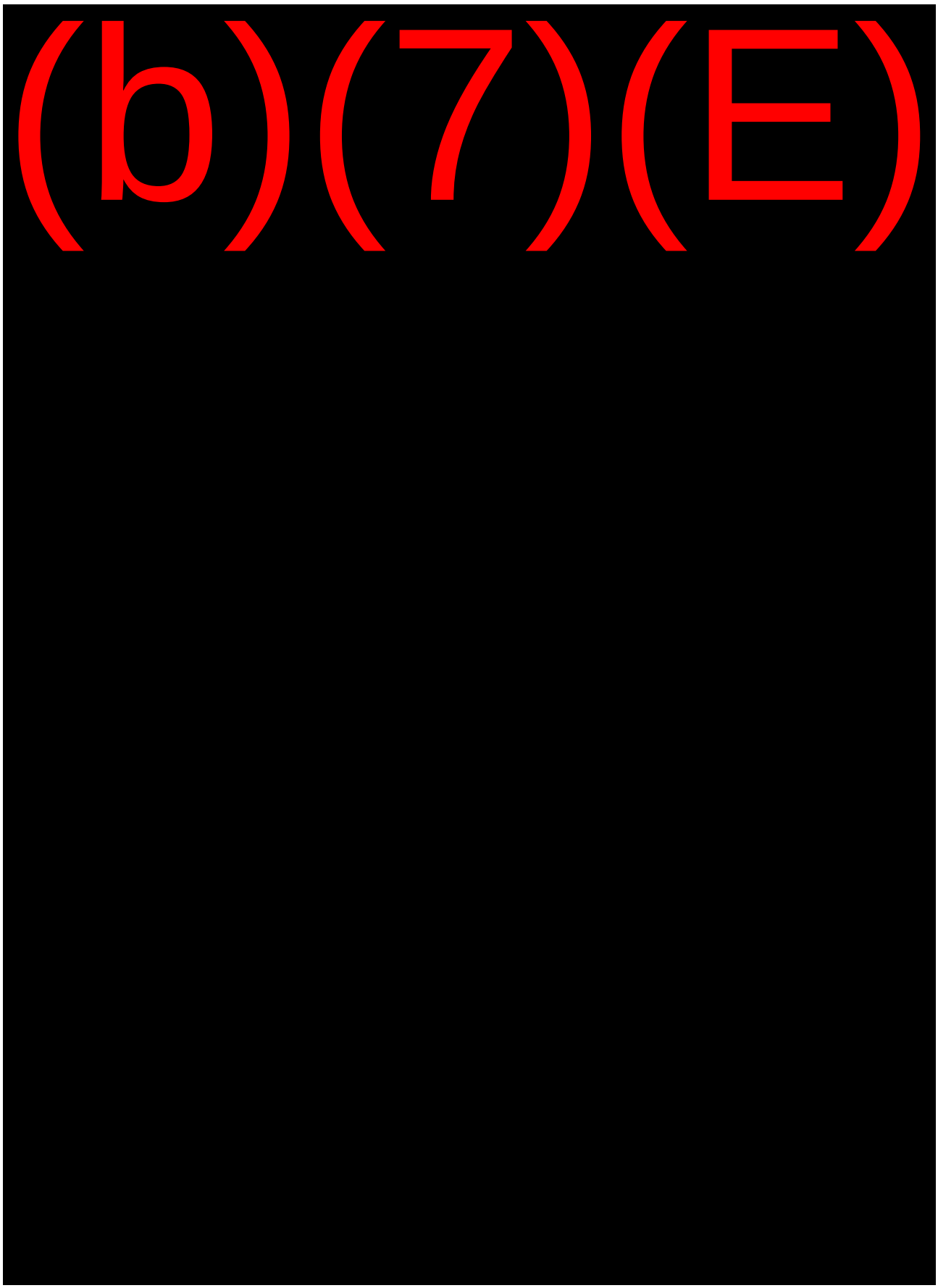

(b)(7)(E)


(b)(7)(E)

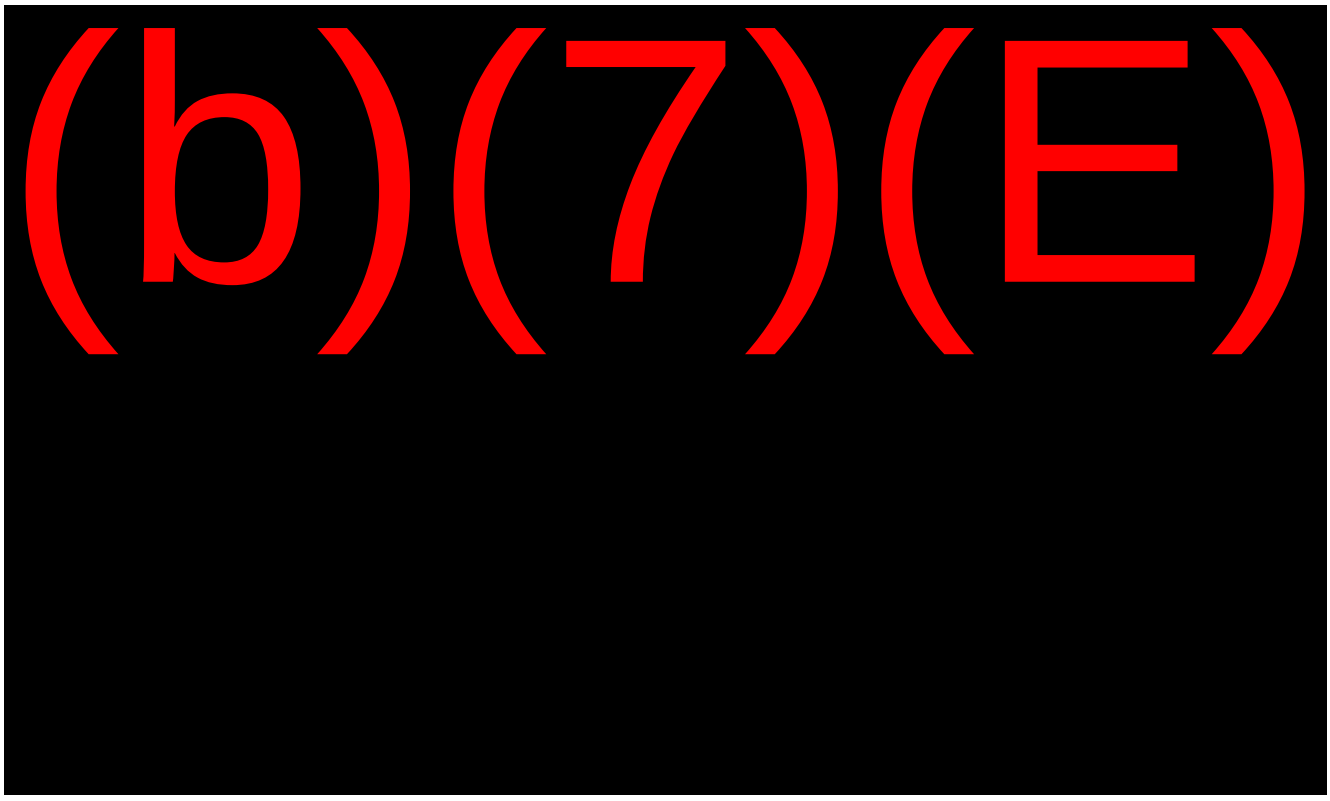

(b)(7)(E)

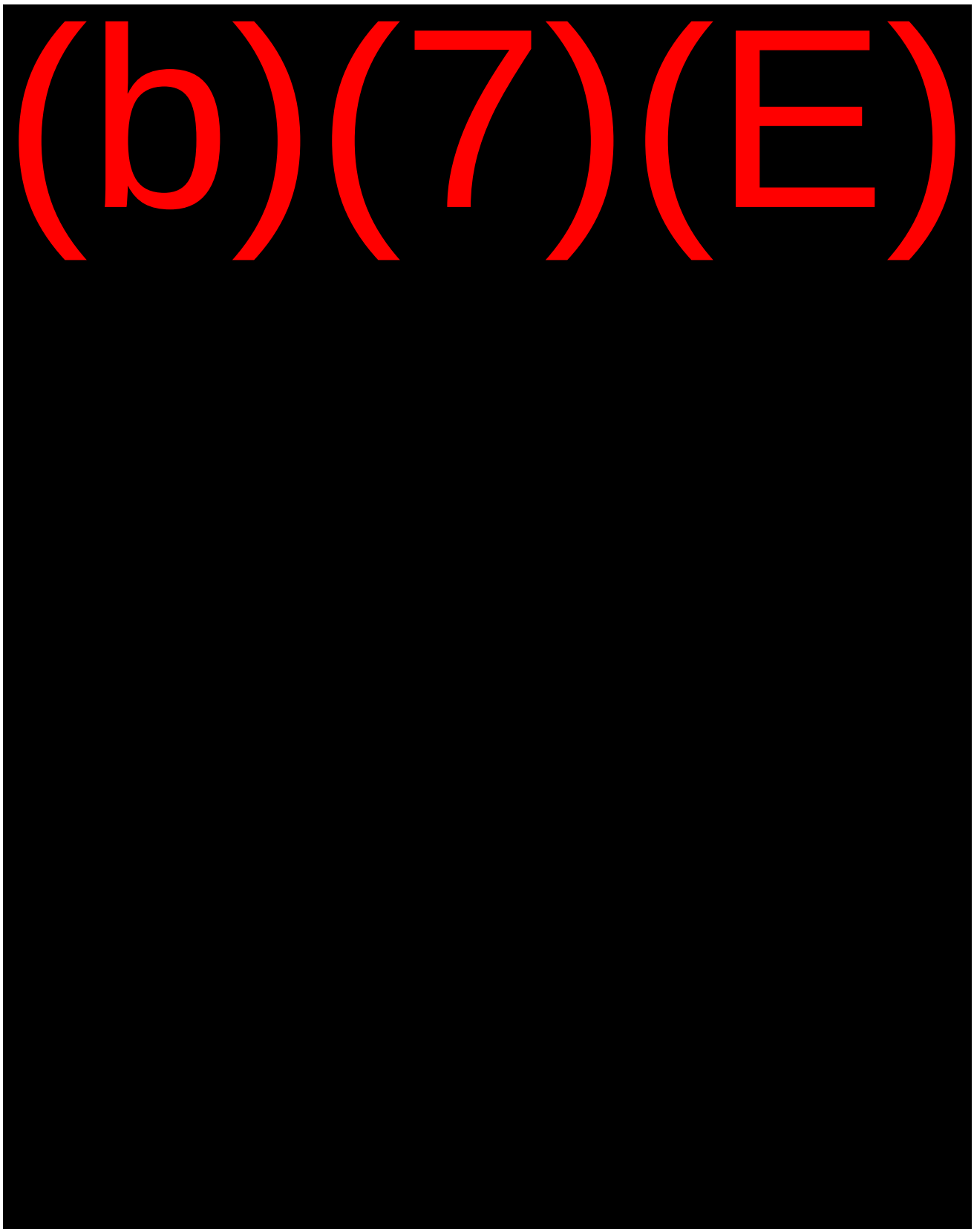

(b)(7)(E)

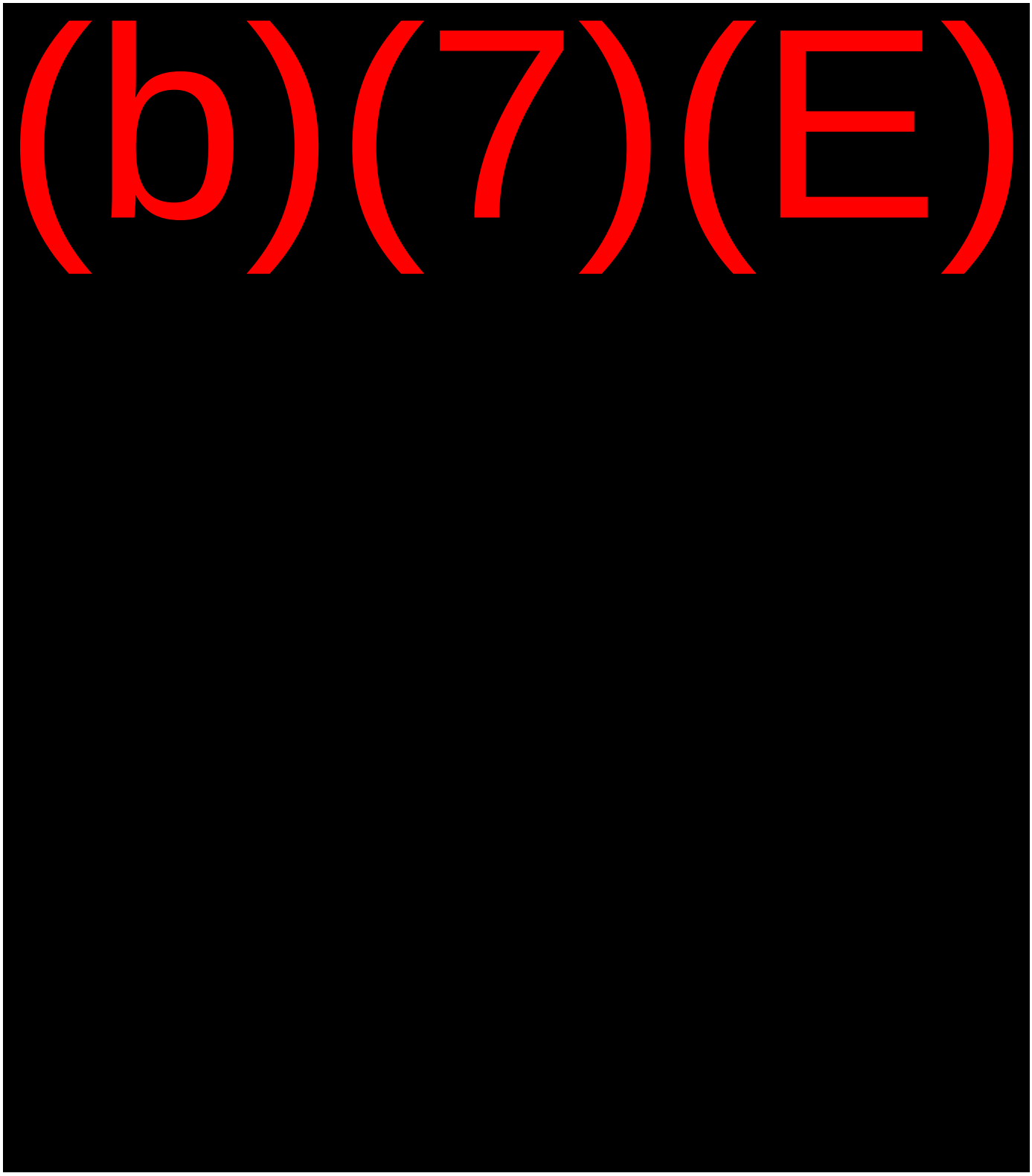

(b)(7)(E)


(b)(7)(E)

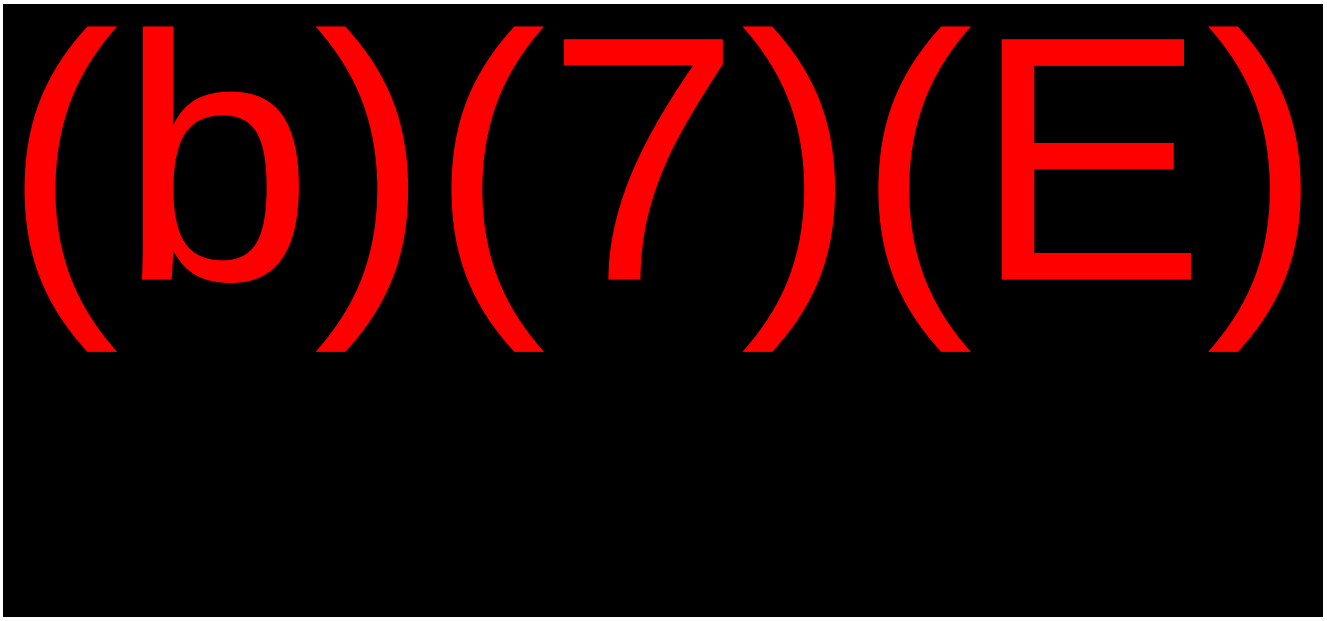

(b)(7)(E)

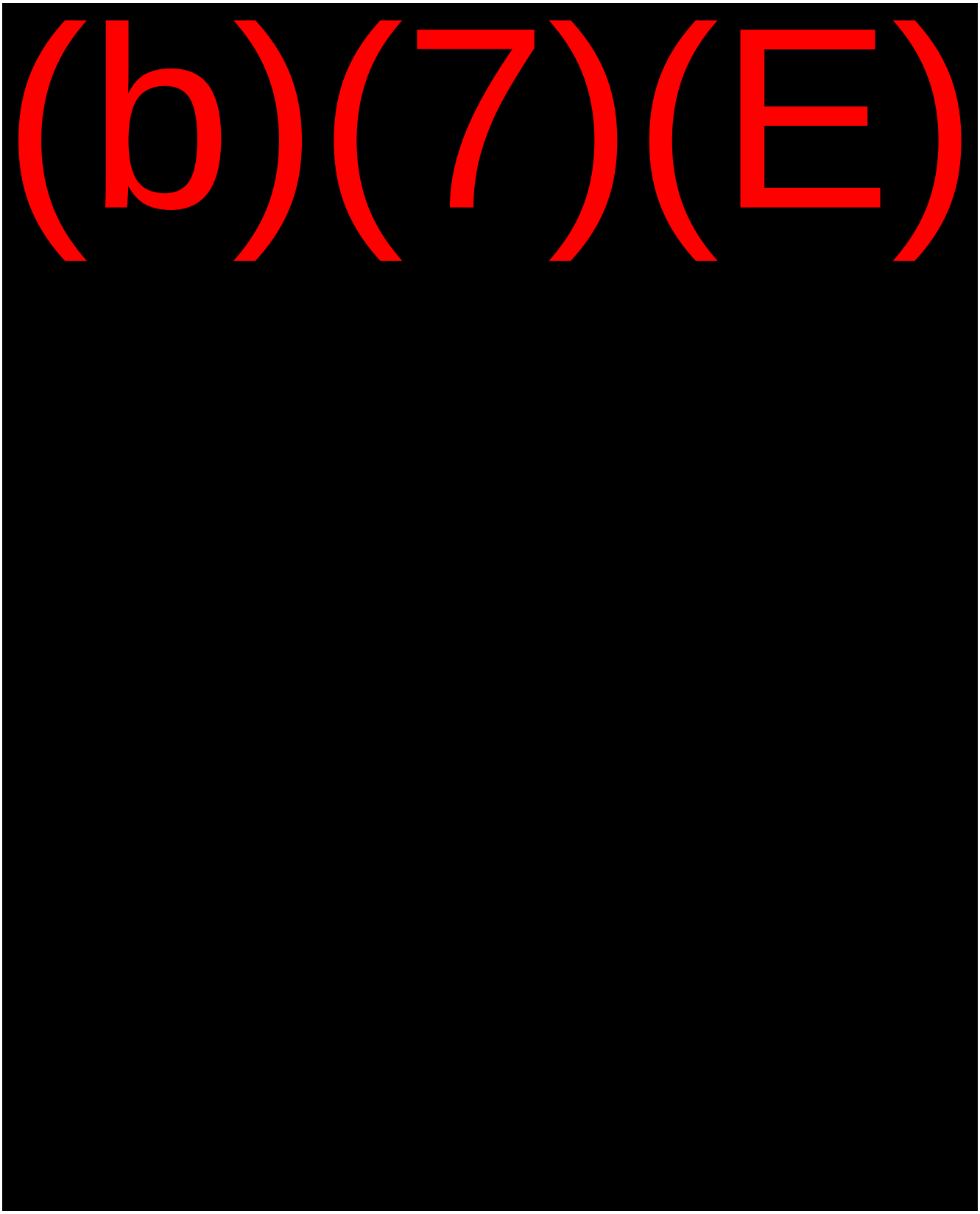

(b)(7)(E)

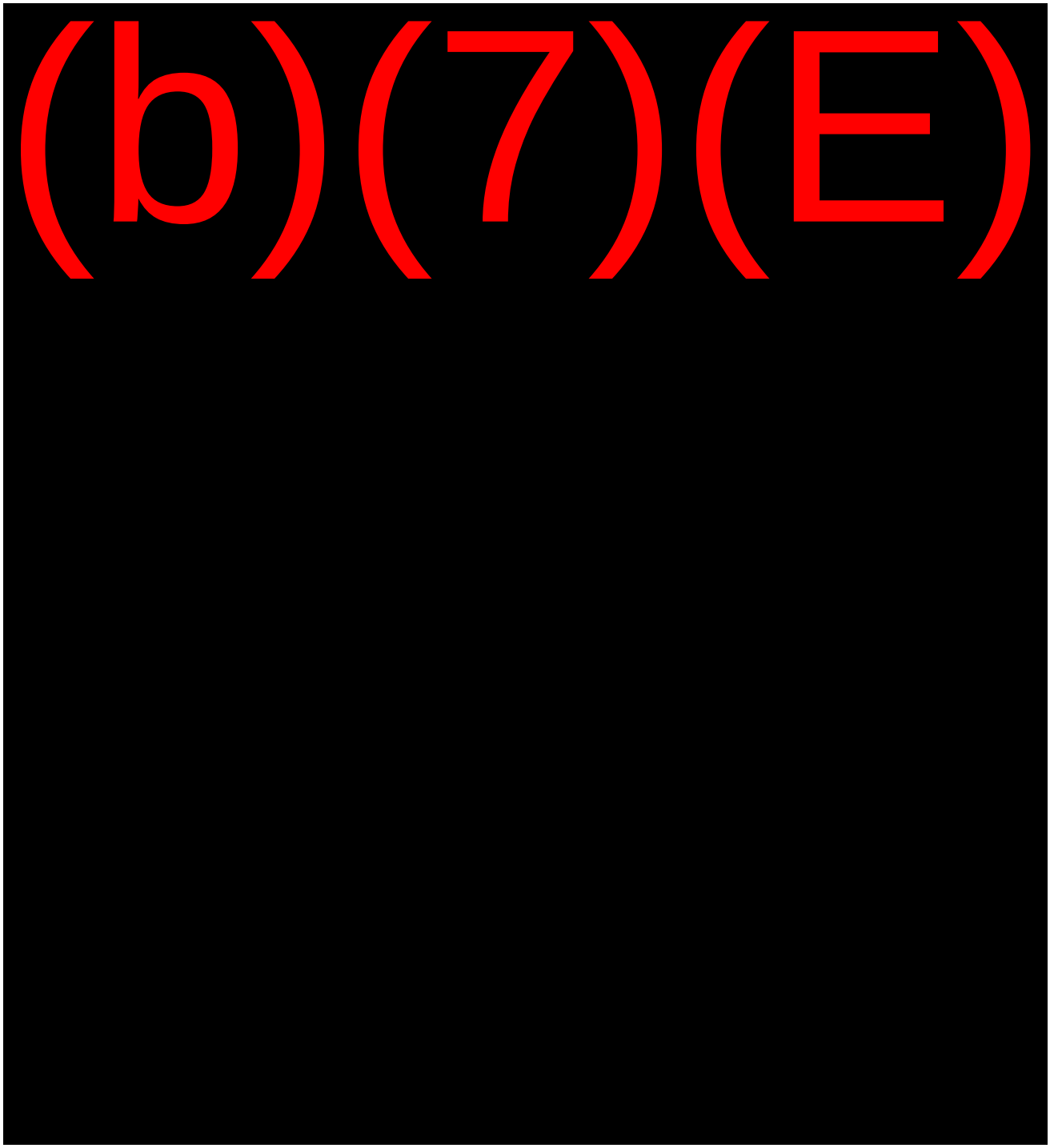

(b)(7)(E)

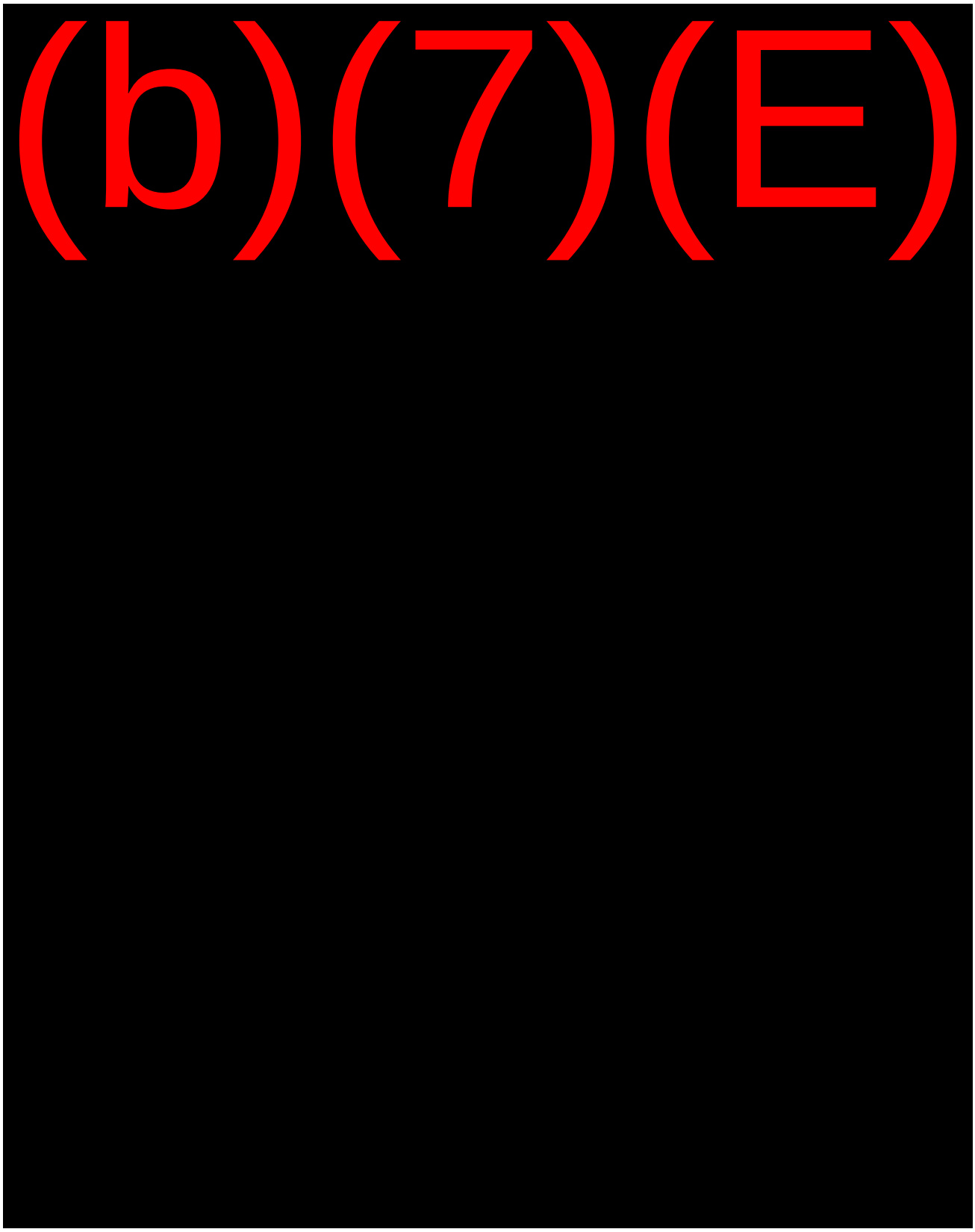

(b)(7)(E)

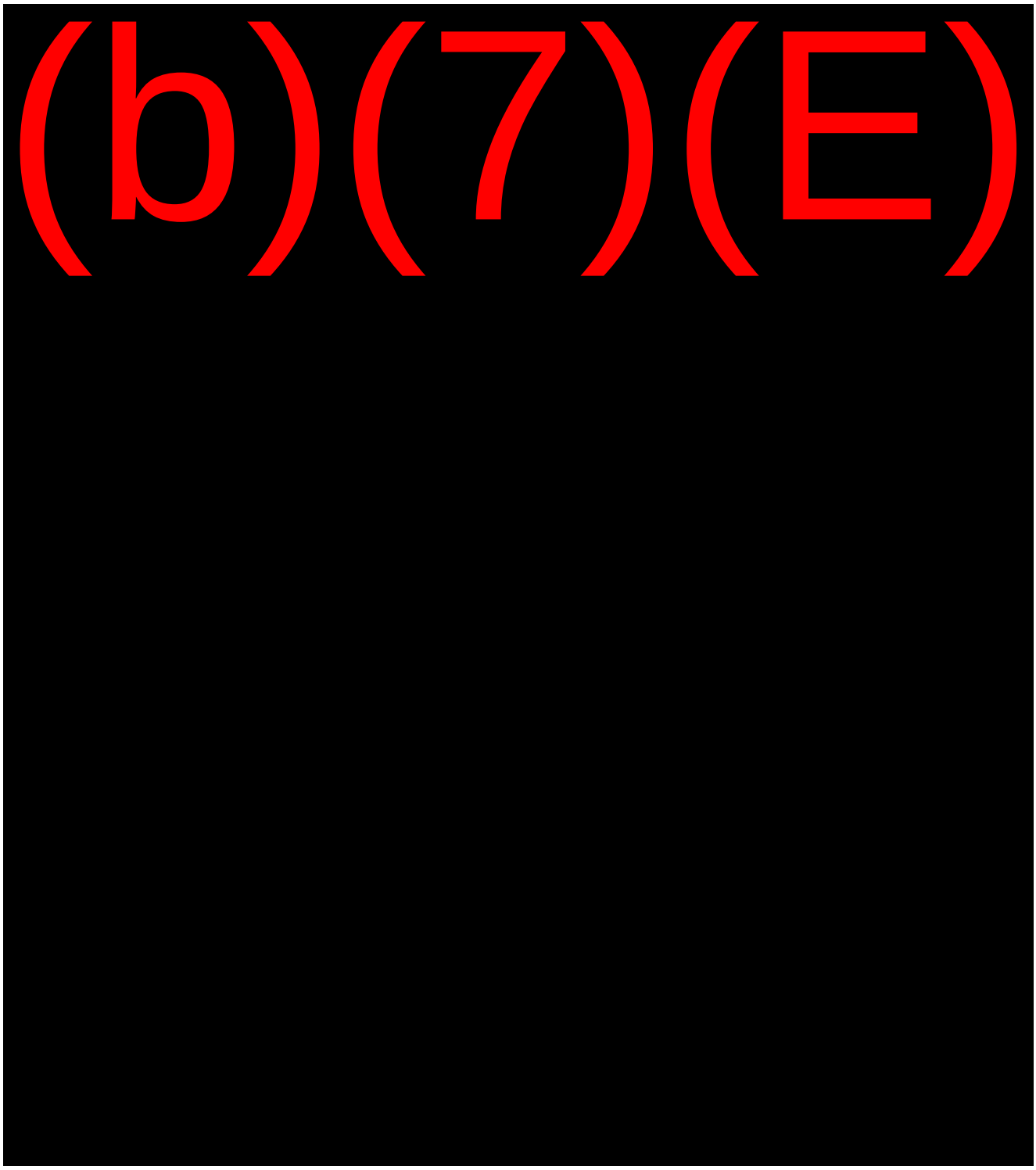

(b)(7)(E)

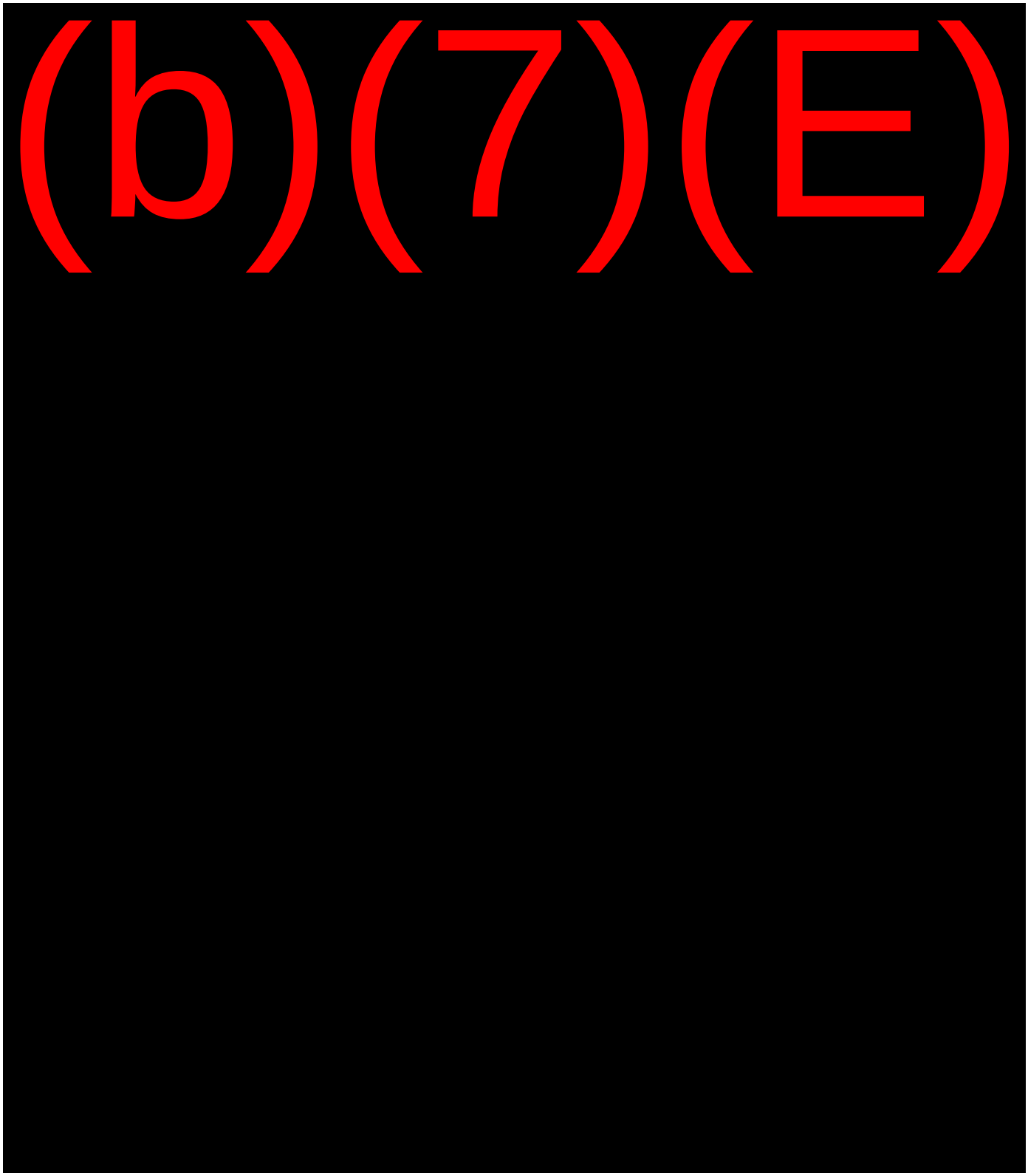

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

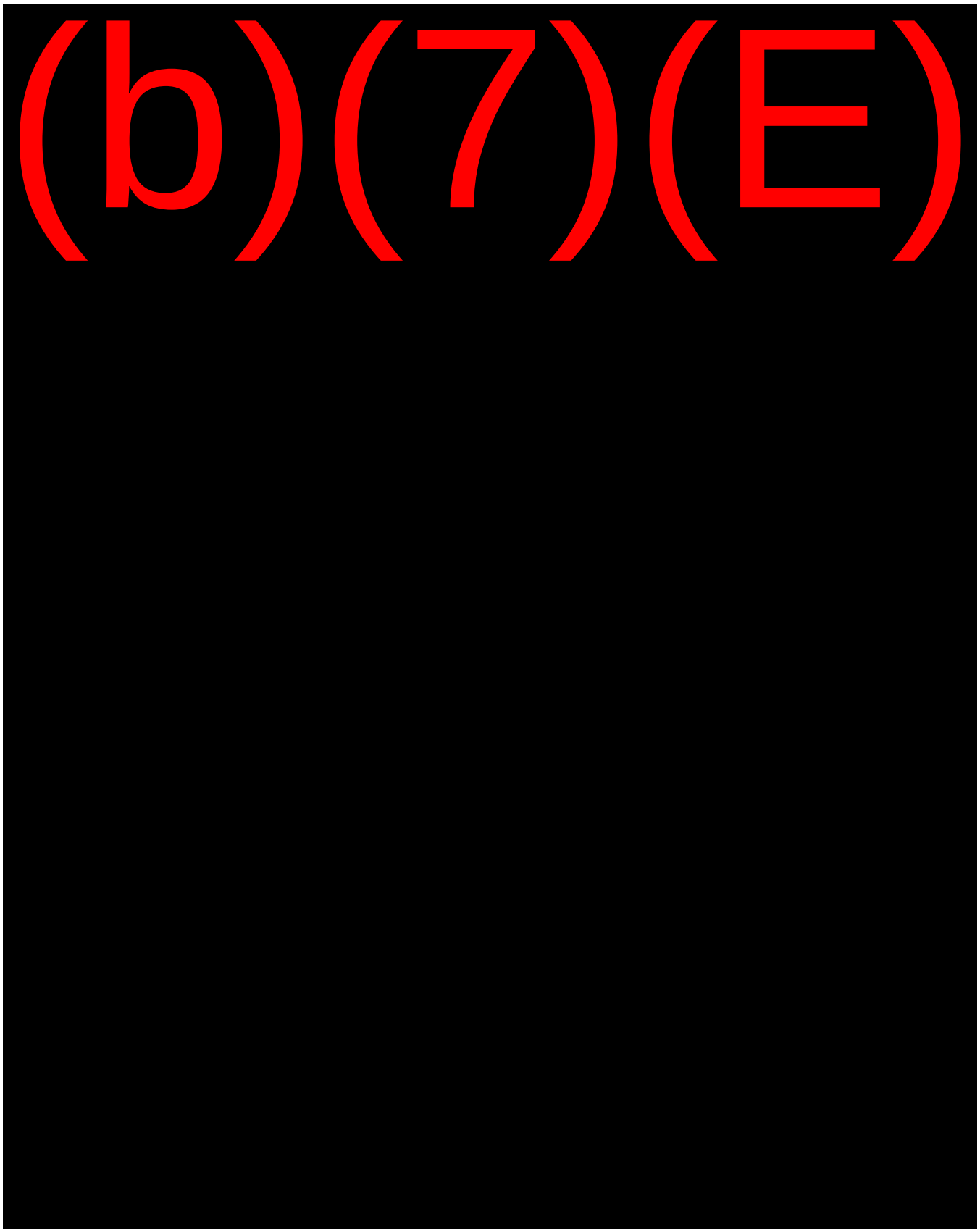

(b)(7)(E)

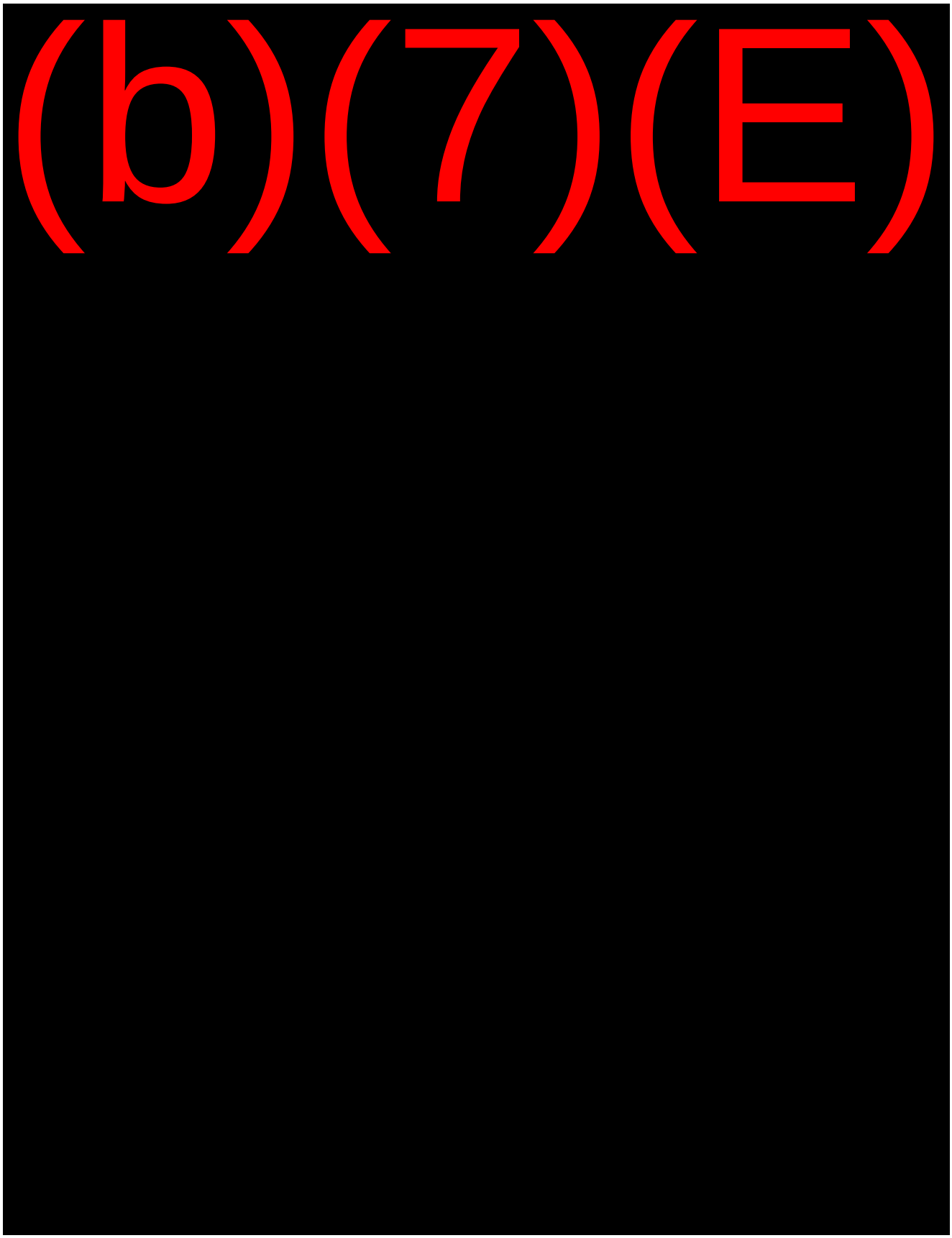

(b)(7)(E)

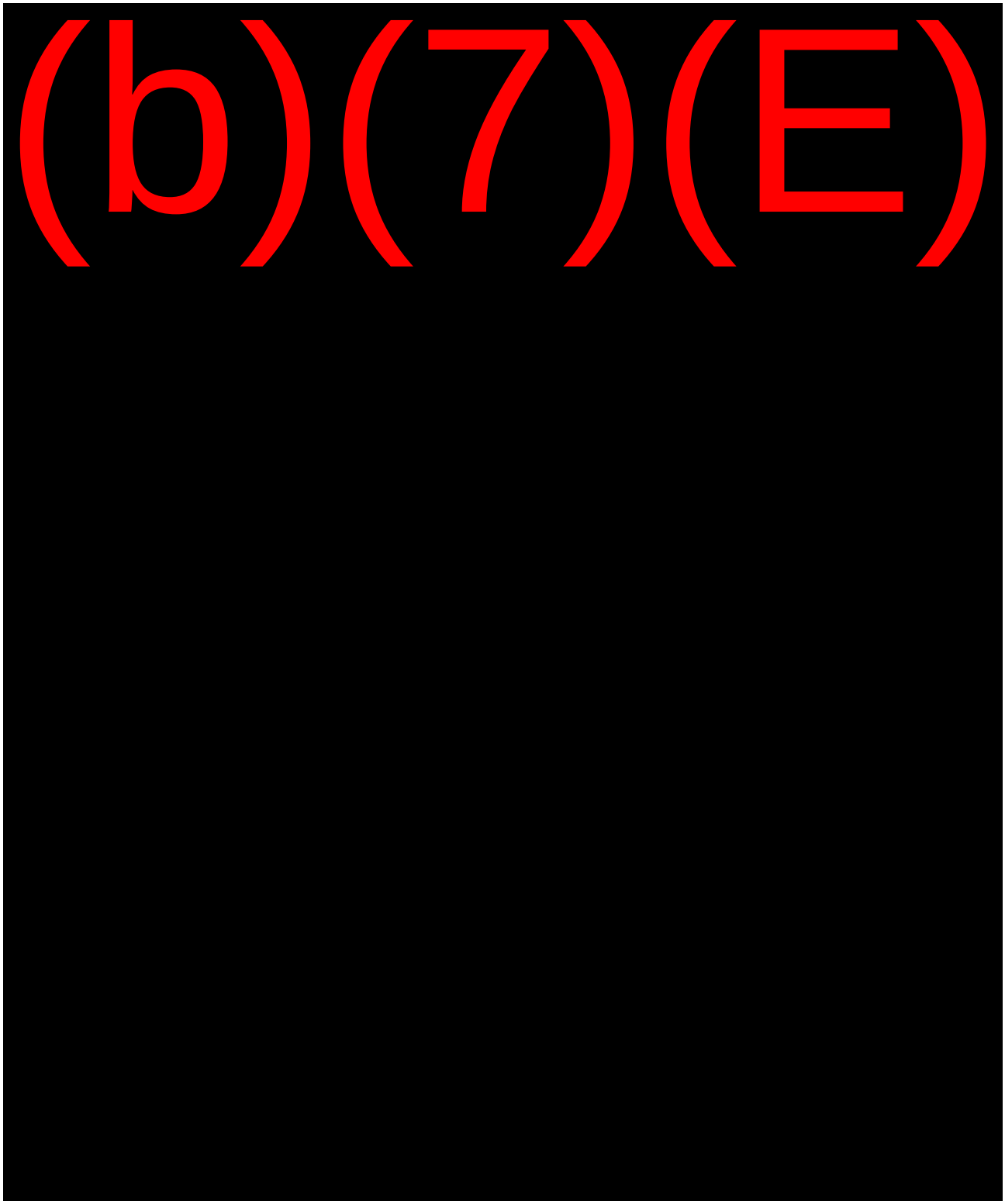

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

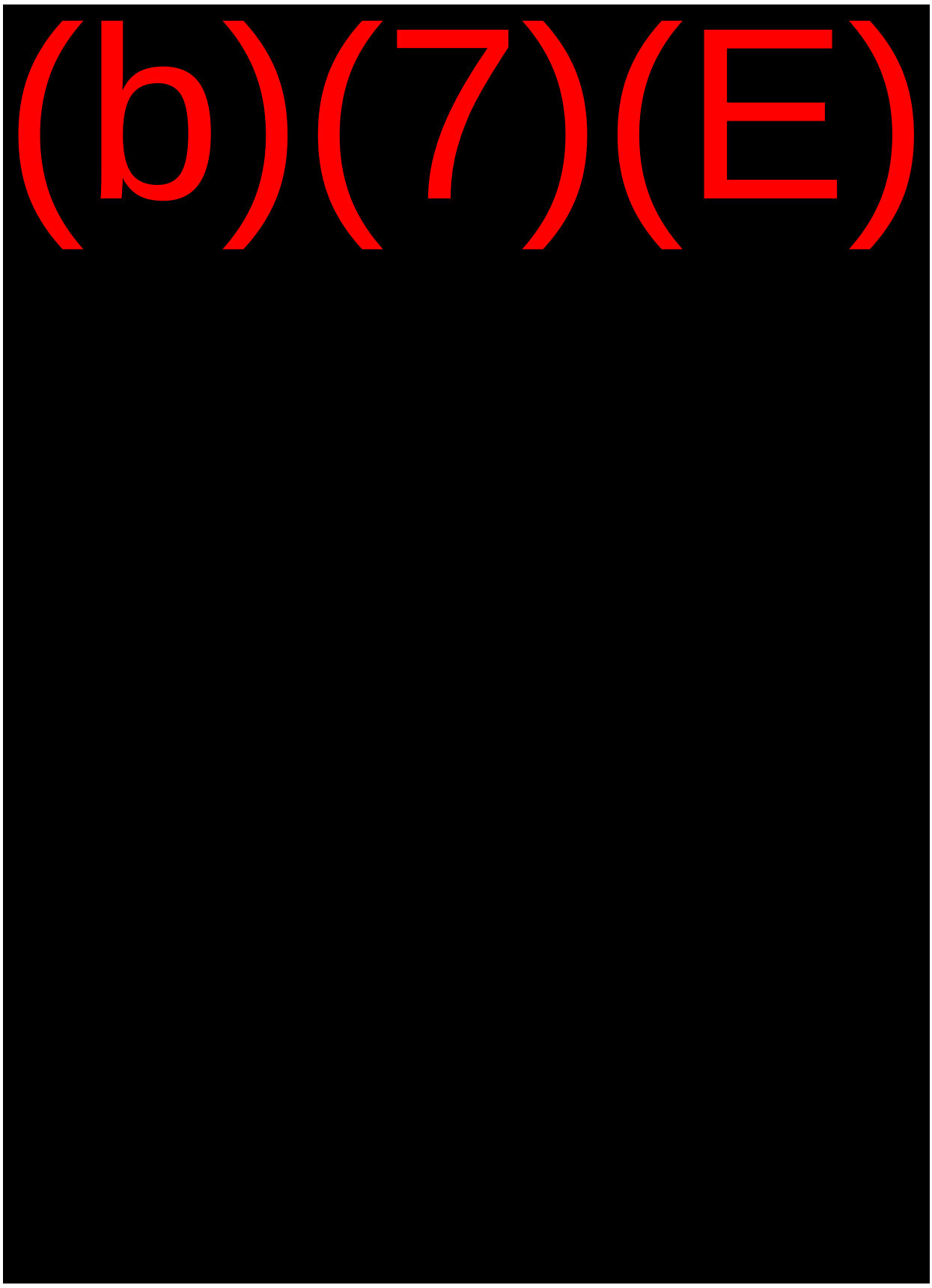

(b)(7)(E)

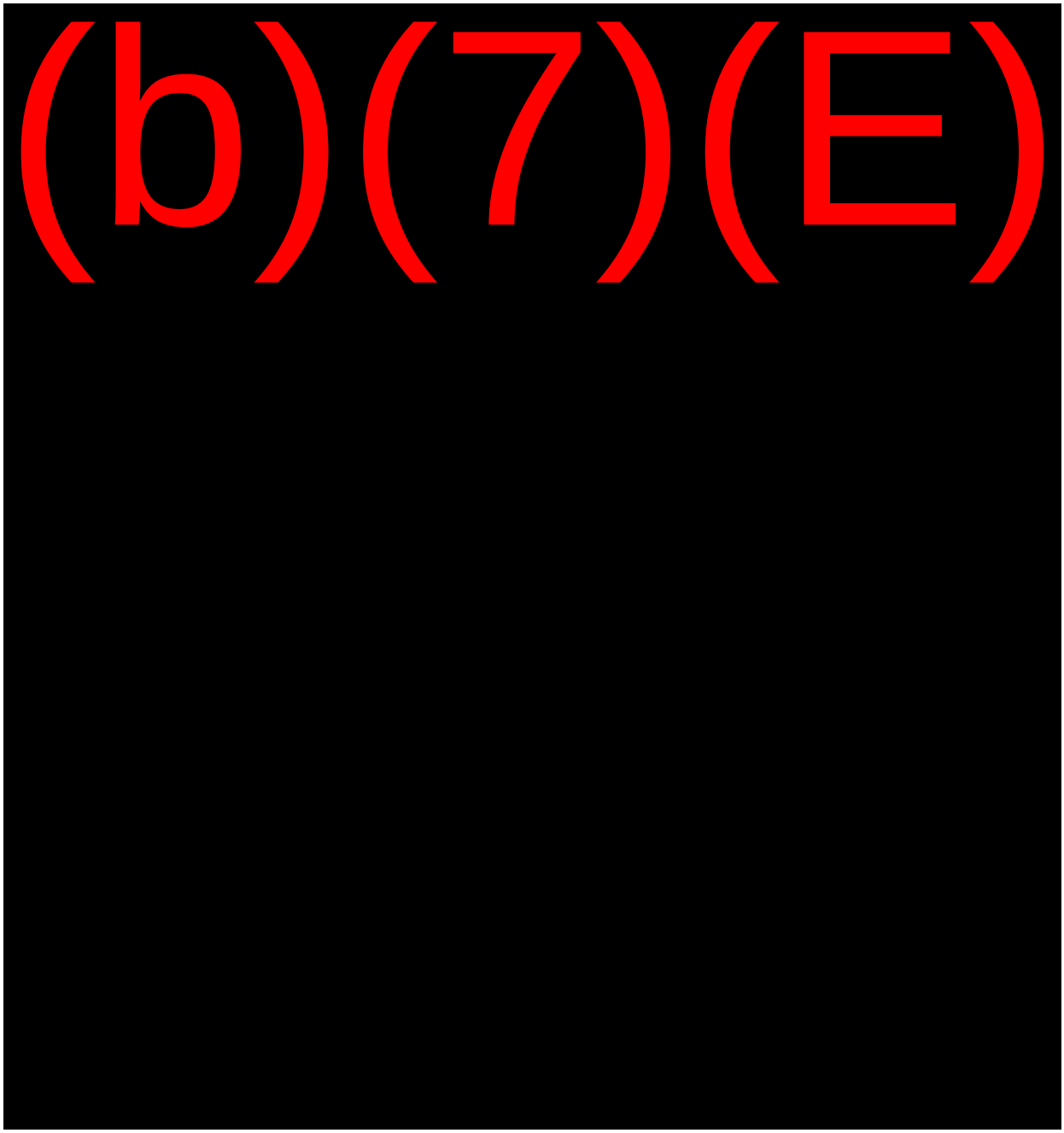

(b)(7)(E)

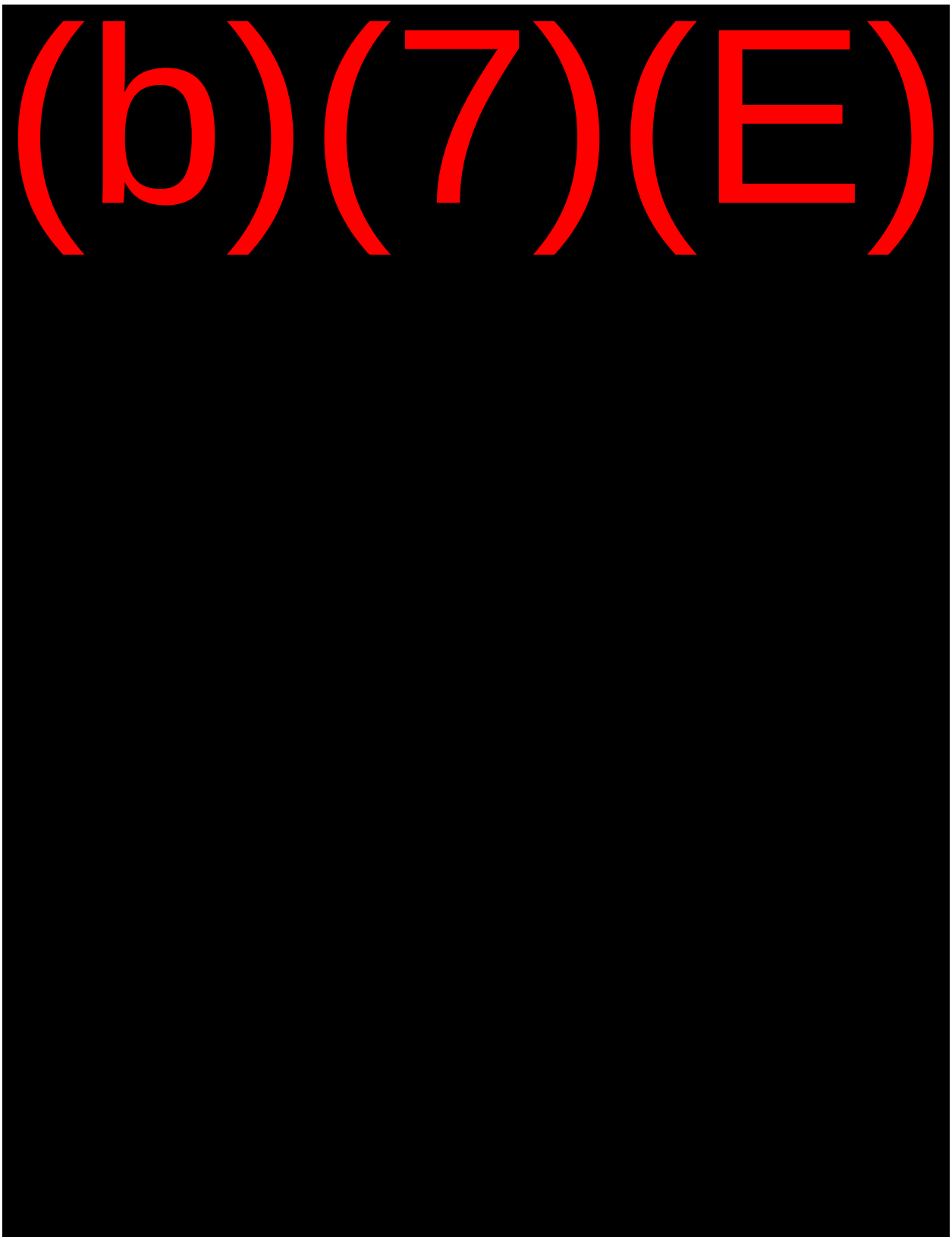

(b)(7)(E)

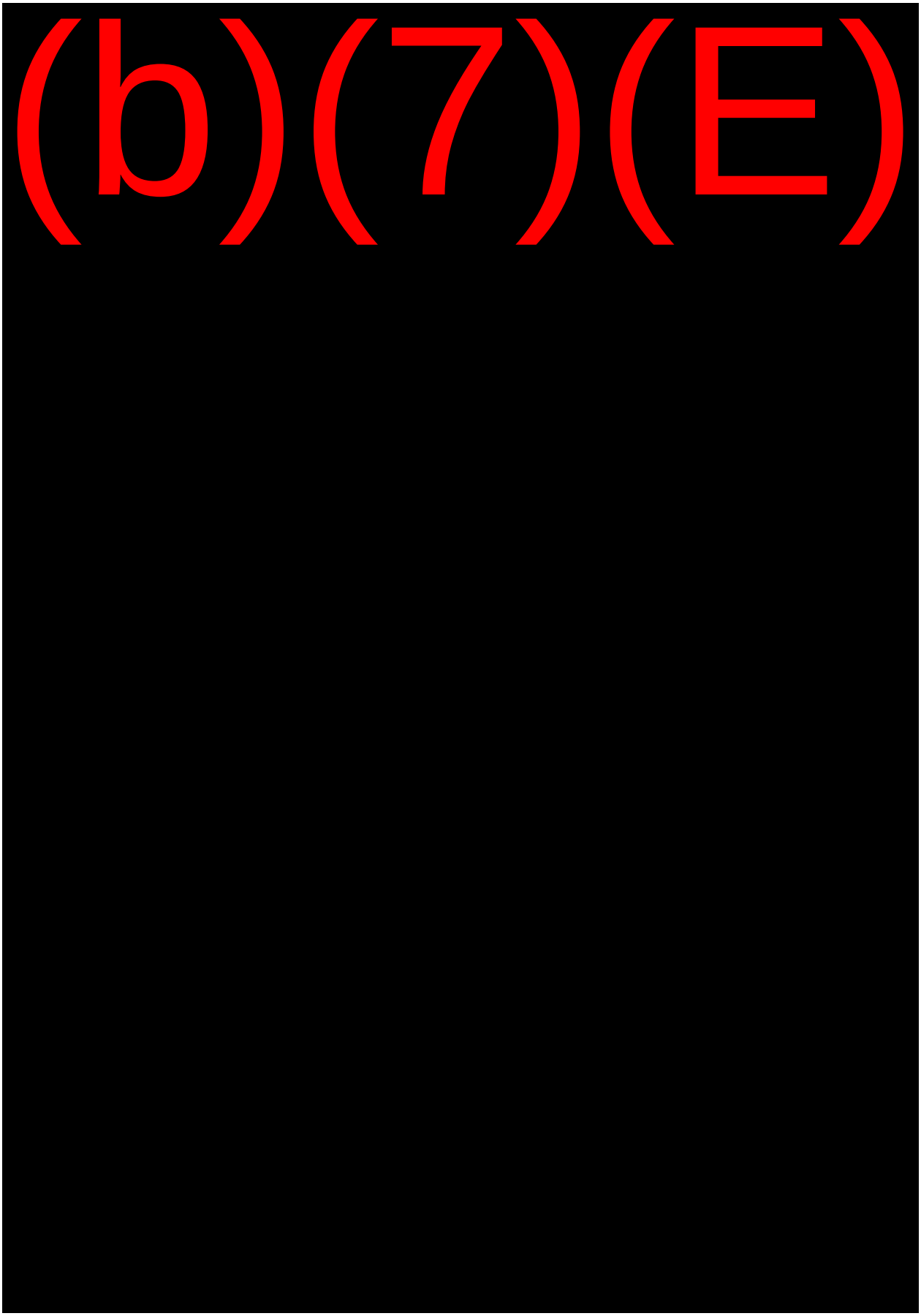

(b)(7)(E)

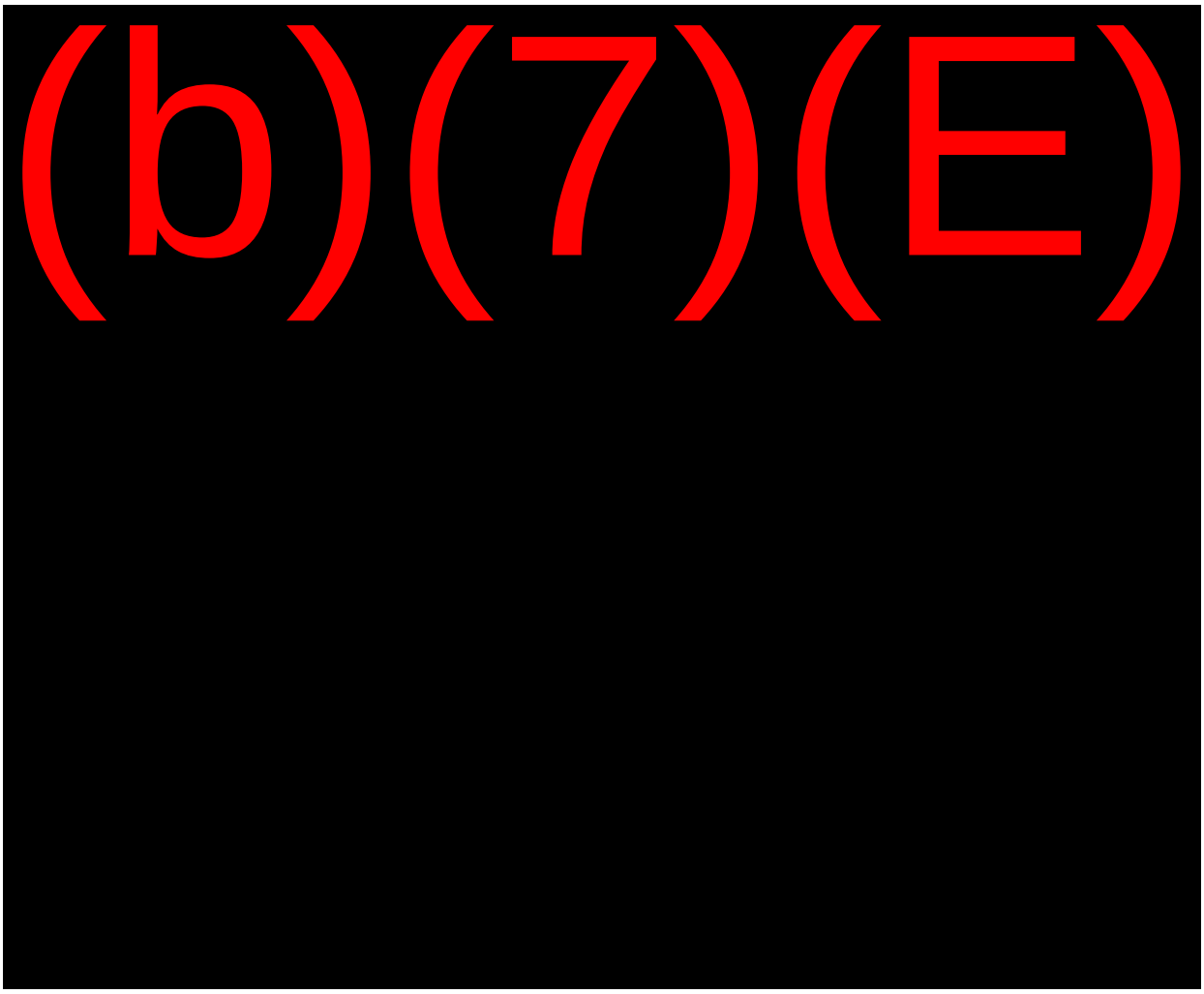

(b)(7)(E)

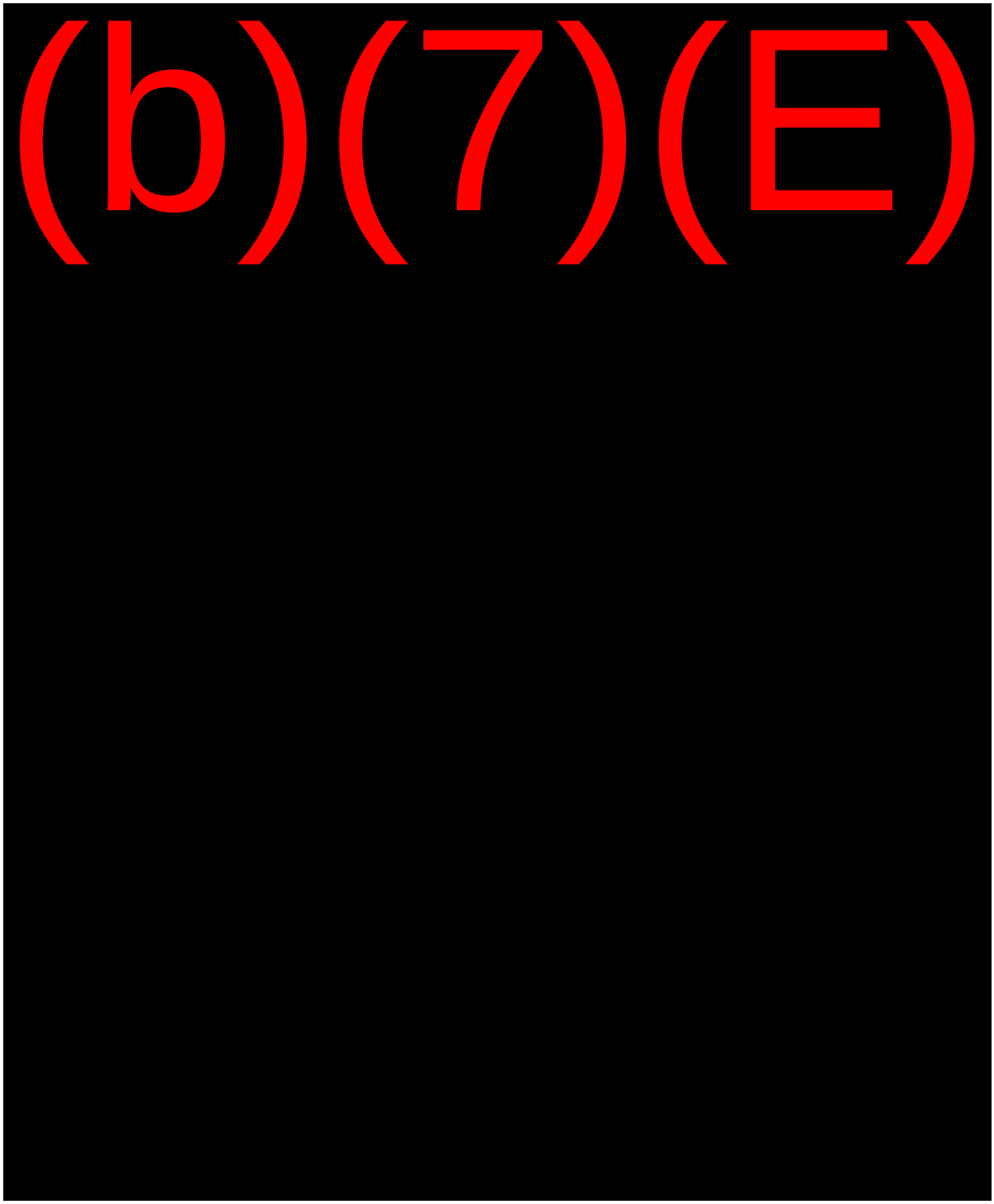

(b)(7)(E)


(b)(7)(E)

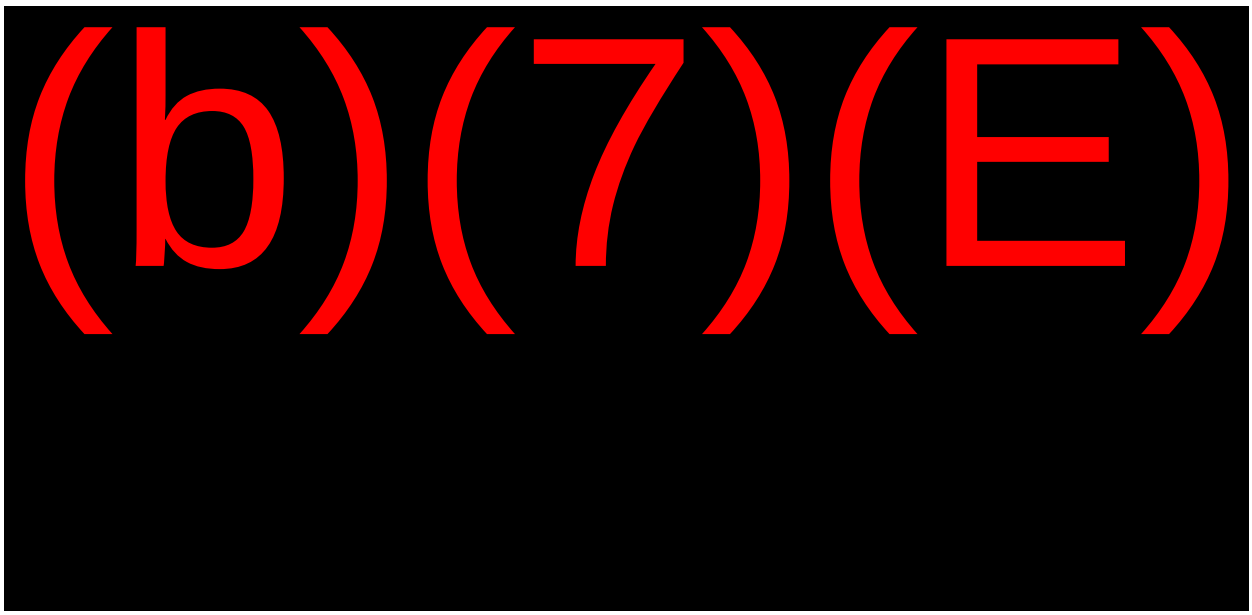

(b)(7)(E)

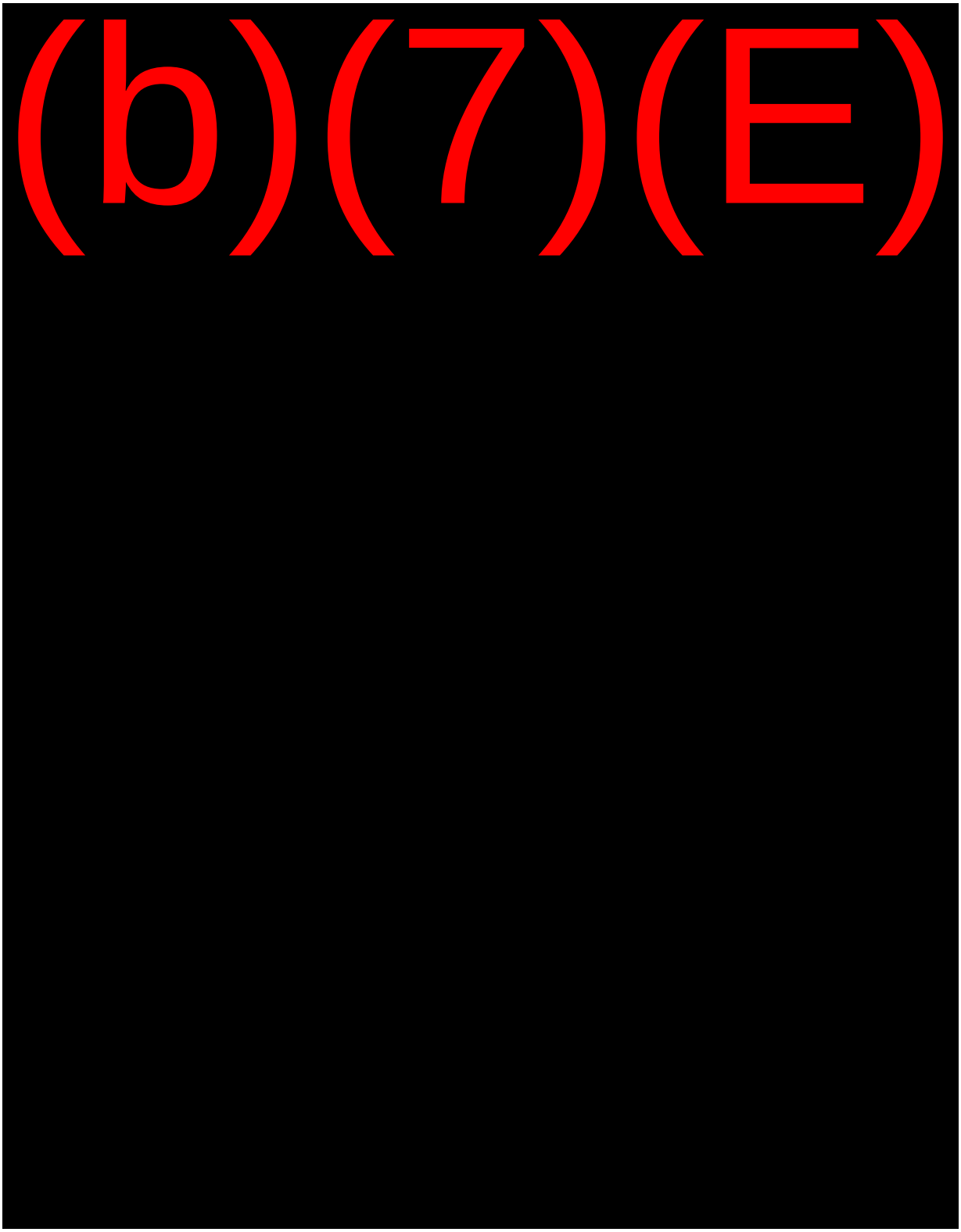

(b)(7)(E)

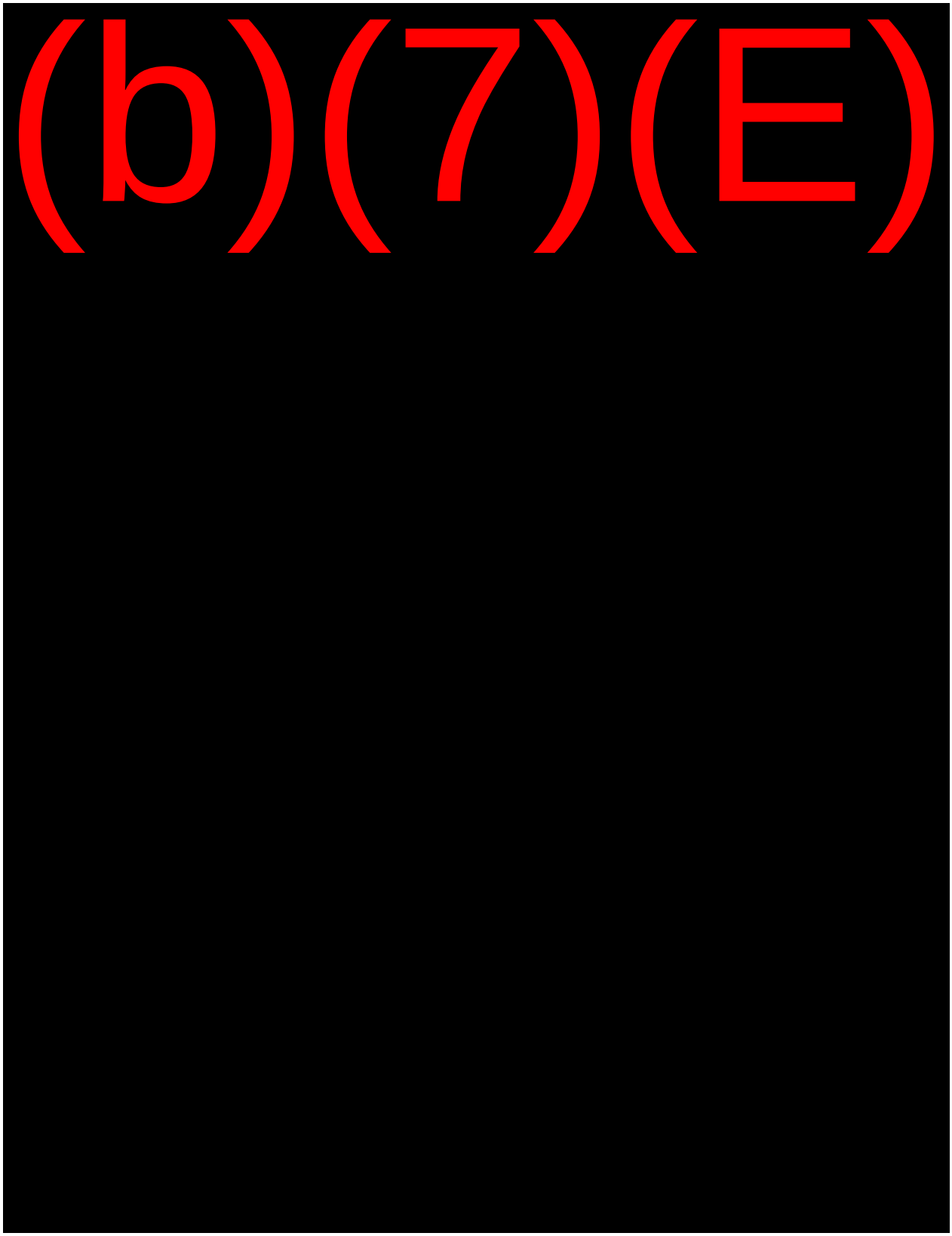

(b)(7)(E)

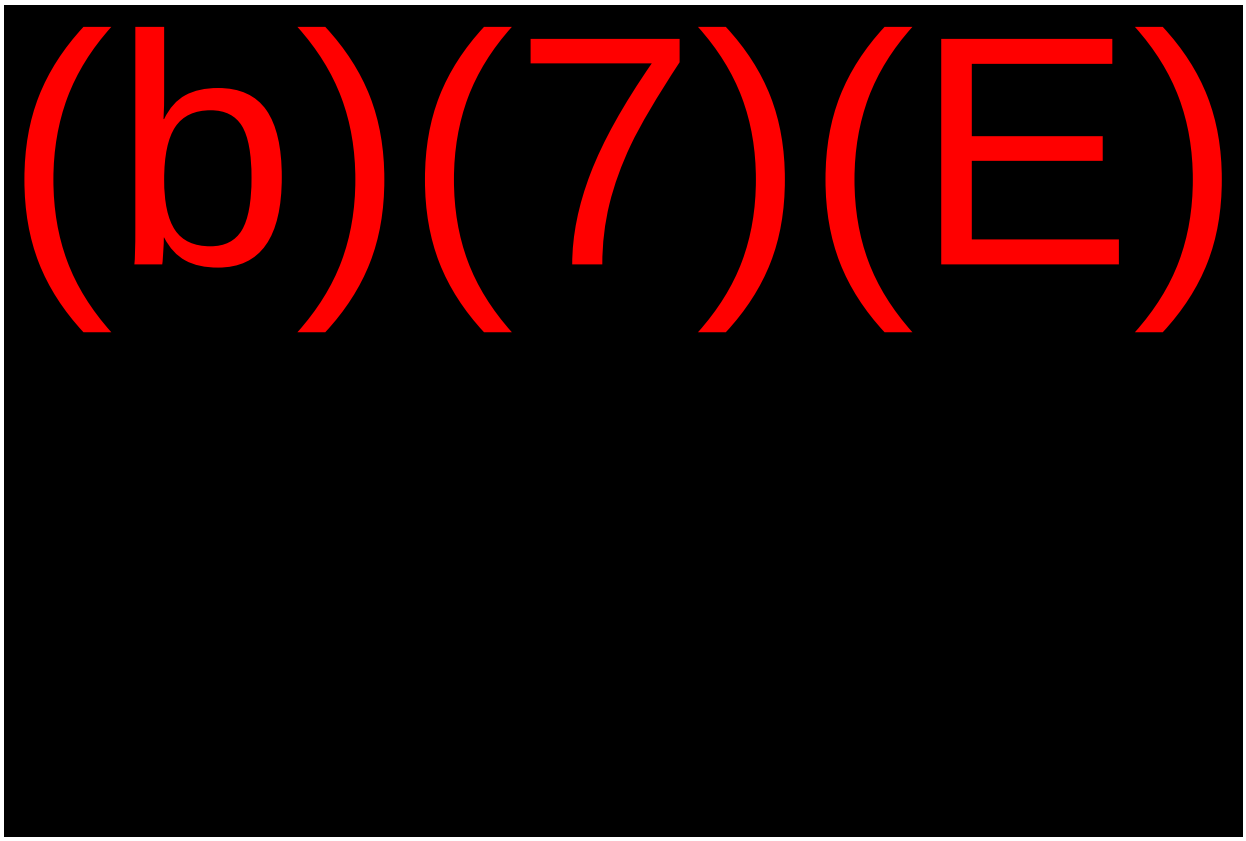

(b)(7)(E)

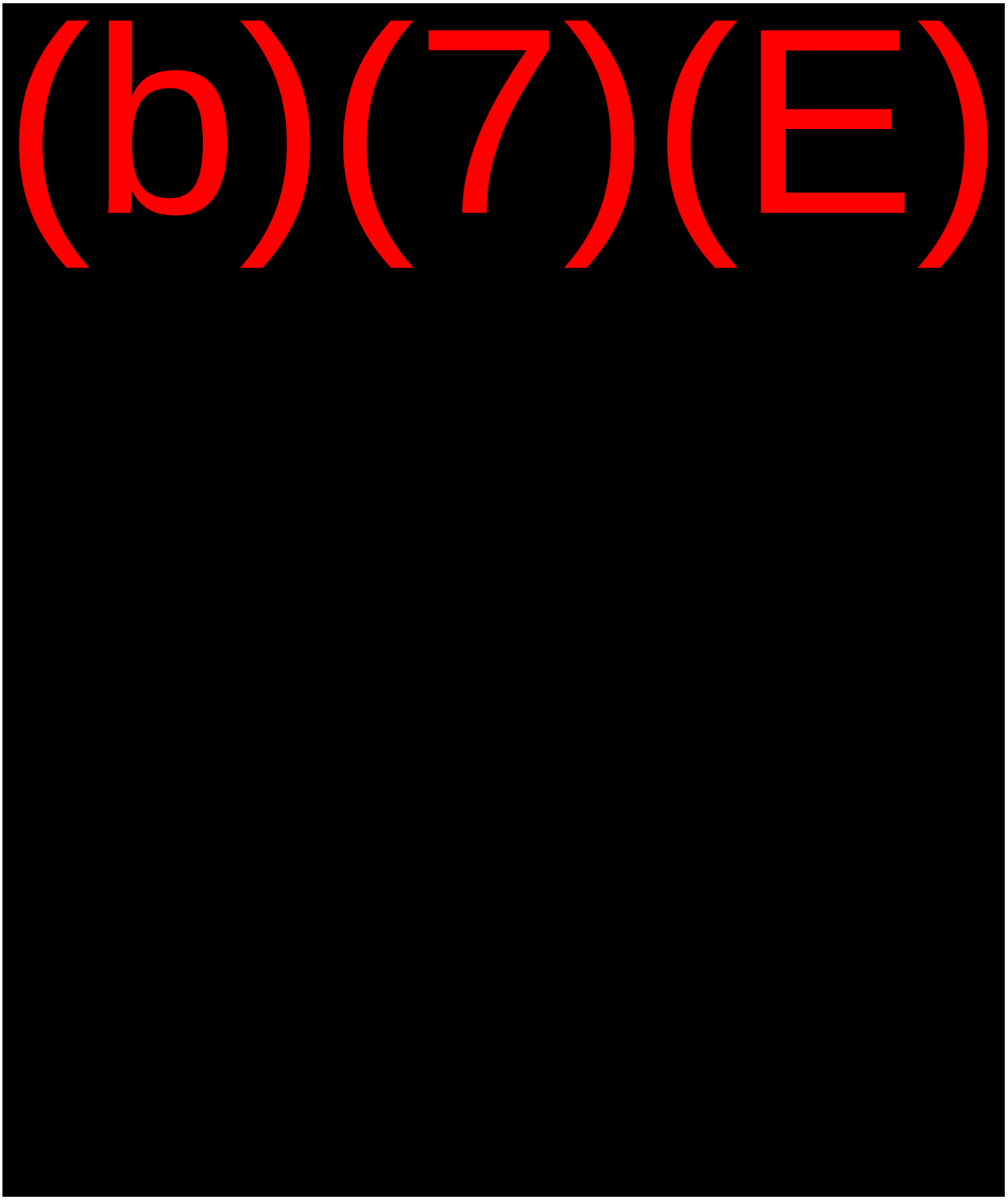

(b)(7)(E)

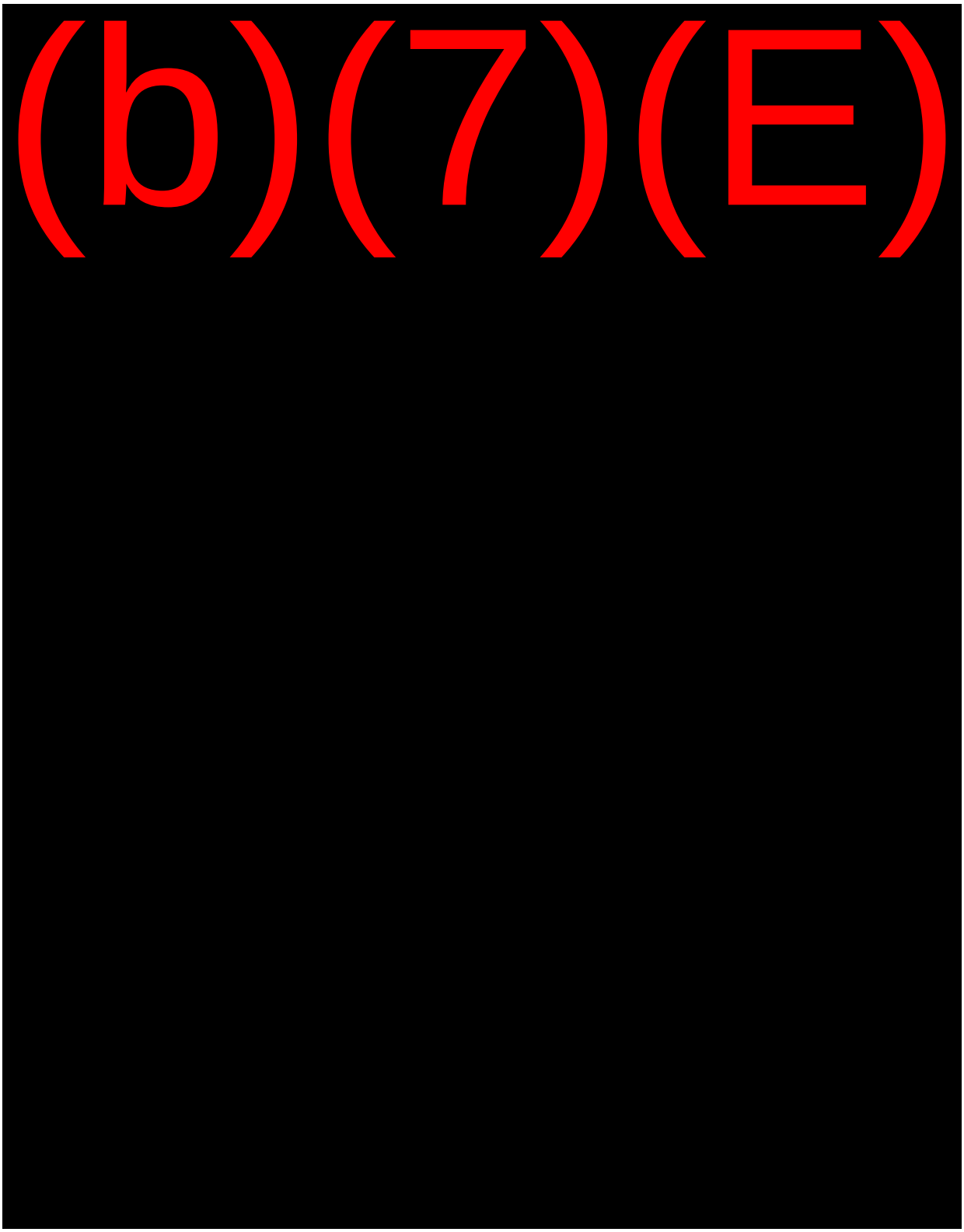

(b)(7)(E)


(b)(7)(E)

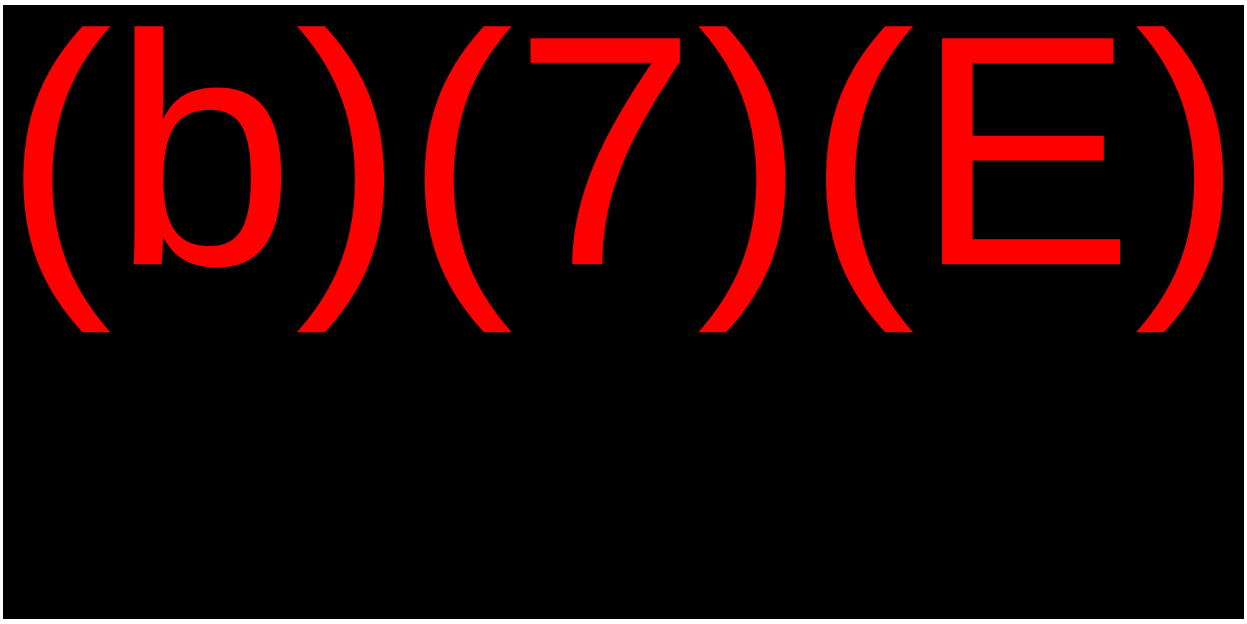

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

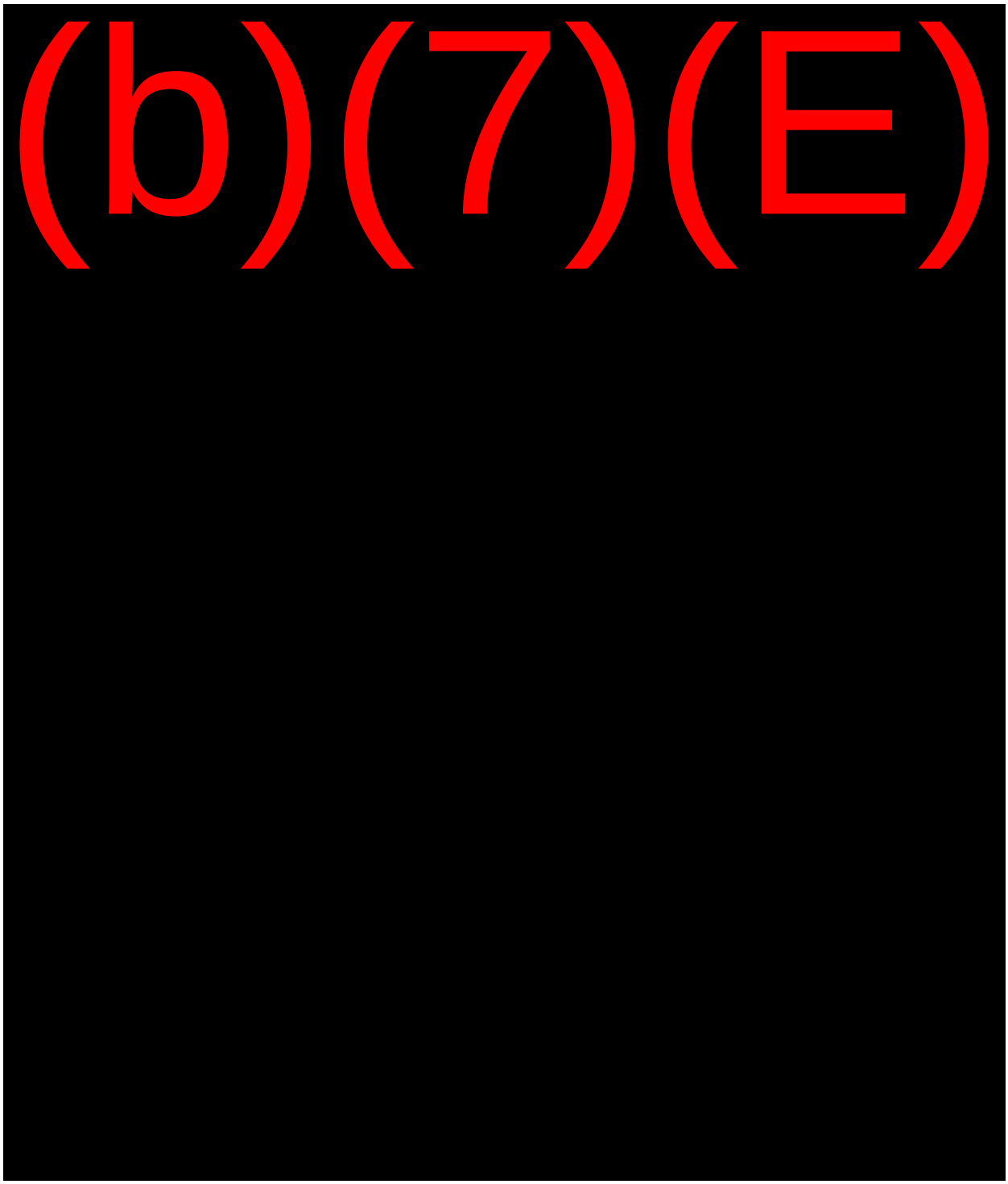

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

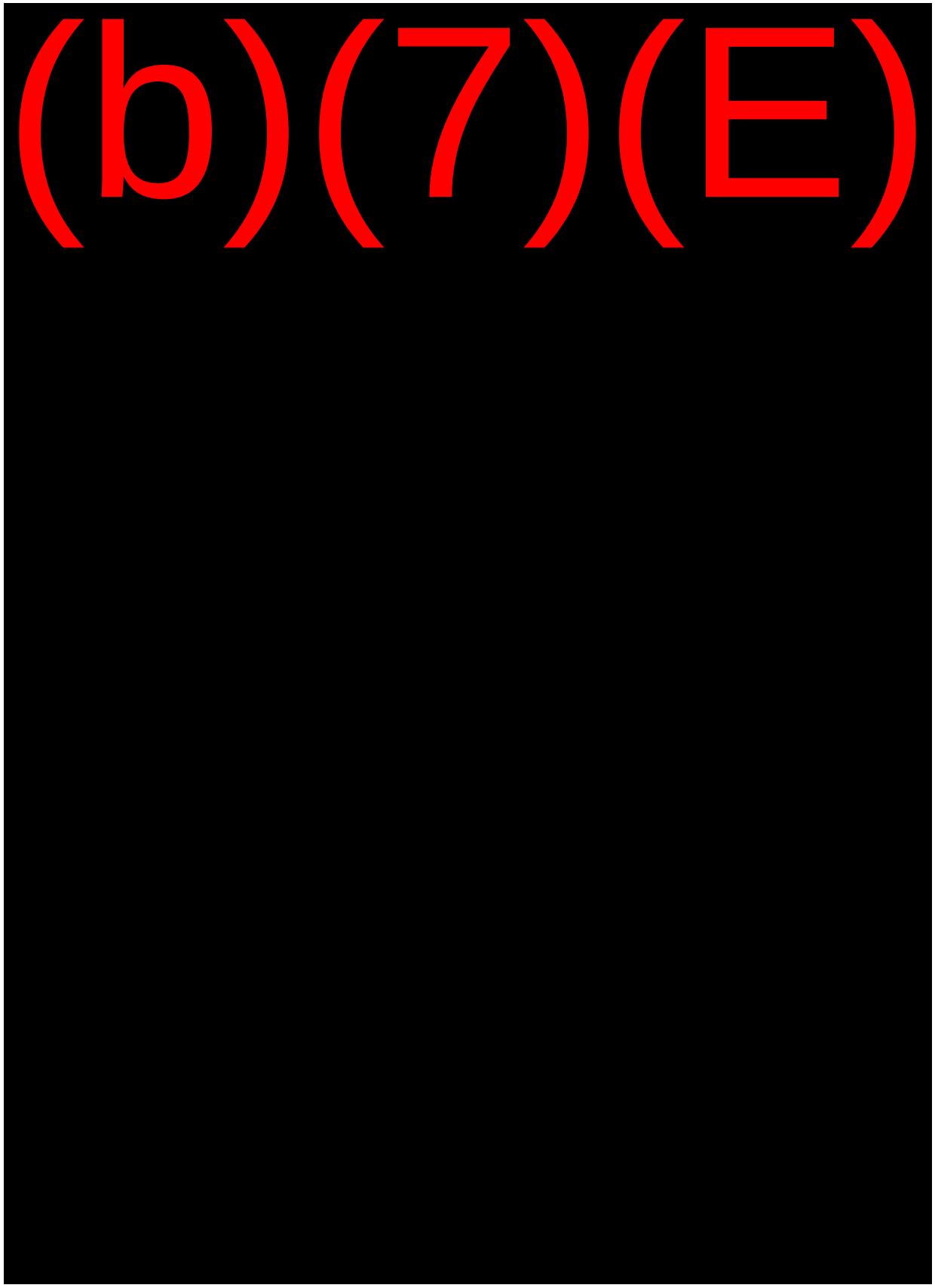

(b)(7)(E)

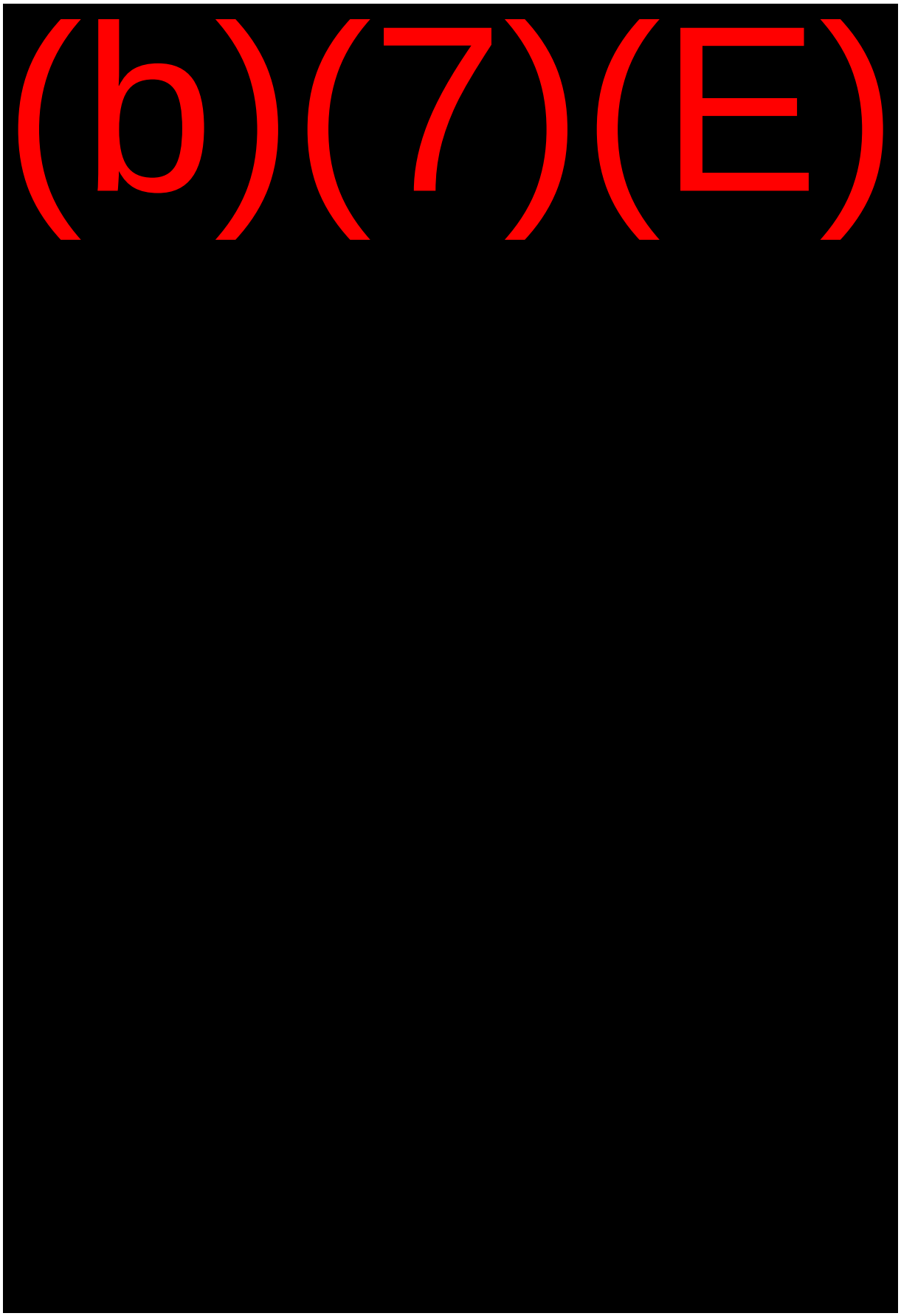

(b)(7)(E)

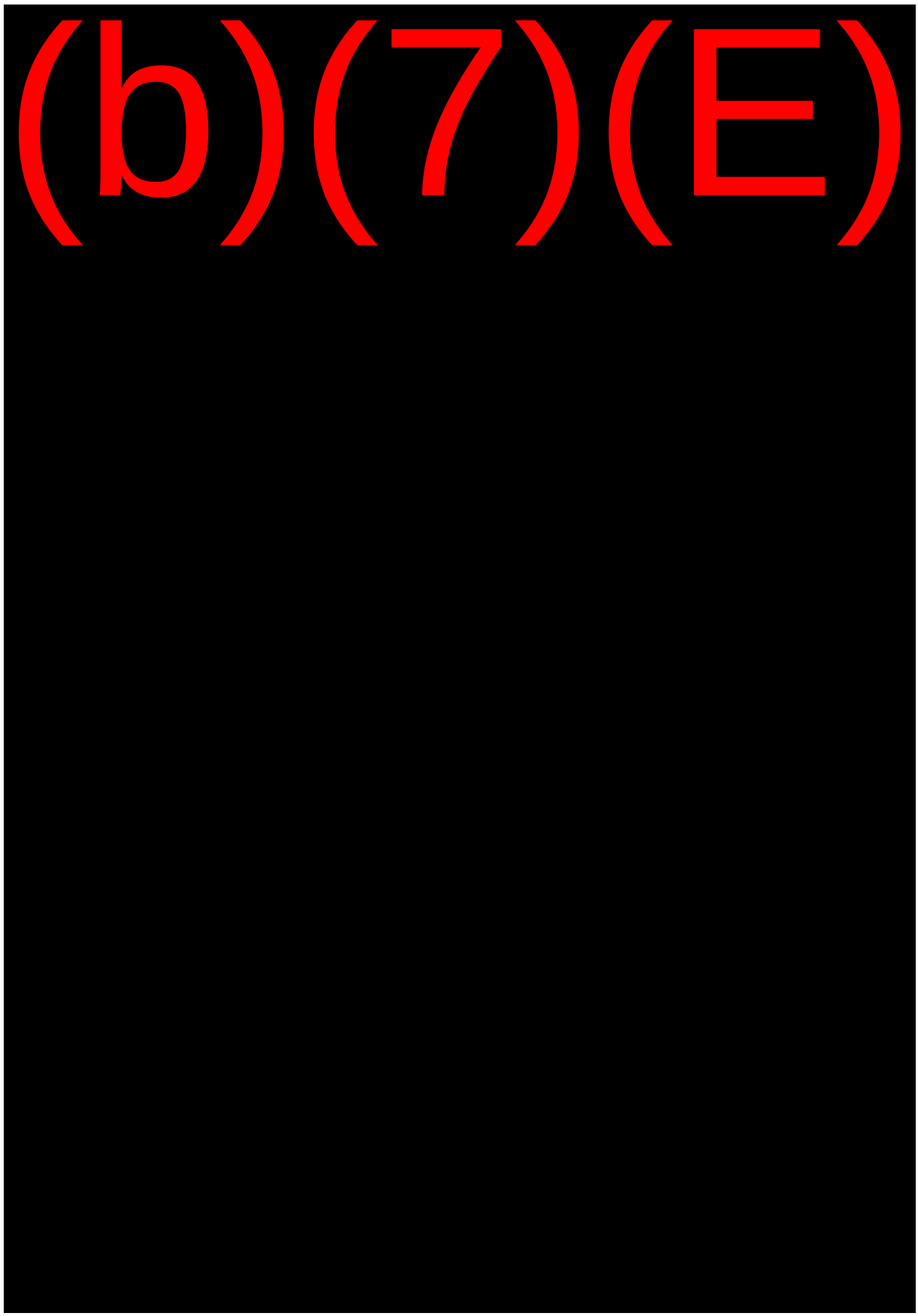

(b)(7)(E)

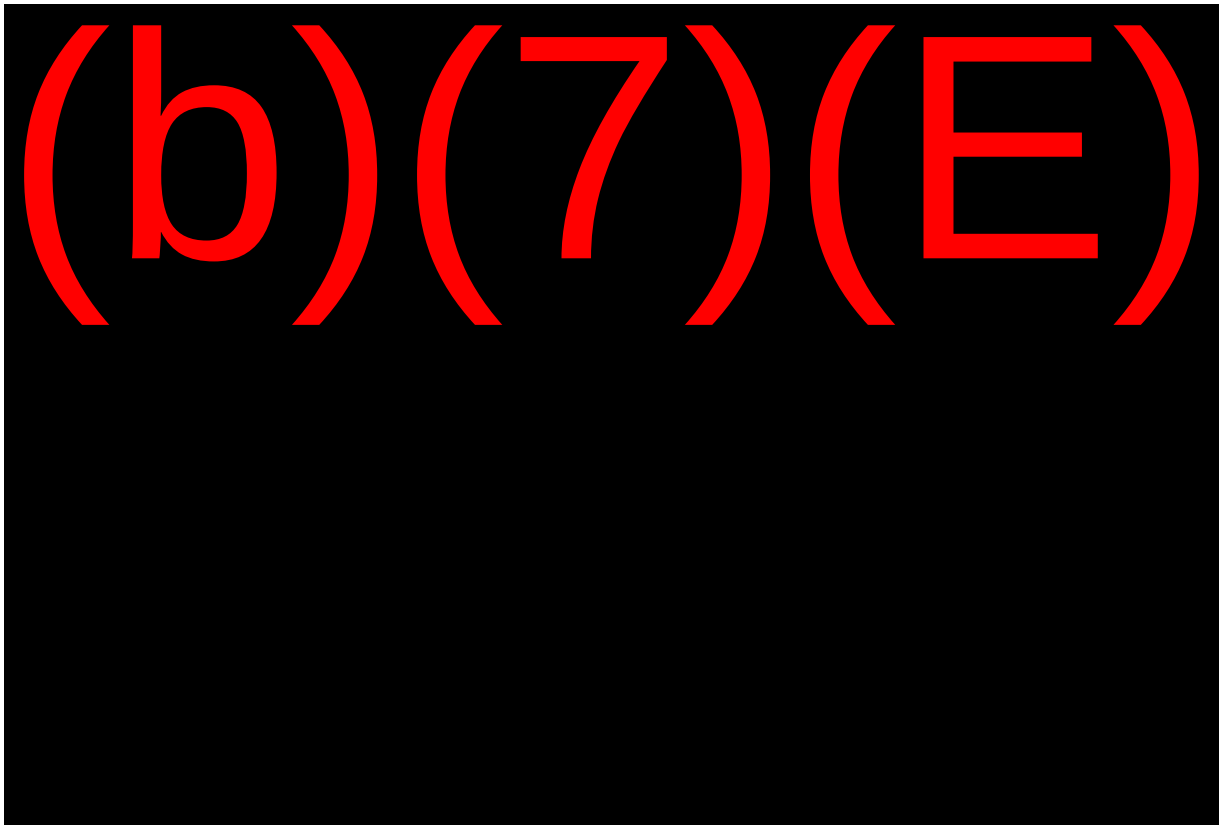
ITSM APPENDICES

This page is intentionally blank.

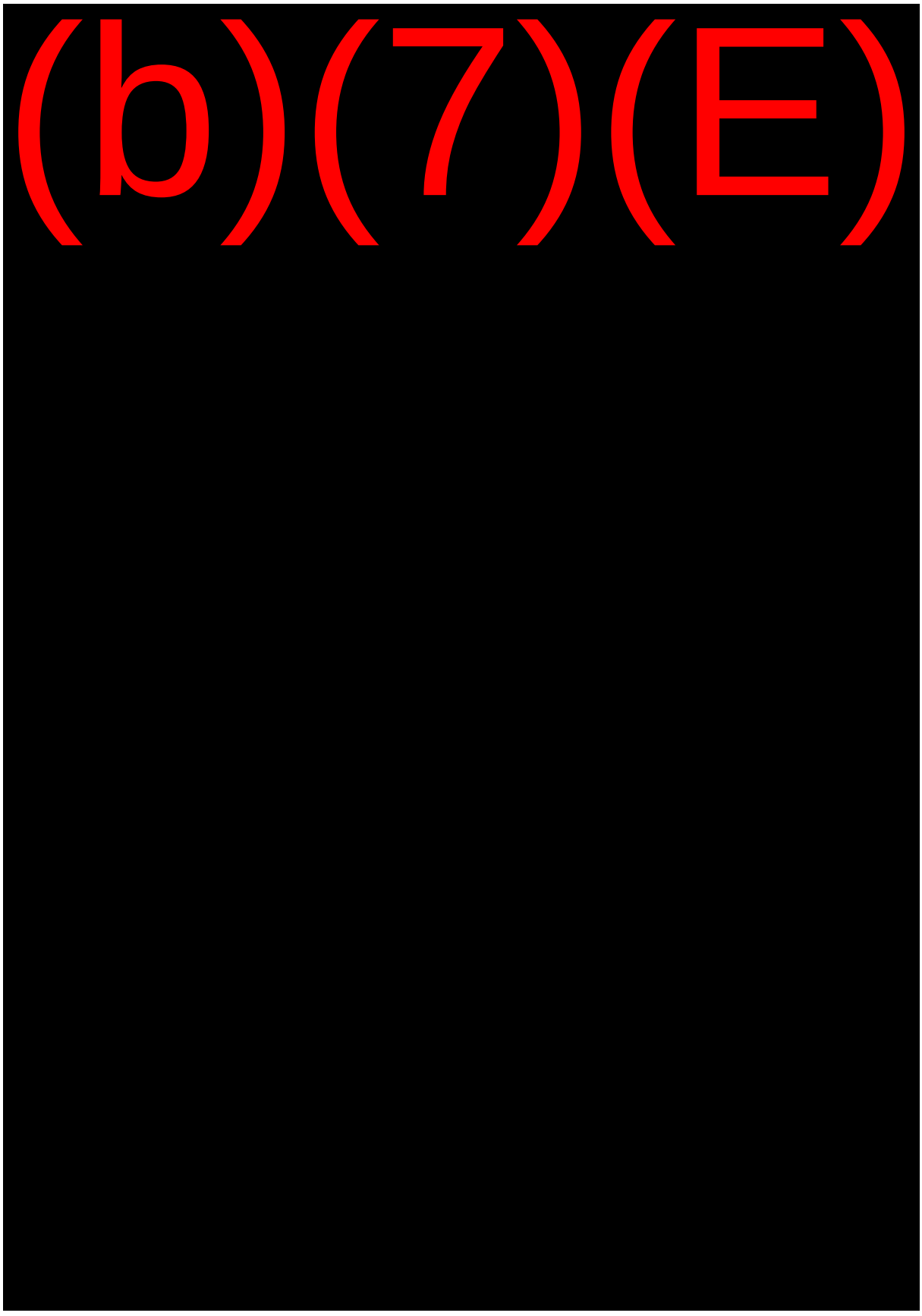

(b)(7)(E)

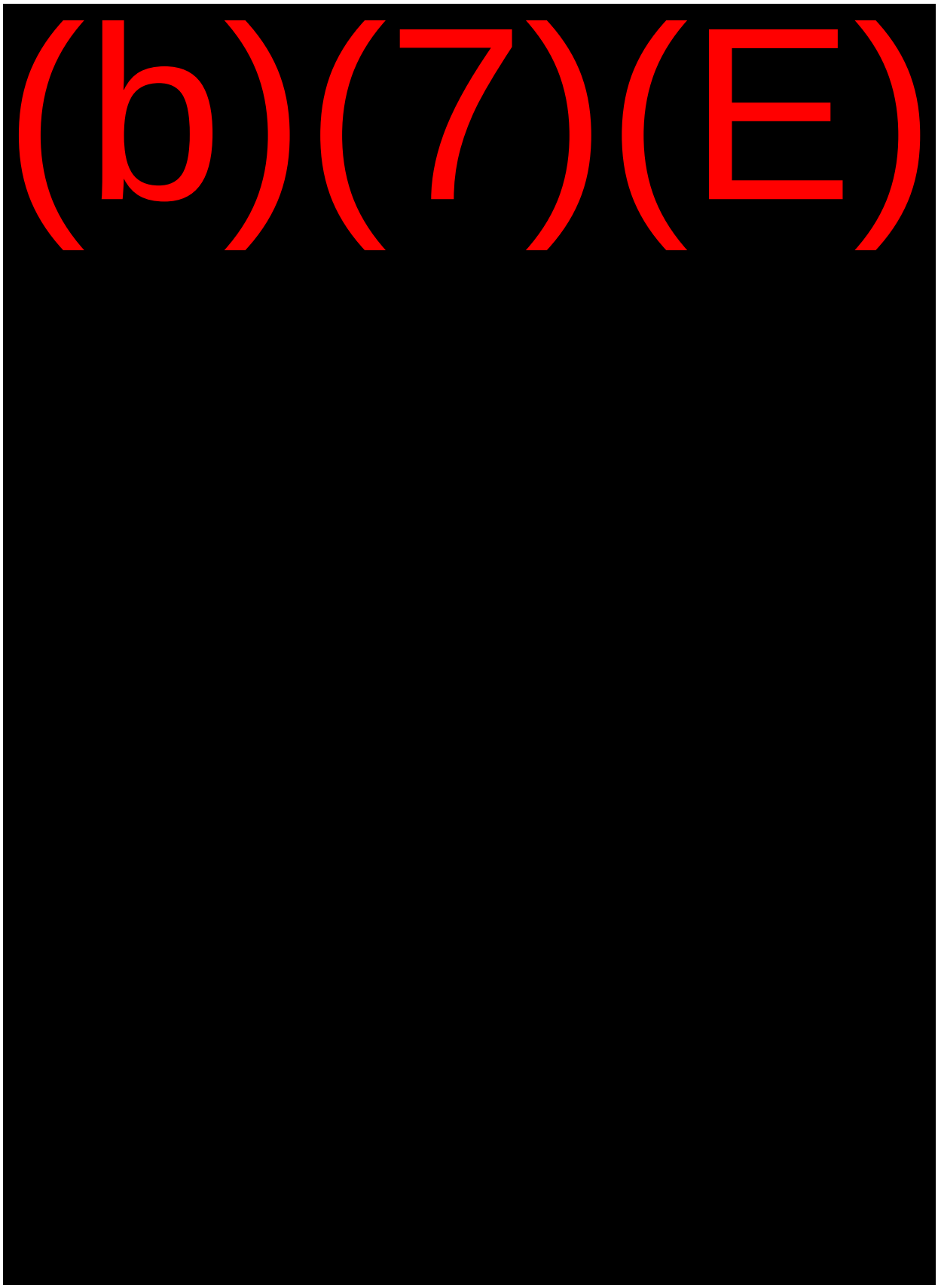

(b)(7)(E)

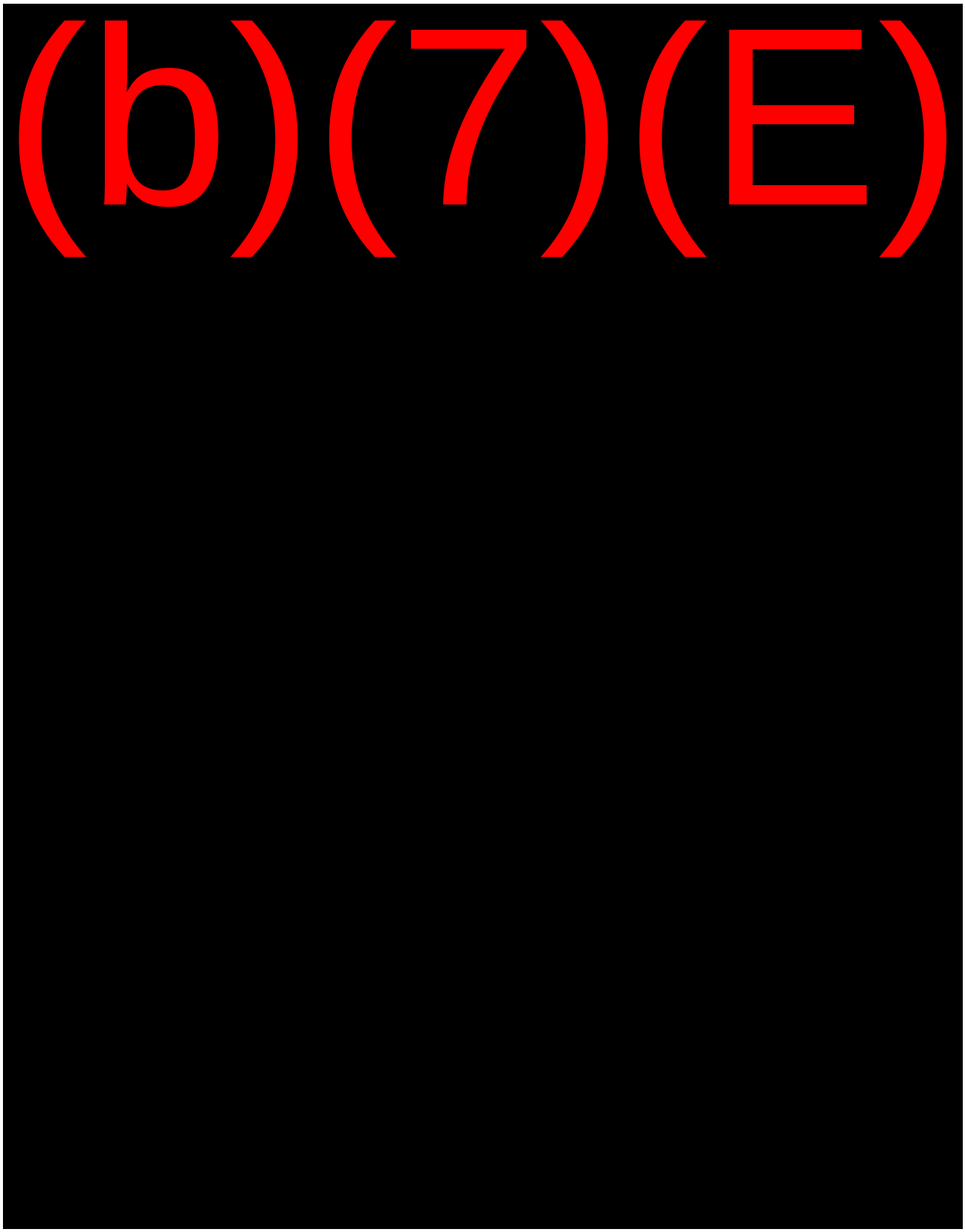

(b)(7)(E)

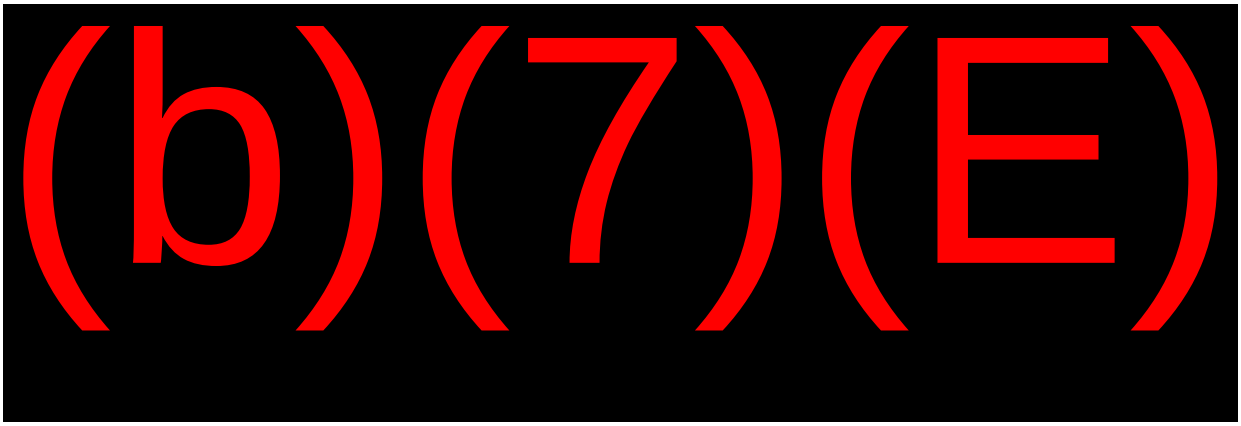

(b)(7)(E)

Appendix B: Wireless Security


(b)(7)(E)

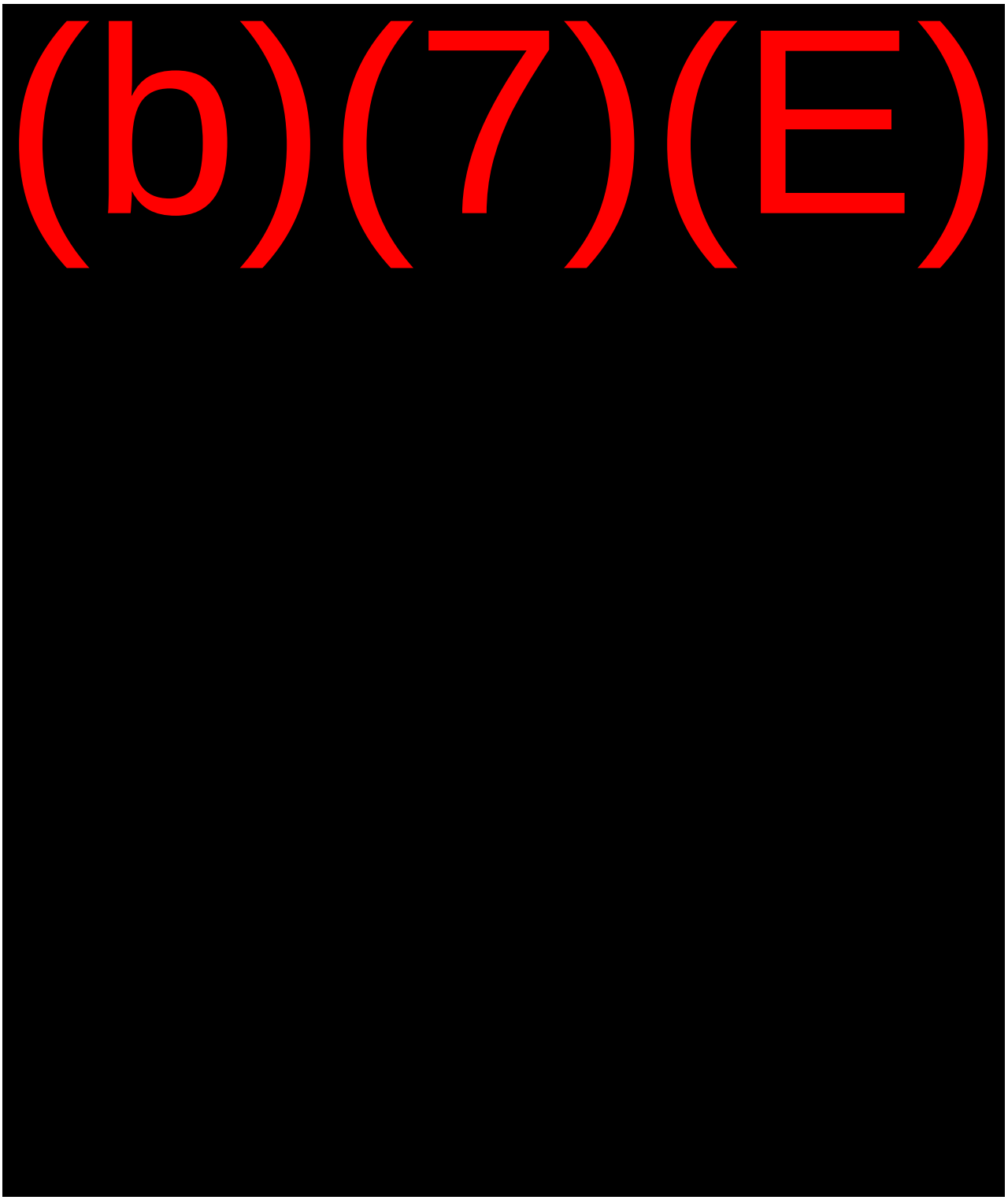

(b)(7)(E)

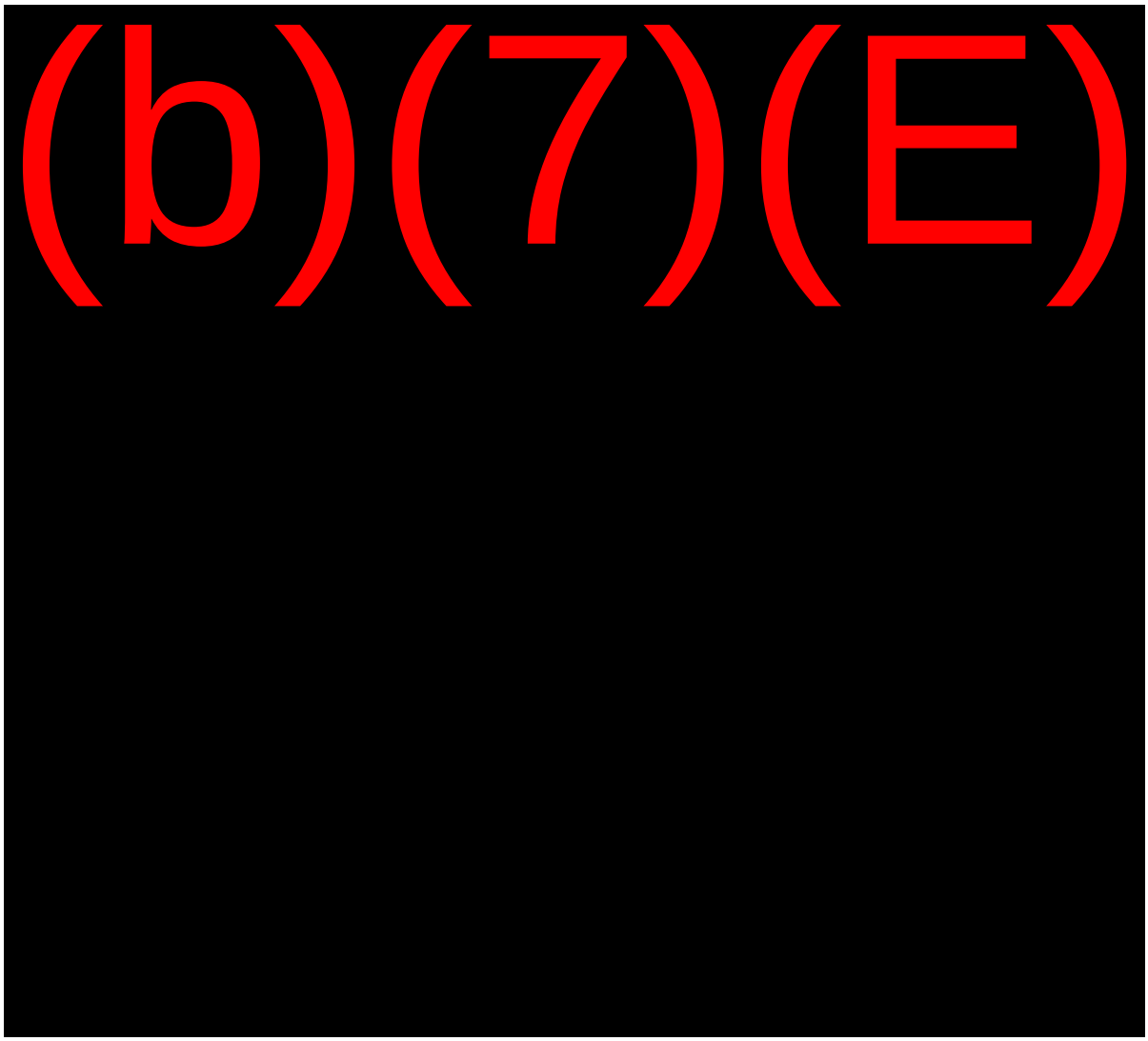

(b)(7)(E)


(b)(7)(E)

Appendix C: Remote Access Agreement

National Oceanic and Atmospheric Administration (NOAA)
Unclassified System Remote Access Approval and User Agreement
(Example)





User's Printed Name/Signature _____ Date

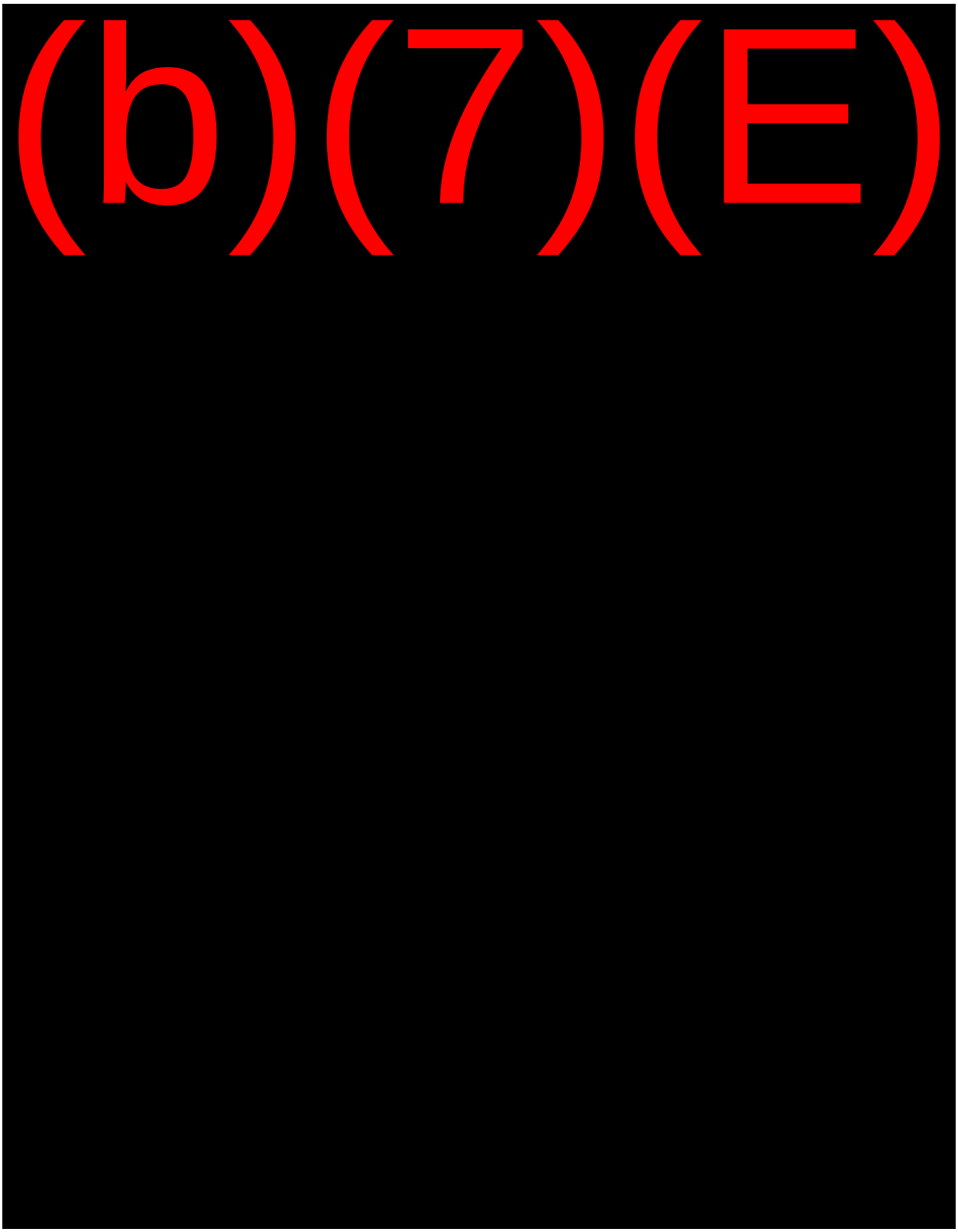
APPROVAL:

Remote access, as described in this agreement, is approved_____ disapproved_____

Printed Name/Signature, Information System Owner _____

Date

Appendix D: Voice over Internet Protocol




(b)(7)(E)

Appendix E: Security Training

NOAA Augmented Security Awareness and Training: FISMA, this document and higher level policies require mandatory periodic training for all employees involved in the management, use or operation of Federal computer systems. This includes contractors as well as employees of the agency. NOAA Security training shall conform to guidance provided in the NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role-and Performance-Based Model*, and will consist of training in basic computer security, security planning and management, computer security policy and procedures, contingency planning and systems life cycle management.

System owners shall determine the level or extent of such security training required to support the security posture and delineate which training shall be mandatory to grant access to their systems. All NOAA Employees including Contractors and Affiliates will complete the NOAA IT Security Awareness Training at https://www.csp.noaa.govwithin 3 days of entry and agree to abide by the NOAA rules of behavior prior to being granted access to NOAA IT resources. This shall be considered minimum mandated security training for access. System Owners will enforce mandatory training by requiring its completion within the specified time frame or revoking system access if not completed after 3 days of entry on duty and if annual refresher training is not completed by the specified deadline for continued access.

All IT Security Awareness training must be recorded in the NOAA Learning Management System (LMS).

IT Security Awareness, Training, and Education. The types of security learning activities applicable to the NOAA environment include:

1. **Awareness**: Programs and products designed to convey general security information to all NOAA systems users. Such activities range from conducting new employee orientation briefings to security alert services, web-based courses for introduction to government computer security requirements, ad hoc awareness events, creating security literature, and promoting good security through the NOAA IT Security Website.
2. **Training**: Programs and products designed to provide more specific information to enable NOAA systems users functional support and needed security skills and competency relevant to their job role. Training topics include: Security Planning and Management activities covering risk assessment, threat analysis, security training ("train the trainers"), and technical information for systems staff in security configuration and security compliance monitoring.
3. **Education**: Programs and products designed to integrate all security skills and competencies into a common body of knowledge, adding a multi-disciplinary study of concepts, issues and principles. Formalized education for individuals seeking professional certifications in IT security is included in this group.
4. **Refresher Activities**: Programs and products designed to provide continuing education to the NOAA community on relevant security topics. Such programs include annual briefings, distance education refresher products, and related items.

NOAA Augmented IT Security Awareness, Training, and Education Program Requirements. The NOAA IT Security Awareness, Training, and Education Program shall ensure a consistent level of understanding that complies with Law, DOC and NOAA IT security training policies. Mandatory requirements are:

A. All new employees are required to attend the New Employee Orientation Briefing on IT Security. In addition, they are required to complete the web-based security training course within 3 days of entrance on duty.

B. IT security training above the awareness level shall be provided to personnel who manage, design, implement or maintain systems.

C. LO SOs shall ensure that all network and system administrators having responsibility for performing installation, configuration and maintenance of systems and networks are identified and receive appropriate training in systems security. ACIOs will ensure system owners implement and manage tailored IT security training for individuals with privileged access

D. All NOAA system-specific training includes:

1) Awareness specific to the system (patch bugs and fix message distribution, posters, booklets, and trinkets);

2) Documentation of the type and frequency of system-specific security training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the-job training); and

3) Procedures for assuring that employees and contractor personnel have been provided and completed system-specific training shall be documented in the SSP (control AT-1).

E. LOs and systems shall augment of the NOAA training program as required to ensure awareness of locally sensitive security issues. An example might be specific daily requirements for IT security on board NOAA ships. Security Awareness, Training and Education Programs will be designed and provided to meet the mandatory general and specialized requirements (based on the employee's role/job function) as identified in Table 1, Mandatory IT Security Awareness, Training, and Education Requirements.

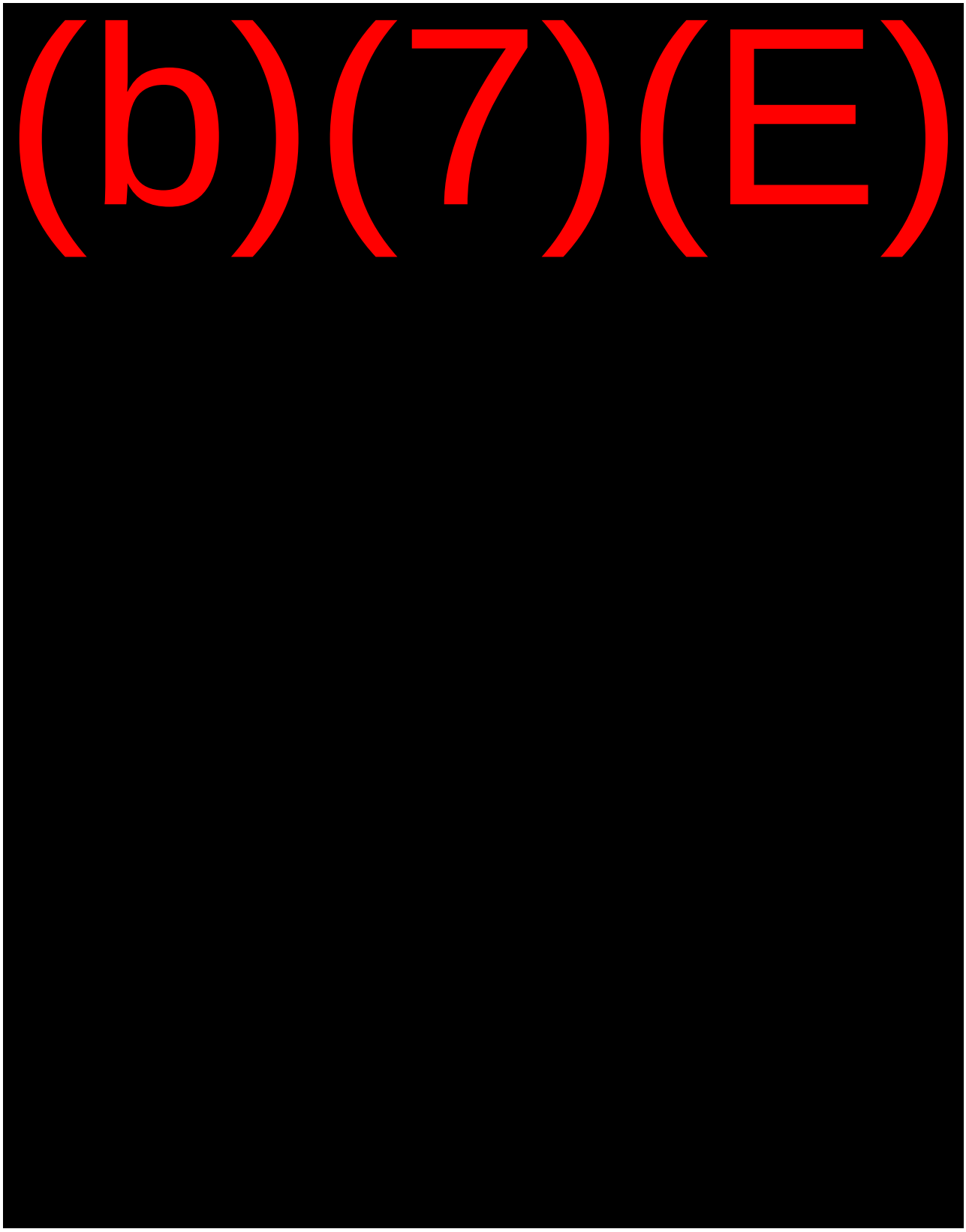
F. Additional IT security training annually that maintains a level of proficiency to support the evolving security needs of the system. This may be a mix of technical and security awareness training offered by many sources (e.g., SANS Institute, N-CIRT workshops, DOC and NOAA E-Learning etc). Additional SANS courses may be available to NOAA employees at a discount. Information on those SANS courses can be found at: https://www.csp.noaa.gov/tea/

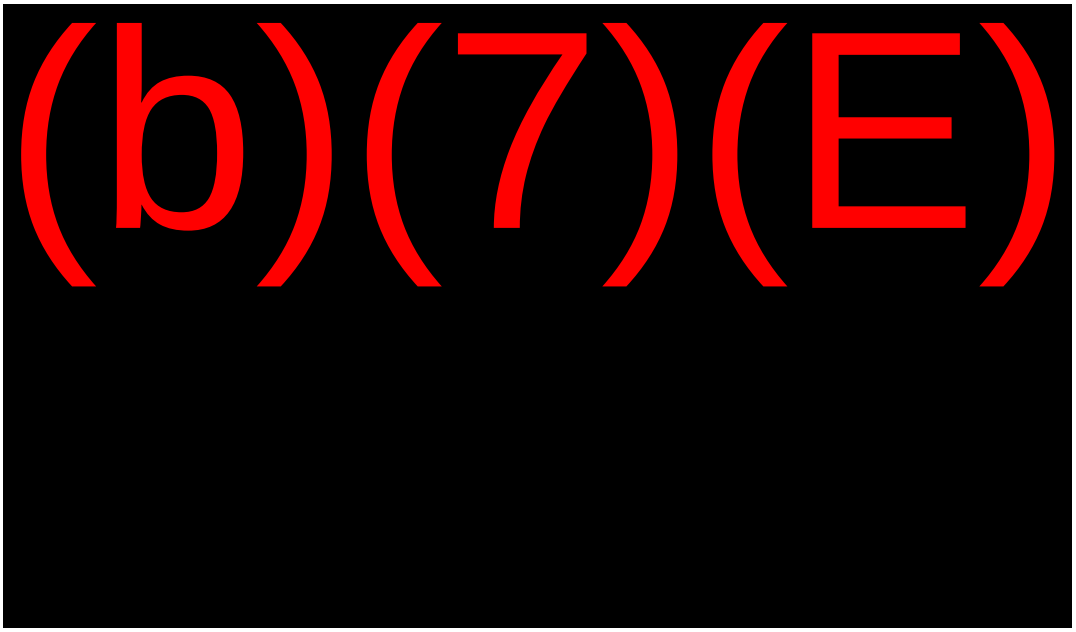
Table 1, Mandatory IT Security Awareness, Training, and Education Requirements

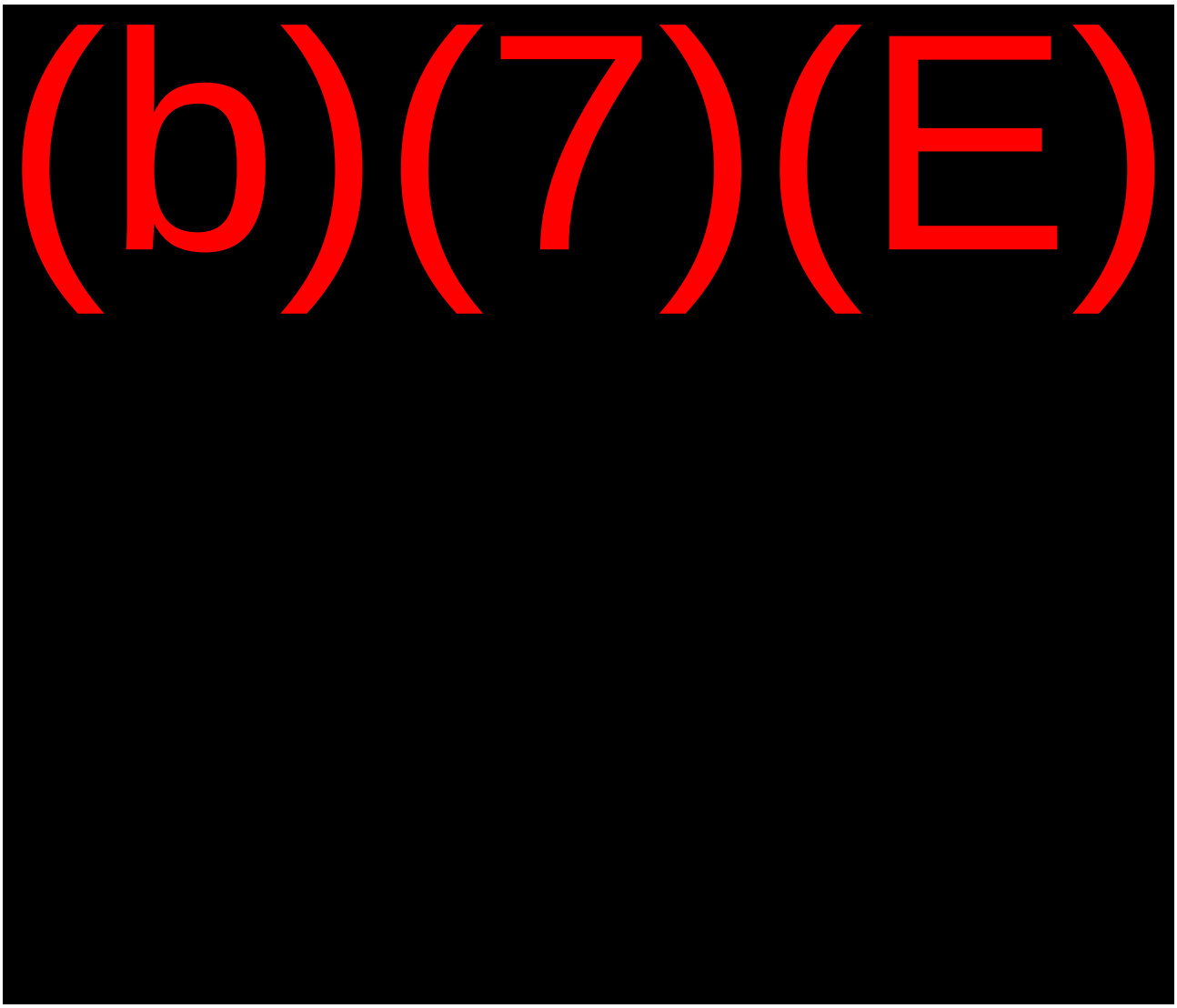
Role/Job Function	Mandatory General Security Awareness and Training Requirements	Mandatory Specialized Security Training and Education Requirements
Senior Management and Budget Officials	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 3 days of entrance on duty)	
System Owners	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 3 days of entrance on duty)	• See CITR-006
SAISOs, ITSOs, ISSOs	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 30 days of entrance on duty)	• Must possess CITR-006 approved professional certification upon appointment and provide annual evidence of credential maintenance.
Network and System Administrators	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 3 days of entrance on duty)	
General IT User	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 3 days of entrance on duty and annually)	

Sources for all of the above training are located on the **NOAA Training, Education. and Awareness page**

Appendix F: Vulnerability Management



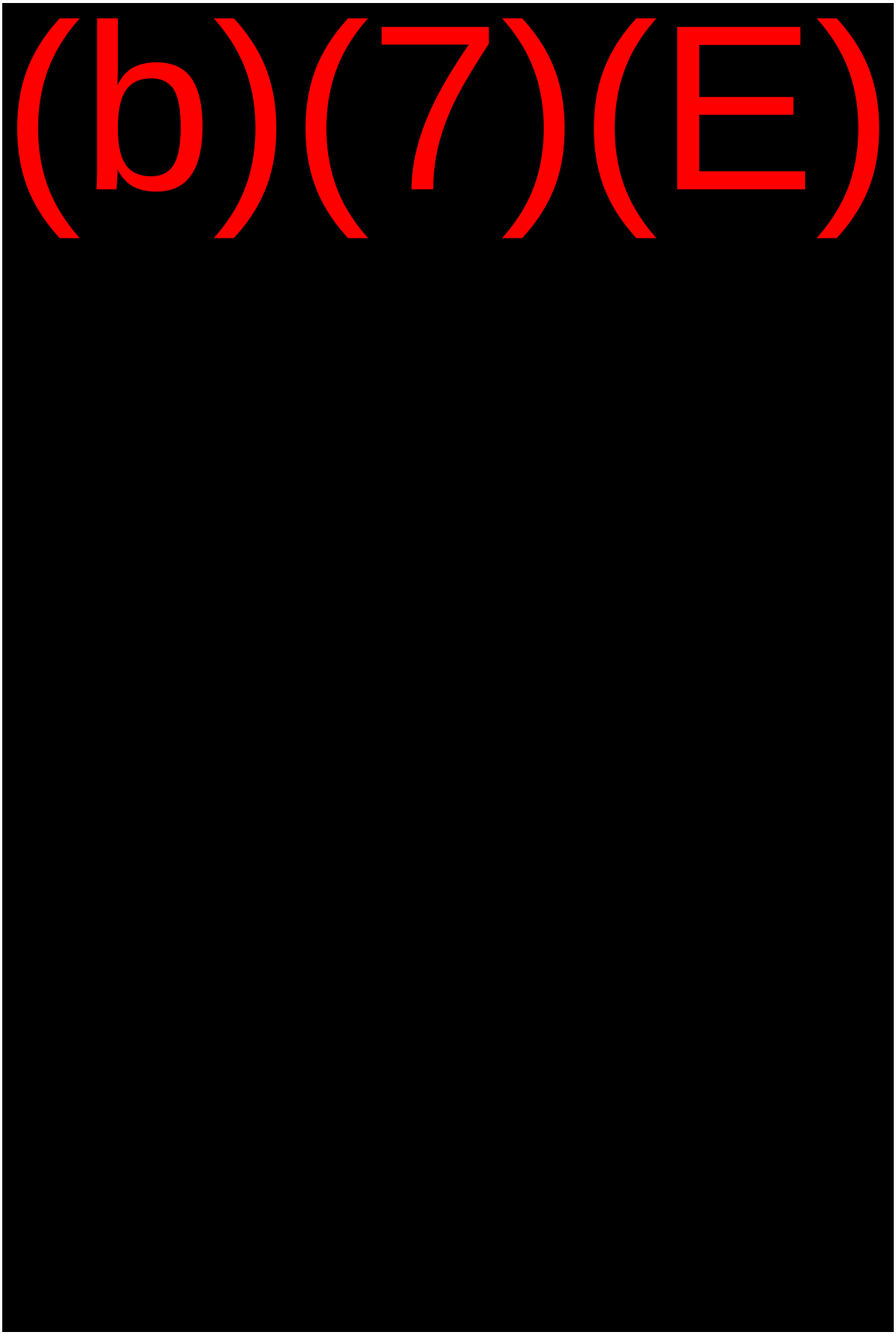

(b)(7)(E)


(b)(7)(E)

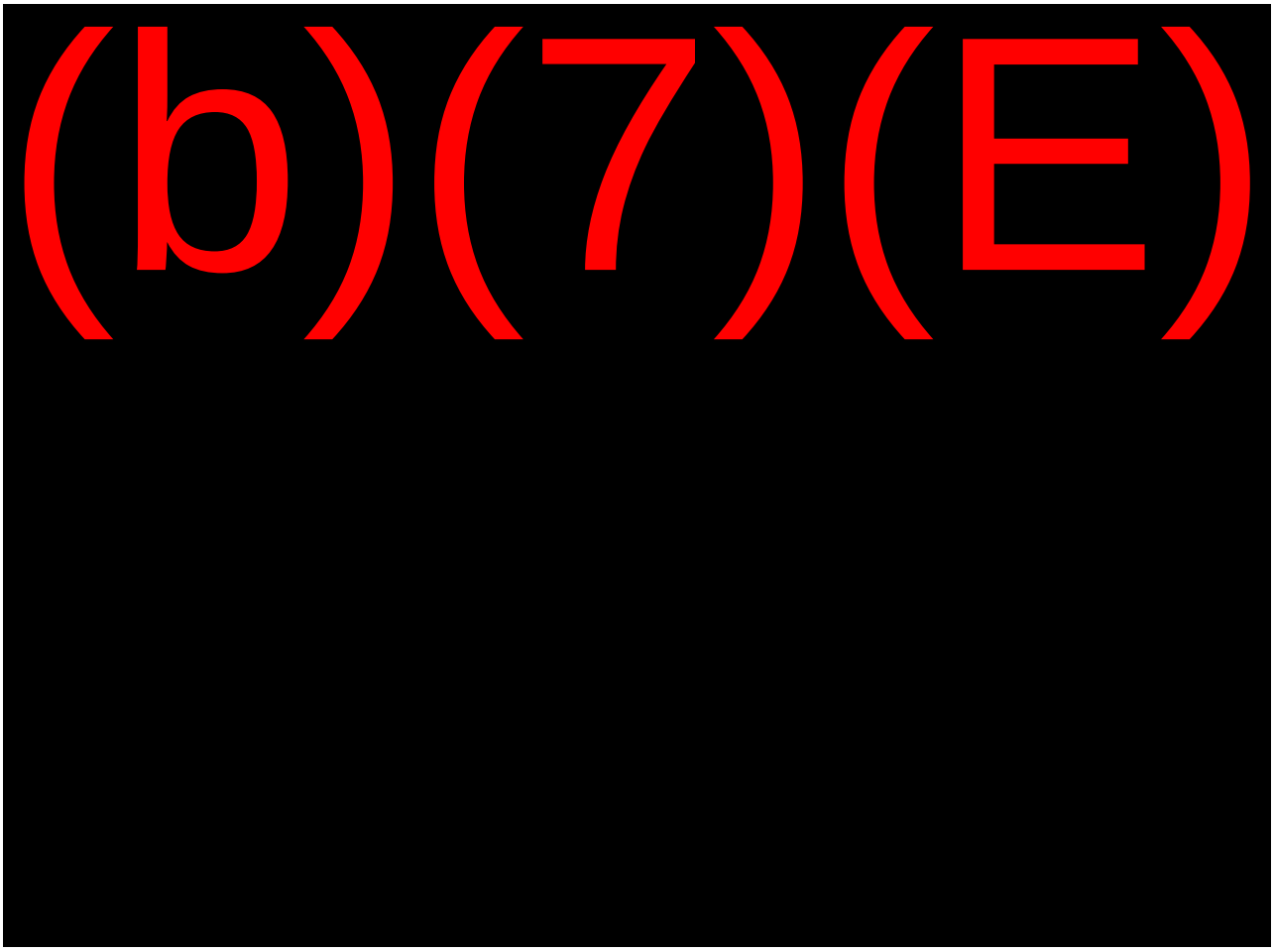

(b)(7)(E)


(b)(7)(E)

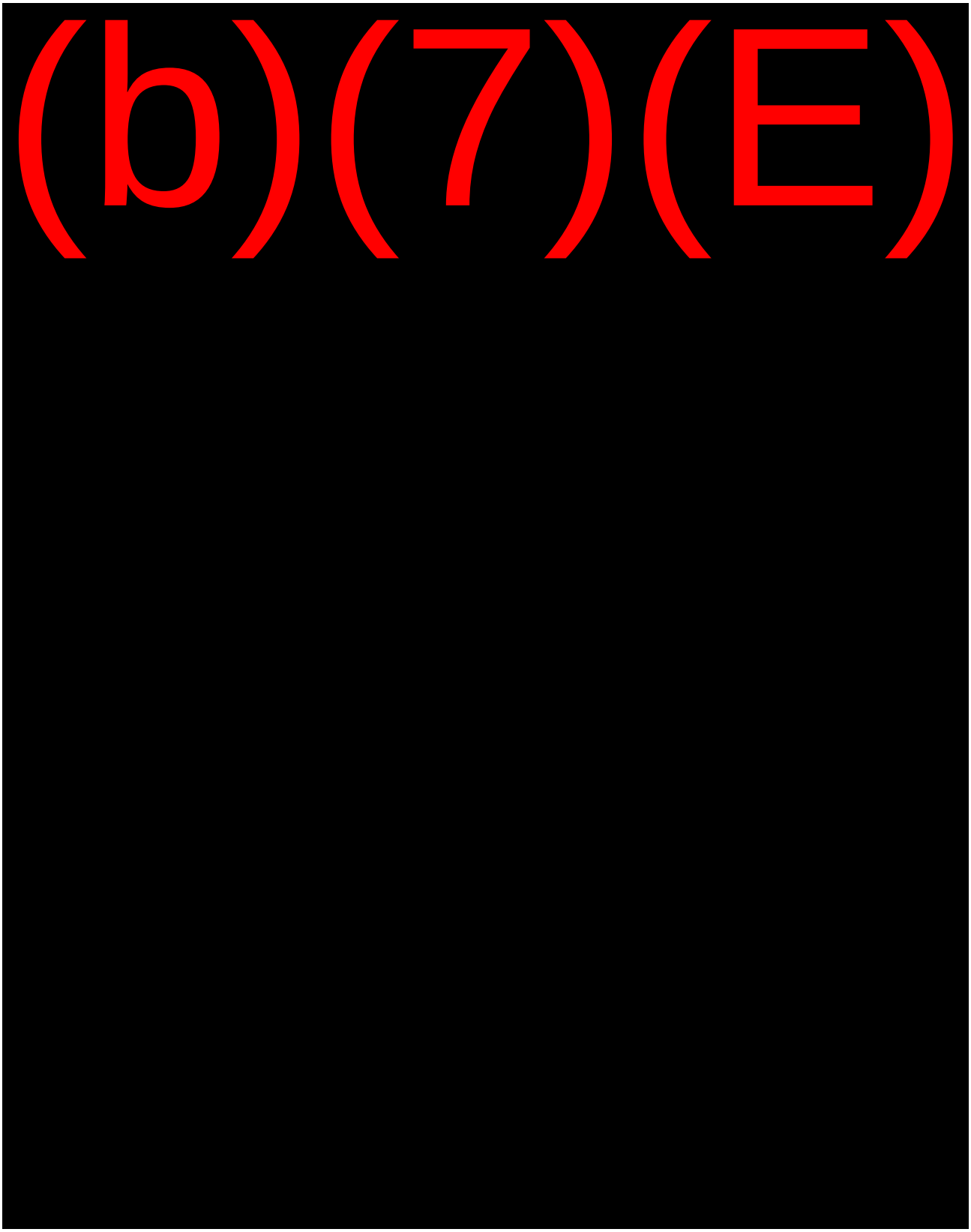

(b)(7)(E)

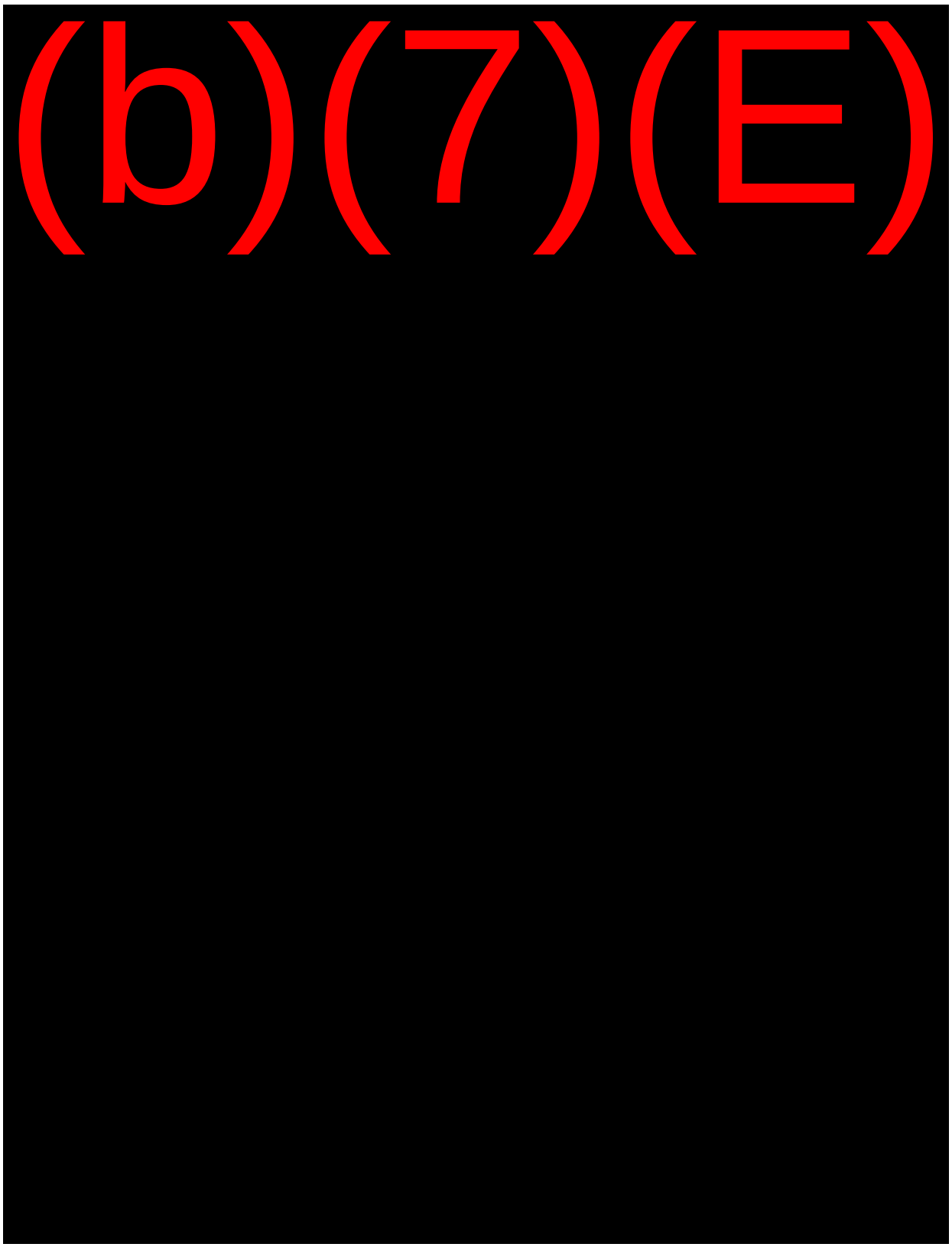

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

Appendix G: Privacy Controls




(b)(7)(E)

E-mail a link to this directive

OFFICE OF INSPECTOR GENERAL

Number: DOO 23-1

Effective Date: 2013-04-26

SECTION 1. PURPOSE.

.01 This Order prescribes the organization and functions of the Office of Inspector General (OIG) established in the Department of Commerce (the Department) under the Inspector General Act of 1978, 5 U.S.C.A. Appendix 3 as amended (the Act). The scope of authority and functions of the Inspector General are set forth in Department Organization Order 10-13.

.02 This revision updates the Order to incorporate the statutory changes brought about by the Inspector General Reform Act of 2008; reflect the recent reorganizations approved by Congress in May 2008 and September 2011, to reflect the current organization of the OIG and to incorporate title changes of certain subordinate officials who assist the Inspector General. Specifically, this Order eliminates the positions of Assistant Inspector General for Inspections and Program Evaluations and Assistant Inspector General for Systems Evaluation. This revision establishes the positions of Associate Deputy Inspector General, Principal Assistant Inspector General for Audit and Evaluation, and Principal Assistant Inspector General for Investigations.

SECTION 2. ORGANIZATION.

The OIG, directed by the Inspector General, is composed of the immediate office of the Inspector General, the Office of Audit and Evaluation, the Office of Investigations, the Office of Administration, and the Office of Counsel to the Inspector General. The OIG conducts its operations at headquarters offices located in the Herbert C. Hoover Building in Washington, D.C., and at such regional and field offices as may be established by the Inspector General.

SECTION 3. OFFICE OF AUDIT AND EVALUATION..

.01 Organization. The Office of Audit and Evaluation (OAE) will be headed by the Principal Assistant Inspector General for Audit and Evaluation (PAIGAE) who shall be responsible for supervising the performance of audits, evaluations, and inspections relating to the programs and operations of the Department, and will report and be responsible to the Deputy Inspector General and/or the Inspector General. The PAIGAE will supervise the performance of all functions and duties assigned to OAE by the Inspector General and will be advisor to, and serve as representative of, the Inspector General on all audits, evaluations, and inspections.

a. The PAIGAE will be assisted by an Assistant Inspector General for Audit (AIGA), an Assistant Inspector General for Systems Acquisition and IT Security (AIG/SAITS), and an Assistant Inspector General for Economic and Statistical Program Assessment (AIG/ESPA).

1. The AIGA will report to the PAIGAE and will be responsible for the audits, evaluations, and inspections carried out by the headquarters audit and evaluation division, and the regional audit offices; will supervise the planning and performance of these audits, evaluations, and inspections; will advise and represent the OIG on matters regarding these audits, evaluations, and inspections; will advise Department officials regarding these audits, evaluations, and inspections; and will represent the OIG with officials of other Federal agencies or other groups regarding these audits, evaluations, and inspections.

2. The AIG/SAITS will report to the PAIGAE and will be responsible for audits, evaluations, and inspections related to the Department's information technology systems, major systems acquisition projects, and IT security; will supervise the planning and performance of systems acquisition, information technology audits, evaluations, and inspections; will advise and represent the OIG on matters regarding these audits, evaluations, and inspections; will advise Department officials regarding these audits, evaluations, and inspections; and will represent the OIG with officials of other Federal agencies or other groups regarding these audits, evaluations, and inspections.

3. The AIG/ESPA will report to the PAIGAE and will generally be responsible for audits, evaluations, and inspections related to the Department's economic and statistical programs; will supervise the planning and performance of economic and statistical program audits, evaluations, and inspections; will advise and represent the OIG on matters regarding these audits, evaluations, and inspections; will advise the Department officials regarding these audits, evaluations, and inspections; and will represent the OIG with officials of other Federal agencies or other groups regarding these audits, evaluations, and inspections.

b. The functions and duties of OAE will be carried out by the Office of Audit, the Division of Systems Acquisition and IT Security, the Division of Economic and Statistical Program Assessment, and such other divisions or specialized units as may be established to facilitate the performance of OAE's assigned responsibilities.

1. Within the OAE, there may be regional and headquarters offices. These offices may be headed by a Director or Regional Inspector General for Audits (RIGA), who reports to the AIGA.

.02 Functions. OAE will conduct, supervise, and coordinate audits, evaluations, and inspections of all organizational units and activities of the Department and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG's mission.

SECTION 4. OFFICE OF INVESTIGATIONS.

.01 Organization. The Office of Investigations (OI) will be headed by the Principal Assistant Inspector General for Investigations (PAIGI), who shall be responsible for supervising the performance of investigative activities relating to programs and operations of the Department, and will report and be responsible to the Deputy Inspector General and/or the Inspector General. The PAIGI will manage the performance of all functions and duties assigned to OI by the Inspector General; will be advisor to and serve as the representative of the Inspector General on all investigative, Hotline, and whistleblower protection matters; will advise Department officials regarding OIG investigative matters; will be responsible for promoting awareness of whistleblower protections throughout the Department; will evaluate the sufficiency of Departmental whistleblower protection policies and activities; and will represent OIG and the Department with officials of the Department of Justice and other Federal agencies or other public or private groups regarding investigative matters covered by the Act.

a. The PAIGI will be assisted by an Assistant Inspector General for Investigations (AIGI), and such other subordinate employees as the PAIGI may appoint to assist in carrying out assigned duties and functions.

1. The AIGI will report to the PAIGI and will supervise the planning and performance of inquiries/investigations; will advise and represent the OIG on matters regarding inquiries/investigations; and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG's mission.

b. The functions and duties of OI will be carried out by the divisions or specialized units as may be established by the PAIGI to facilitate the performance of OI's assigned responsibilities.

.02 Functions. The OI will conduct, supervise, and coordinate criminal, civil, and administrative inquiries/investigations involving Department programs, operations, and personnel, as authorized by the Act; will perform related activities designed to prevent and detect fraud, waste, and abuse related to the programs and

operations of the Department; and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG's mission.

SECTION 5. OFFICE OF ADMINISTRATION.

.01 Organization. The Office of Administration (OADM) will be headed by an Assistant Inspector General for Administration (AIG/ADM), who will report and be responsible to the Deputy Inspector General and/or the Inspector General.

a. The AIG/ADM will supervise the provision and management of administrative resources and services to the OIG, and will be the principal advisor to the Inspector General on matters relating to OIG resource management, including planning, information and information technology management, personnel administration and security, budget formulation and execution, and support services; will advise and represent the Inspector General on resource management and administrative matters; will advise Department officials regarding these matters; and will represent the OIG with officials of other Federal agencies or other public or private groups regarding resource management and administrative matters.

b. The functions and duties of the OADM will be carried out by Information Technology, Administrative Operations, Human Resources, and other such offices or specialized units as may be established to facilitate the performance of OADM’s assigned responsibilities.

.02 Functions. The OADM will be responsible for the provision and management of administrative resources and services for the OIG, as provided below; and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG’s mission.

a. The OADM will formulate, justify, and defend the OIG’s annual budget requests; will develop its annual budget operating plan and oversee the plan’s implementation; and will provide for sound financial management of the OIG by effectively monitoring and controlling costs and ensuring that budget outlays and obligations do not exceed appropriated funds and reimbursements.

b. The OADM will administer the OIG’s responsibilities relating to employee health and safety and security (personnel, facilities, information, systems, and other resources).

c. The OADM will administer the OIG’s procurement program, including ensuring that the OIG has appropriate policies, systems, and procedures in place to acquire the goods and services it needs in a timely, efficient, and cost-effective manner.

d. The OADM will manage travel and transportation services for OIG employees, including overseeing use of the contractor-issued government travel card.

e. The OADM will administer the OIG's human resources function in accordance with the authorities established in the Act. This function includes recruitment, staffing, personnel security; position classification, employee relations, performance management and recognition, development and training; equal employment opportunity (EEO) and affirmative action; and personnel/payroll processing.

f. The OADM will plan for, acquire, secure, control, and manage OIG office space, facilities, and personal property, and manage conference meeting planning activities for the OIG.

g. The OADM will be responsible for the provision and management of information technology resources and services for the OIG and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG’s mission.

SECTION 6. OFFICE OF COUNSEL TO THE INSPECTOR GENERAL.

.01 Organization. The Office of Counsel to the Inspector General (OC) will be headed by a Counsel to the Inspector General (Counsel), who will report and be responsible to the Inspector General.

a. The Counsel will be the legal advisor to the Inspector General and the OIG staff; will represent the Inspector General on legal matters; and will represent the OIG with officials of the Department of Justice and other Federal agencies or other public and private groups regarding legal matters.

b. The Counsel may be assisted by Senior Assistant Counsels or Deputy Counsel(s), who will be the chief operating aide to the Counsel; will perform other duties and functions as the Counsel may assign; and will perform the duties and functions of the Counsel in his or her absence.

.02 Functions. OC will provide legal services to the Inspector General and OIG staff in connection with the activities and operations of the OIG and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG's mission.

a. The Inspector General shall obtain legal advice from OC or a counsel reporting directly to another Inspector General except that the General Counsel will provide the Inspector General advice in the areas of conflict of interest statutes, ethics regulations, and related laws.

b. The Inspector General or Counsel to the Inspector General shall consult with the General Counsel on legal matters when they involve significant issues which may have an impact on the operations of the Department or legal matters of applicability to other Departmental bureaus, or concern statutes of government-wide applicability.

.03 In the performance of the responsibilities of his or her office, the General Counsel will respect the independence and integrity of the OIG; in the performance of the responsibilities of his or her office, the Inspector General will give due regard to the authority of the General Counsel as chief legal officer for the Department.

SECTION 7. EFFECT ON OTHER ORDERS

This Order supersedes DOO 23-1, dated August 31, 2006.

Signed by: Inspector General

Approved Deputy Secretary of Commerce

Questions and Comments

Send Questions or Comments on the Commerce Directives Management program to Directives@doc.gov.

Office of Privacy and Open Government
Office of the Chief Financial Officer and Assistant Secretary for Administration
U.S. Department of Commerce

Page last updated:May 24, 2013

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, April 4, 2018 10:15 AM
To:	William Rogers NOAA Federal; Robert Hembrook NOAA Federal; Chi Kang NOAA Federal
Subject:	Fwd: User Rules of Conduct Discussion
Attachments:	NOAA IT Security Manual.pdf; Office of Investigations Scope.pdf; Examples in Congressional Testimony from EPA OIG.pdf

FYI below.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

Forwarded message
From: **Mark Graff - NOAA Federal** <mark.graff@noaa.gov>
Date: Wed, Apr 4, 2018 at 9:29 AM
Subject: User Rules of Conduct Discussion
To: "Bogomolny, Michael (Federal)" <MBogomolny@doc.gov>
Cc: Robert Hogan <robert.j.hogan@noaa.gov>

Hi Bogo,

I'm meeting today with our Cyber folks who've asked for a meeting to discuss, among other things, the

(b)(5)

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

OIG Investigations of Employee Misconduct at the U.S. Environmental Protection Agency

Statement of Patrick Sullivan
Assistant Inspector General for Investigations

Before the Committee on Oversight and Government Reform
U.S. House of Representatives

May 18, 2016

Statement of
Patrick Sullivan
Assistant Inspector General for Investigations
Office of Inspector General
U.S. Environmental Protection Agency
Before the
Committee on Oversight and Government Reform
U.S. House of Representatives
May 18, 2016

Good morning, Chairman Chaffetz, Ranking Member Cummings and members of the committee. I am Patrick Sullivan, Assistant Inspector General for Investigations for both the U.S. Environmental Protection Agency (EPA) and the U.S. Chemical Safety and Hazard Investigation Board (CSB). I am pleased to appear before you today to discuss specific Office of Inspector General (OIG) investigations of employee misconduct issues at the EPA.

Employee Misconduct at the EPA

The EPA OIG is charged with conducting investigations and audits related to programs and operations at the EPA and CSB. The OIG remains committed to its statutory role of detecting waste, fraud and abuse, as well as promoting the effectiveness and efficiency of government operations. We operate with a separate budget and decision-making authority, and neither EPA nor CSB senior leaders may prohibit, prevent or obstruct us from conducting our work. Our independence from the agencies over which we have oversight ensures enhanced transparency and accountability in the OIG's investigations of alleged employee misconduct.

This committee specifically has asked about a number of OIG investigative cases that we previously reported on in summary fashion, and has sent the OIG a formal written request to obtain the Reports of Investigation regarding many of those, which we have provided to the committee. My testimony will provide an overview of several cases of EPA employees who viewed and downloaded pornography on government-issued computers, as well as other types of misconduct, some of which resulted in criminal prosecution. It is important to note that most of the alleged misconduct occurred at least 2 years ago.

I am happy to report that since I last testified before this committee to discuss misconduct by EPA employees, in April 2015, the agency's internal adjudication process has dramatically improved. At the suggestion of both Chairman Chaffetz and Ranking Member Cummings, the OIG, the EPA's Office of General Counsel, and the EPA's Office of Administration and Resources Management (which includes a Labor and Employee Relations section) now meet biweekly about pending misconduct cases and their adjudication by the agency. Misconduct cases are now being addressed faster and more consistently by EPA management. This increased efficiency is a result of the coordination and communication between the OIG and the agency to create a streamlined process to address employee misconduct issues. I believe that this process can serve as a "best practices" model for the federal government.

In addition, I note that while many allegations lodged against EPA employees are investigated by the OIG, some are ultimately determined to be unfounded or unsupported. In other words, OIG investigations often clear an individual. Our job is to collect and present the facts in a fair and unbiased manner. We are just as proud of our work in the cases that clear an employee as we are when our work leads to a criminal conviction or the removal of an employee who engaged in serious misconduct.

Now, I would like to summarize two of our more significant misconduct investigations that will be cited in our next Employee Integrity Cases report that will be posted to our website over the next weeks. Then I will highlight seven significant cases from our last three Employee Integrity Cases reports.

OIG Investigation of a Contractor in the EPA's Western Ecology Division

In May 2014, the OIG Seattle Field Office received a complaint from the EPA's Office of Environmental Information that a government computer assigned to an EPA contractor who was working in the EPA Western Ecology Division, Office of Research and Development, in Corvallis, Oregon had logged over 700 denials to blocked pornography, gaming and gambling sites on two occasions.

OIG special agents interviewed the EPA contractor, who stated that he was an information technology specialist who had provided support for the past 20 years. Stating he was "addicted" to pornography, he admitted to viewing pornography on his government-issued computer for the last 18 years. In the past year, he had watched pornography at least one to two hours per day. According to the contractor, he avoided detection for many years because he used commercial software to scrub/wipe his government computer. The contractor accessed pornographic sites using search engines hosted in foreign nations, including one located in Russia. He said that traditional search engines, such as Google and Yahoo, lead to pornographic sites blocked by the EPA.

Shortly after the OIG's interview, the EPA contractor was fired by his company. In addition, the OIG was successful in recovering $22,088 in repayments to the EPA by the company for the amount of time the contractor had viewed pornography during the prior year. Furthermore, the OIG made the EPA's Office of Environmental Information aware of EPA network vulnerabilities that had enabled the contractor to avoid detection for 18 years.

OIG Investigation of a GS-13 Special Agent in the EPA's Criminal Investigations Division

In February 2013, the OIG Office of Professional Responsibility was notified by the U.S. Attorney's Office (USAO) District of Connecticut, that a GS-13 special agent assigned to the EPA's Criminal Investigations Division (CID) in New Haven, Connecticut may have been engaged in criminal activity in connection with a Ponzi scheme. The special agent's name had surfaced during the prosecution of the ringleaders of a four-level pyramid scheme involving "gifting tables." New participants in this scheme would pay a $5,000 "gift" to the person occupying the top level.

Shortly after the OIG opened its investigation, the USAO District of Connecticut recused itself from the case because the EPA CID special agent was well known to the local Assistant U.S. Attorneys. The special agent had participated in numerous environmental crimes prosecutions by that office. The U.S. Department of Justice then assigned the case to the USAO District of Massachusetts.

The OIG investigation determined that the EPA CID special agent had made a false statement on a required Office of Government Ethics financial disclosure form in January 2012, wherein she concealed the fact that she had received $2,500 cash from her participation in the pyramid scheme.

In January 2015, the special agent retired from the EPA. In March 2015, she pleaded guilty to one felony count of 18 U.S.C. 1001, False Statements. In July 2015, she was sentenced to 1 year of probation and ordered to pay $7,500 in restitution, as well as a fine of $500.

OIG Investigation of a GS-14 Employee in Dallas (Case 5: April 1, 2015, to September 30, 2015)

In January 2012, the OIG Dallas Field Office received information alleging that a GS-14 program manager in EPA Region 6, Dallas, Texas, who was responsible for managing grants for the Border Environment Cooperation Commission, was using grant money for purposes not related to the grant.

The OIG investigation determined that the EPA program manager misused her position to divert agency grant funds, resulting in several improper payments by Border Environment Cooperation Commission officials totaling $5,195.

The USAO Northern District of Texas declined to prosecute the EPA program manager for potential violation of various federal statutes, including 18 U.S.C. 641 (theft of government funds) and 18 U.S.C. 666 (theft or bribery concerning programs receiving federal funds). The USAO declined to prosecute primarily because the program manager did not personally benefit from the diversion of the grant funds.

In July 2014, although termination was proposed in lieu of this, the EPA Region 6 Director of Multimedia Planning and Permitting Division agreed to let the program manager enter into an Abeyance/Last Chance Agreement. The terms of the agreement included the following:

- The effective date of the program manager's removal from employment would be held in abeyance in return for her compliance with the terms of this agreement.
- Within 2 years of signing this agreement, she would pay back $5,195 to the federal government based on a process determined by the agency.
- She would be demoted to a position chosen by the agency at the pay rate of GS-12, Step 10.

OIG Investigation of a GS-13 Employee in EPA's Office of Pollution Prevention and Toxics (Case 17: April 1, 2015, to September 30, 2015)

In March 2012, the OIG Washington Field Office received a complaint from the EPA's Office of Environmental Information alleging that a GS-13 biologist who worked in the EPA's Office of Pollution Prevention and Toxics downloaded pornographic images to an EPA shared file. During the course of the investigation, the employee admitted that he viewed and downloaded videos, movies and photographs, including those of pornographic nature, onto his EPA-issued computer.

The OIG reviewed the pornographic material on the employee's EPA-issued computer through a forensic examination, and found approximately 500 pornographic images. Additionally, the OIG determined that more than 2,560 videos and 435 music files were accessed and/or downloaded by the employee. The review also discovered sexually explicit videos on the employee's EPA-issued computer.

In 2014, the employee was barred from EPA facilities and placed on paid administrative leave pending a decision on the matter. In March 2015, a notice of proposal for removal for the misuse of government equipment for other than official purpose was provided to the employee. In May 2015, the employee's retirement after receiving a written notice for the proposal of removal went into effect.

OIG Investigation of a GS-12 Employee in Atlanta (Case 8: October 1, 2014, to March 31, 2015)

In October 2013, an OIG special agent in the Atlanta Field Office proactively checked a list of EPA property reportedly lost or stolen from EPA Region 4 in Atlanta through a law enforcement database. This search resulted in a "hit" on an EPA digital camera pawned at a store in Decatur, Georgia, in July 2012. The person who pawned the camera had the same name as an EPA Region 4 employee a GS-12 public affairs specialist in the Office of External Affairs. The camera was assigned to the Office of External Affairs.

The subsequent OIG investigation revealed that, on seven occasions between July and September 2012, the EPA employee pawned EPA digital cameras and camcorders at the same pawn shop. She failed to reclaim EPA property on five occasions, and the property was then sold by the pawn shop, resulting in a loss to the government of $3,117. The USAO Northern District of Georgia declined prosecution for violation of 18 U.S.C. 641 (theft of government property). However, the District Attorney's Office in Fulton County, Georgia, accepted the case for local prosecution.

In January 2014, the EPA Region 4 Director of the Office of External Affairs issued a memorandum that proposed the suspension of the employee for 120 days. Following an appeal by the employee, the Deputy Regional Administrator issued, in May 2014, a memorandum detailing the final decision to suspend the employee for 30 days.

In October 2014, the EPA employee pleaded guilty to theft, in violation of Georgia Code, Title 16, Section 16-8-2, in Superior Court of Fulton County. She was sentenced to 3 years of probation, and ordered to pay restitution in the amount of $3,117, as well as a fine of $1,000.

The OIG investigation further revealed that the EPA Region 4 property custodian falsely certified her physical property inventories in fiscal years 2012 and 2013. The property custodian signed and certified that she conducted an inventory of all of the property items assigned to her inventory for that period. It was determined that two of the items allegedly inventoried by the property custodian were previously pawned by the GS-12 public affairs specialist and not returned. Therefore, these items were not physically present within Region 4, and could not have been inventoried. In June 2014, the Director of the Office of External Affairs issued the property custodian a letter of warning in reference to her false certifications of inventories.

OIG Investigation of a GS-12 Employee in the Office of Administration and Resources Management in Research Triangle Park (Case 9: October 1, 2014 to March 31, 2015)

In August 2013, the OIG Research Triangle Park (RTP), North Carolina, Field Office was notified that a GS-12 employee, who was working as a Contracting Officer's Representative at the Facilities Support Branch, Office of Administration and Resources Management, in RTP, was suspected of having a financial interest in a company doing business with the EPA.

The OIG's investigation determined that the EPA employee did have a financial interest in a company doing business with the EPA, which is a potential violation of 18 U.S.C. 208 (acts effecting a personal financial interest). The USAO Middle District of North Carolina declined prosecution and referred the matter back to the EPA for administrative action.

In July 2014, the OIG submitted a Report of Investigation to the Office of Administration and Resources Management senior management official at RTP, in which allegations of misconduct were supported. The OIG's investigation determined that the EPA employee had not reported that she had a financial interest in a company doing business with the EPA. Further, she used EPA computers for conducting personal business. She also provided false information when interviewed by OIG special agents.

In August 2014, EPA rescinded the EPA employee's authority to act as a Contracting Officer's Representative. In September 2014, the employee resigned. At the time of her resignation, the EPA was considering a proposal to remove her from federal service. However, she had not yet been served with termination papers.

OIG Investigation of a GS-13 Employee in Dallas (Case 17: October 1, 2014, to March 31, 2015)

In March 2006, the OIG Dallas Field Office was informed that a GS-13 EPA Enforcement Officer was cited by the Dallas Police Department for the improper use of emergency lights on his personal vehicle while also being a registered sex offender. He previously had been convicted, in April 1997, on a deferred adjudication for indecent acts with a minor. (Note: An EPA Enforcement Officer is NOT a federal law enforcement officer (LEO), but rather an administrative enforcement officer. Unlike a federal LEO who carries a gun and badge and is authorized to execute arrest and search warrants, an EPA enforcement officer is not armed and cannot make arrests). The EPA employee also possessed a make-shift badge which accompanied his administrative EPA

Enforcement Officer credentials, which were displayed by the employee to the police officer. This led the police officer to believe that the employee was an EPA law enforcement officer. The EPA employee also used emergency lights affixed to his personal vehicle at an accident scene. The police officer checked the employee's vehicle license plate and determined that he was a registered sex offender.

The subsequent OIG investigation disclosed that the EPA employee had designed and purchased 20 similar badges. He also possessed a bullet-proof vest and installed emergency lights on his personal vehicle, which was a violation of his probation for a sex offender charge. (Note: In March 1999, the same employee had been counseled by EPA Region 6 officials for using emergency lights on his personal vehicle. He was then told to remove all law enforcement equipment from his personal vehicle.)

In April 2006, the USAO Northern District of Texas declined to prosecute the EPA employee for violation of 18 U.S.C. 912 (false personation) and 18 U.S.C. 701 (counterfeit badges). EPA Region 6 then imposed discipline in the form of a 60-day suspension, and the EPA employee was removed from his position as an EPA Enforcement Officer. He was reassigned to an administrative position within the office.

In August 2013, the Dallas Police Department Sex Offender Unit requested assistance from the OIG in arresting the same EPA employee for violation of probation. He was arrested on the probation violation charge. As a result of this arrest, the OIG developed information that the employee may have viewed and possessed child pornography on his EPA-issued computer. A subsequent OIG forensic examination of his computer revealed no evidence of child pornography or any pornography on his EPA computer.

Following the employee's arrest for probation violation, EPA Region 6 indefinitely suspended him. In January 2014, the employee was terminated from his employment with the EPA.

Subsequently, the Merit Systems Protection Board overturned the employee's termination and ordered that he be re-hired by the EPA. In September 2014, the employee returned to work at the EPA. In January 2015, the employee entered into a Settlement Agreement, which was overseen by Merit Systems Protection Board, in which he agreed to resign from the EPA in exchange for certain considerations.

OIG Investigation of SES-Level Director in EPA's Office of Administration and Resources Management (Case 3: April 1, 2014 to September 30, 2014)

In January 2014, while conducting an investigation into an unrelated misconduct case, an OIG special agent in the Washington Field Office discovered that an Senior Executive Service (SES)-level EPA employee, who was the Director of the Office of Administration and Resources Management's Facilities Management and Services Division, incurred $22,315 in international roaming charges on her EPA-issued mobile device between December 2010 and October 2012. The EPA Director had no authorized international travel on behalf of EPA. The OIG investigation ultimately supported the following charges in which the EPA Director:

1. Improperly used her EPA issued mobile device while overseas on personal travel and incurred over $22,000 in charges.
2. Made false statements on the SF-86, Questionnaire for National Security Positions when she failed to disclose five trips to Israel and one trip to Germany.
3. Made false statements on the same SF-86 when she failed to disclose that she wired $90,000 to a foreign national in Jericho, Palestine.
4. Claimed approximately 24 hours of regular work time while on personal travel to Israel, when she should have claimed annual leave.

The USAO District of Columbia declined to prosecute for violations of 18 U.S.C. 1001 (false statements) and 18 U.S.C. 641 (theft of government funds).

In May 2014, the OIG provided the EPA with a report of investigation; however, shortly thereafter, and prior to the agency taking administrative action, the EPA Director resigned her position. Subsequently, the agency conducted an initial review and was unable to determine what portion of the employee's charges were due to personal activity versus work activity. In April 2016, the EPA informed the OIG that the matter was being reviewed. The agency is now considering issuing a debt notice to the EPA Director for the charges incurred.

OIG Investigation of a GS-14 Employee in Kansas City (Case 10: April 1, 2014 to September 30, 2014)

In August 2010, the EPA Regional Administrator, Region 7, Kansas City, Kansas, made a formal referral to the OIG based upon a complaint filed in the U.S. District Court, District of Nebraska by the Union Pacific Railroad Company. The referral alleged that the EPA violated the Freedom of Information Act and other statutes in connection with the Omaha Lead Superfund Site. It was alleged that the agency destroyed emails and other records.

In 2012, the OIG opened a criminal investigation, in concert with the FBI, after developing preliminary information indicating that a GS-14 EPA environmental engineer assigned to Region 7 destroyed emails concerning the Omaha Lead Superfund Site and encouraged other agency employees to do the same. Because of a potential conflict of interest, the USAO District of Nebraska recused itself from the criminal investigation. The U.S. Department of Justice assigned the case to the USAO District of Kansas. Ultimately, the USAO declined to prosecute the EPA employee for violation of 18 U.S.C. 1519 (destruction or alteration of records in federal investigations and bankruptcy) or other statutes due to a lack of provable criminal intent.

In November 2013, the OIG submitted to the Region 7 Regional Administrator a Report of Investigation in which administrative misconduct by the employee was supported. The OIG investigation revealed through the use of computer forensics, and the results of interviews, affidavits and depositions that the employee deleted emails and directed and/or instructed other EPA employees to delete emails pertaining to the Omaha Lead Superfund Site.

In May 2014, the OIG was informed that a notice of proposed removal was served on the employee, but the employee retired from federal service before the termination became effective.

Additional EPA Employee Integrity Cases

The OIG posts to its publicly-accessible Investigations web page reports summarizing the closed EPA employee integrity cases. The following, available in those posted reports, describe a number of additional OIG investigations that were closed within the previous three reporting periods (April 1, 2014, to September 30, 2014; October 1, 2014, to March 31, 2015; and April 1, 2015, to September 30, 2015). The OIG intends to publish its next report on employee integrity cases (October 1, 2015, to March 31, 2016) in late May or early June 2016.

List of Selected Closed Employee Integrity Cases: April 1, 2015, to September 30, 2015

CASE 1: An SES-level supervisor allegedly engaged in inappropriate behavior, hiring, promotions and management of programs. Also, the supervisor allegedly compromised his ability to be objective in his conduct at work and in his management of senior staff. The supervisor admitted involvement in an inappropriate romantic relationship with a subordinate, GS-15-level, employee. Additionally, evidence showed that the supervisor attempted to influence other EPA employees in an effort to promote the subordinate employee. The supervisor retired from the EPA before a report of investigation could be presented to the agency.

CASE 6: Potential conflicts of interest were alleged to have resulted from the appointment of an EPA attorney as Chairman of an environmental quality board. The allegation noted that the employee claimed to speak for or represent the EPA in meetings with the local regulated community, and may have misused the dual positions for private gain. In addition, according to the allegation, the EPA employee may have sponsored and organized a fundraising event, and required board employees to make donations and attend the event for the re-election campaign of a governor. The investigation was unable to substantiate that the employee had used the EPA position for private gain or that the employee had made board employees contribute to a fundraising event. The employee resigned from the EPA during the investigation. This case was presented to the U.S. Office of Special Counsel and the USAO; both declined advancing the matter.

CASE 9: An EPA employee allegedly was cited for attempting to bring approximately three grams of marijuana and two marijuana pipes through the security checkpoint at an Internal Revenue Service facility in Denver, Colorado, and arrested on an active warrant for failure to appear. The investigation confirmed that the employee had appeared in the U.S. District Court for the District of Colorado and was found guilty of one count of possession of marijuana on federal property. The employee was sentenced to a 3-day suspended sentence, 12 months' unsupervised probation and 20 hours of community service, and was ordered to pay a $2,500 fine. The employee was suspended from the EPA for 21 days.

CASE 10: An EPA employee allegedly failed to disclose criminal and financial indebtedness when completing form OF-306, *Declaration for Federal Employment*, and form SF-85P, *Questionnaire for Public Trust Positions*. The investigation revealed that, during an employment suitability background investigation of the EPA employee conducted by the Office of Personnel

Management, criminal and financial indebtedness information surfaced that previously had not been divulged on forms OF-306 and SF-85P. The EPA's Personnel Security Branch requested from the employee documentation of the paying down of accumulated debts. The documentation tendered did not appear authentic and was determined to be fraudulent. The employee provided false information to the EPA concerning criminal history and failed to pay accrued personal debts, which included an EPA travel card balance of $10,226. The EPA presented the employee with a letter of proposed removal; however, the employee retired from the EPA prior to removal.

CASE 11: An EPA employee allegedly misused an EPA-issued travel credit card for personal expenses. During an interview, the employee admitted using the EPA-issued travel credit card for personal charges totaling $625. The employee stated a belief that there was no loss to the government as the expenses were subsequently paid for with cash. The employee had not been candid with supervisors and the OIG when initially questioned about the personal charges. The employee was issued a 14-day suspension.

CASE 16: An EPA employee may have violated conflict of interest laws by representing two nonprofit organizations back to the federal government. The investigation did not substantiate the allegation but uncovered evidence of other violations. The employee had misused EPA resources, such as EPA email and an EPA-issued computer, to conduct business on behalf of the two nonprofit organizations. The employee had neglected to disclose involvement with the nonprofit organizations on the *Confidential Financial Disclosure Report* (OGE Form 450). The employee also had allowed biographical information to be posted on one nonprofit organization's website, and the biography gave more prominence to the employee's EPA position than to other details. After this discovery, the biography was removed from the organization's website. Additionally, the employee was acting in a "leader" capacity at the same nonprofit and previously had been a board member there (while concurrently working for the EPA). A report of investigation was presented to the EPA, which later notified the OIG that the employee was suspended for two days.

List of Selected Closed Employee Integrity Cases: October 1, 2014, to March 31, 2015

CASE 5: An EPA employee was alleged to have potential conflicts of interest and ethical violations. The investigation found that the employee had violated the Code of Federal Regulations and the EPA ethics code by submitting a letter of support to the EPA on EPA letterhead, resulting in a potential unfair competitive advantage to a prospective grant recipient and disqualification of the grantee's proposal from further consideration. The employee was issued a warning letter for assisting the prospective grant recipient with a proposal.

CASE 13: An EPA employee allegedly misused the employee's position by allowing two nonprofit organizations to use an EPA leased trailer and surrounding property to conduct non EPA related activities without authorization. The investigation supported and the employee admitted to allowing two nonprofit organizations unauthorized use of the trailer, free of charge, for non project related activities. The employee was suspended for five days.

CASE 18: An EPA employee was arrested on felony charges of marijuana possession after local police discovered a marijuana growing operation in her residence. The employee was placed on

paid administrative leave in March 2014, and the employee signed a separation agreement in May 2014. She remained on paid administrative leave until her retirement on October 30, 2014. In as much as there was no violation of federal law, this case was not presented to the USAO.

List of Selected Closed Employee Integrity Cases: April 1, 2014, to September 30, 2014

CASE 8: An EPA employee allegedly misused an EPA-issued mobile device by placing personal international calls. The investigation disclosed that the employee had incurred more than $4,500 in international roaming charges when the mobile device was used in a foreign country while the employee was on leave. The employee and all division staff were counseled by management on the appropriate use of EPA-issued mobile devices. The USAO-District of Columbia declined prosecution for violation of 18 USC 641 (theft of government funds).

CASE 11: A GS-15-level employee viewed pornographic material on an EPA-issued computer while in duty status. The employee admitted to the allegation, and a forensic analysis of the hard drive substantiated that the employee had watched pornography regularly at work for the past several years. The employee was suspended for 5 working days, is no longer allowed to telework, and is not allowed to attach any unauthorized external drive devices to a government computer.

CASE 13: There was an alleged conflict of interest between an EPA employee and a contractor when the employee became involved with an initial contract task order. The investigation substantiated the allegation, but the case was declined for criminal prosecution by the U.S. Attorney's office. The EPA's administrative proposal recommended removal of the employee, but the employee retired before the proposal was finalized.

CASE 15: An EPA employee allegedly misused his EPA-issued travel card for services unrelated to government travel and attempted to mislead EPA officials regarding how the travel card had been used. Management initiated removal of the employee; however, the employee resigned prior to being formally served with a notice of proposed removal. The USAO-Northern District of California, declined prosecution for violation of 18 USC 1001 (false statements). There was no dollar loss to the government.

CASE 16: An EPA employee and a contractor allegedly exchanged emails containing procurement-sensitive information relative to the EPA's Central Data Exchange support contract valued at $220 million. The emails allegedly constituted a violation of the Procurement Integrity Act, which prohibits the disclosure of contractor bid or proposal information and source selection information. The investigation confirmed that the employee had engaged in conversation, via email, with the contractor, revealing sensitive procurement information. The email exchange took place during the open procurement period for the contract. The allegation regarding violation of the act was proven. The EPA issued a warning to and counseled the employee concerning improper communications. The employee was relieved of the role of Contracting Officer's Technical Representative and instructed to take interpersonal skills training.

CASE 17: An EPA employee allegedly used an office purchase card to pay off a personal debt to a university in the amount of $1,678. This case was prosecuted by the USAO-District of

Columbia. The employee pleaded guilty to one count of first degree fraud misdemeanor and entered into a deferred sentencing agreement. The conditions of the agreement were for the employee to perform 48 hours of community service and not be rearrested in the next 6 months with any incident where probable cause could be established. No restitution was ordered by the court. The employee resigned following her conviction.

CASE 18: An EPA employee allegedly incurred improper international roaming charges on an EPA-issued mobile device. The employee agreed to pay back $1,725. The employee also was orally reprimanded and counseled on the appropriate use of government-issued equipment and the EPA's international travel policies. The employee's manager indicated that all staff would be made aware of the EPA's policy on government equipment and international travel.

Conclusion

The OIG takes very seriously its overall responsibility for investigations into allegations of employee misconduct at the EPA. To that end, we will continue to work closely with the agency, U.S. Department of Justice, our law enforcement partners and Congress to ensure that allegations of employee misconduct are quickly and properly addressed. We appreciate your continued interest in the work of the OIG.

Mr. Chairman, this concludes my prepared statement. I will be happy to answer any questions that you, the Ranking Member and the committee members may have.

Biography of Assistant Inspector General for Investigations
Patrick Sullivan

Patrick Sullivan is the Assistant Inspector General for Investigations, Office of the Inspector General of the U.S. Environmental Protection Agency (EPA). He supervises the OIG's criminal investigative activities, including allegations of grant fraud, contract fraud, employee misconduct, threats directed against EPA officials and facilities, and other violations of federal law within the OIG's jurisdiction. He has more than 30 years of service in federal law enforcement with significant supervisory, administrative, intelligence, counter-terrorism and criminal investigative experience.

Prior to his appointment at the EPA-OIG, Mr. Sullivan served as a Deputy Assistant Director with the Transportation Security Administration's (TSA's) Federal Air Marshal Service. He supervised TSA's participation in the Joint Terrorism Task Force program, the Federal Air Marshals' intelligence program and the imbedding of Federal Air Marshals with the Federal Bureau of Investigation, the Central Intelligence Agency, Immigration and Customs Enforcement, and Customs and Border Protection. He also was responsible for supervising TSA's domestic and foreign law enforcement liaison activity.

Previously, Mr. Sullivan was an Assistant Director with the Government Accountability Office, Office of Special Investigations, where he worked on cases involving allegations of misconduct by high-level government officials as well as special investigations requested by congressional committees.

He spent more than 20 years in the U.S. Secret Service, where his last assignment was the worldwide supervision of counterfeiting investigations. He also was assigned to the U.S. Department of Justice, Organized Crime Strike Force, in Brooklyn, NY, where he worked cases targeting the traditional mafia crime families in New York City. Furthermore, he spent four years assigned to the Presidential Protection Division under Presidents Ronald Reagan and George H.W. Bush.

Early in his career, Mr. Sullivan worked for the FBI as an Investigative Assistant assigned to the surveillance of foreign intelligence officers engaged in suspected espionage and other intelligence activities directed against the United States.

He is a graduate of the John Jay College of Criminal Justice with a B.S. degree in Police Science and Criminal Justice. He is also a graduate of the Naval Postgraduate School, Center for Homeland Defense and Security, Executive Leadership Program and a member of the federal Senior Executive Service.

Department of Commerce • National Oceanic & Atmospheric Administration

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

IT SECURITY MANUAL 212-1301

Effective Date: September 01, 2016

Management, Operational, and Technical Controls

NOTICE: This publication is available at: NOAA IT Security Web Site

Date of Issuance: May 25, 2016

Version 5.6

This page is intentionally blank.

Changes/Revisions:

Modifications made to this document are recorded in the Change/Revision Record below. This record shall be maintained throughout the life of the document.

Change / Revision Record				
Date	**Version**	**Section**	**Description of Change**	**Author**
2007-05-15	3.3	All	Initial Version	L. Reed
2008-02-04	4.0		Added Revision History	L. Reed
2008-02-04	4.0		Aligned control selections with NIST SP 800-53 rev2 CP-4 changed from Not Selected to CP-4 for Low Baseline	L. Reed
2008-02-04	4.0		Corrected alignment with SP 800-53 rev2 AU-8 changed from Not Selected to AU-8 for Low Baseline MP-3 changed from MP-3 to Not Selected for Moderate Baseline AC-18 changed from Not Selected to AC-18 for Low Baseline SI-3 added enhancement 2 for Moderate Baseline SI-4 added enhancement 4 for Moderate Baseline	L. Reed
2008-02-04	4.0	All	Added Section numbers	L. Reed
2008-02-04	4.0	RA-5	Added requirements for remediation and reporting	L. Reed
2008-02-04	4.0	IR-1	Clarified N-CIRT role during incident (suspected incident) response	L. Reed
2008-02-25	4.0	RA-1,RA-5, IR-1, AT-2, AT-3, PL-1	Changed to address ITSC comments	L. Reed
2008-02-28	4.1	RA-5	Grammar correction	L. Reed

Change / Revision Record				
Date	**Version**	**Section**	**Description of Change**	**Author**
2008-02-28	4.1	CA-1.B	Changed Certification Official to Certification Agent. Clarified "recommendation" to CA recommendation.	L. Reed
2008-02-28	4.1	CA-6	Removed reference to National Critical systems	L. Reed
2008-02-28	4.1	MP-1.k	Removed moderate systems to align with SP 800-53	L. Reed
2008-02-28	4.1	SC-11	Grammar correction	L. Reed
2008-03-10	4.1	IR-1	Added escalation requirement	L. Reed
2008-03-11	4.2	IR-1	Clarifications	L. Reed
2013-06-30	5.0	All	Addressed requirements for NIST SP 800-53, Rev.4	Team Ambit
2015-01-23	5.1	All	Draft updates per ITSC reviews	Team Ambit
2015-03-24	5.2	Sections 2, 3 and Appendices	Updates per CSD and LO ITSO reviews	D. Stevens
2015-05-12	5.3	All	Updates per CSD and LO ITSO reviews	D. Stevens
2015-06-17	5.4	All	Updates per CSD and LO ITSO reviews	D. Stevens
2016-4-29	5.5	All	Updated cover page/removed Water marks, corrected contents table.	H. Burgos
2016-5-11	5.6	Cover Page/Sect. 1.3	Effective Date updated	H. Burgos

This page is intentionally blank.

Contents

SECTION 1: INTRODUCTION

This page is intentionally blank.

1 INTRODUCTION

The U.S. Department of Commerce National Oceanic and Atmospheric Administration (NOAA) have adopted a set of security controls to protect sensitive information and information systems. The Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, specifies the minimum security requirements for federal information and information systems. NOAA is responsible for ensuring that all information systems meet the minimum security requirements defined in FIPS 200 through the use of the security controls provided in the NOAA System Security Plan (SSP) which includes updates from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. NOAA developed the security policies and procedures to ensure security controls are properly implemented and maintained.

The development of sound policies provides both direction and management support. The NOAA Information Technology Security Manual (ITSM) sets the NOAA-wide direction for protecting NOAA information and information systems. This ITSM defines the key roles and responsibilities for carrying out information security program activities at NOAA. The ITSM also establishes the "NOAA-defined" parameters for identified NIST SP 800-53 Revision 4 security controls and additional security policies.

These policies and procedures are established to ensure all NOAA users adhere to the following three security objectives:

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Confidentiality ensures that NOAA information is protected from all unauthorized disclosure.

Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Information integrity ensures that NOAA information is protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:

- **Authenticity –** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- **Non-repudiation –** Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
- **Accountability** The property that enables the tracing of system activities to their sources who may then be held responsible for such activities. Auditing is a primary means of monitoring accountability.

Availability - Ensuring timely and reliable access to and use of information. Availability ensures that NOAA information resources (system or data) are accessible on a timely basis to meet mission requirements or to avoid substantial losses. Information availability also includes ensuring resources are used only for intended purposes.

1.1 PURPOSE

The purpose of this ITSM is to define the requirements necessary for all of NOAA systems to meet the fundamental security and privacy objectives of system and data confidentiality, integrity, and availability.

1.2 SCOPE AND APPLICABILITY

The policies and procedures in this document, and its attachments, apply to all NOAA information resources. NOAA information includes data that is owned, sent, received, or processed by NOAA or third parties on behalf of NOAA and includes information in either physical or digital form. NOAA information resources include NOAA hardware, software, media, and facilities.

Finally, this policy applies to other Agencies' systems as delineated in Memorandums of Understanding (MOU) and Interconnection Security Agreements (ISA) with NOAA.

Everyone who uses, manages, operates, maintains, or develops NOAA applications or data wherever the applications or data reside must comply with the ITSM, unless a specific waiver is obtained from the NOAA Chief Information Officer (CIO) or the NOAA Senior Agency Information Security Officer (SAISO), following the process specified in section 1.4 below.

1.3 COMPLIANCE AND ENFORCEMENT

Compliance: NOAA ITSM is mandatory for all NOAA employees and contractors. All users must adhere to all policies detailed in this manual by its effective date of **1 September 2016.**

Enforcement: Under authority outlined in the NOAA Administrative Order (NAO) 212-13, the NOAA CIO is responsible for continually reviewing the status of NOAA's

Information Security Programs by monitoring:

- The effectiveness of security and privacy control measures;
- Compliance with existing policies, procedures, standards, and guidelines; and
- User awareness of information security and privacy.

Violations of the policies contained in the ITSM including any related NOAA Information Technology Policies may result in the loss of, or limitation of, access to NOAA information systems and information. Anyone in NOAA who violates the policy may face administrative action ranging from counseling to removal from the NOAA, as well as, criminal penalties or financial liability, depending on the severity of the misuse.

NOAA employees and contractors are subject to penalties established by the Privacy Act of 1974. Certain penalties apply to the misuse or unauthorized disclosure of personally identifiable information. The Act (5 U.S.C. 552a (g)) provides for civil remedies for injured parties, including actual damages, attorney fees, and litigation costs.

A policy violation is an infringement or nonobservance of NOAA policy. If policy violation is suspected, NOAA employees shall report it to their NOAA supervisor, manager, and Staff and Line Office ITSO, as appropriate. Contractors shall report suspected violations to their contracting officer's technical representative and the System Owner. The following preemptive

actions must be taken to isolate the suspected violators and systems to prevent additional risk to NOAA:

- The suspected violator's group lead shall notify the NOAA Cyber Security Division for additional guidance;
- Management shall be responsible for any disciplinary actions;
- The NOAA CIO or respective ACIO shall be responsible for any technical actions; and
- The NOAA CIO or respective ACIO shall restrict access to NOAA information systems until the violator proves, to the satisfaction of the CIO or respective ACIO, that the issue is resolved and there is no future risk.

1.4 ADOPTION OF THE INFORMATION SECURITY AND PRIVACY POLICY REQUIREMENTS

NOAA users are responsible for using the current official version of the ITSM posted on the NOAA intranet (https://sites.google.com/a/noaa.gov/cio/internal-use-only). NOAA leadership will hold users responsible for adhering to the policies and standards in the current official version.

1.5 WAIVER PROCESS

Waivers are to be adjudicated by the NOAA CIO, except for controls and/or policies which explicitly require a waiver be adjudicated at the DOC CIO level. Circumstances for waivers differ from controls baseline tailoring as described in Waiver requests shall document:

1. Explanation of unique circumstance justifying foregoing the implementation of the requirement/control (to be documented in a single waiver to cover multiple systems affected, and in the SSP for each system on which the control/policy will not be implemented must reference the single waiver.)

2. Description of compensating control(s) that provide(s) an equivalent or comparable protective value to that of the requirement/control objective not being implemented in the manner described by policy. This will be documented in a single waiver to cover multiple systems affected, and in the SSP for each system on which the control/policy is compensated must reference the single waiver.

3. Description of any residual risk introduced as a result of meeting the requirement/control objective through application of compensating controls to be documented in a single waiver to cover multiple systems affected. The Risk Assessment must reference the single waiver.

4. A written recommendation from the system's responsible Authorizing Officials (AOs) in regard to accepting the risk and approving the waiver.

5. Controls not currently being employed but which are planned to be employed must be documented in a POA&M and the POA&M referenced in the respective control section in the SSP or Risk Assessment.

6. Decision by the NOAA CIO (or DOC CIO in cases where policy requires DOC CIO approval of waivers).

Waivers shall be made available through CSAM to the DOC CISO/SAISO.

1.6 MAINTENANCE OF THE OFFICIAL VERSION

The CIO will be assisted by the IT Security Committee (ITSC) in the review of the policy at least annually from its initial distribution, and will review and update it as needed based on emerging information security policy and procedure requirements.

When document revisions are formally approved, the CIO will issue a new version or an amendment to the ITSM and post it to the NOAA Intranet (https://sites.google.com/a/noaa.gov/cio/internal-use-only).

1.7 LEGAL AUTHORITY

NOAA developed the ITSM to comply with applicable laws and directives related to information security and policies. This policy document acquires its legal authority from the NOAA Administrative Order (NAO) 212-13 and Federal Information Security Management Act (FISMA); the Privacy Act of 1974; the Computer Security Act of 1987; the Computer Fraud and Abuse Act of 1987; OMB A-130, Appendix III; the Clinger-Cohen Act of 1996; Executive Order 13011, Federal IT; and all relevant NIST standards, regulations in the Code of Federal Regulations (CFR); and the Office of Management and Budget (OMB) memorandums, circulars, and directives.

SECTION 2: ROLES AND RESPONSIBILITIES

This page is intentionally blank.

2 ROLES AND RESPONSIBILITIES

All NOAA users have information security policy and procedure responsibilities. The key roles and responsibilities for carrying out this policy are outlined below as defined in the NIST Special Publication 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems, Appendix D*.

2.1 UNDER SECRETARY OF COMMERCE FOR OCEANS AND ATMOSPHERE AND ADMINISTRATOR (Head of Agency/Chief Executive Officer)

The NOAA agency head is the Under Secretary of Commerce for Oceans and Atmosphere and Administrator. This individual has the responsibility to ensure that (i) information security management processes are integrated with strategic and operational planning processes; (ii) senior officials within the organization provide information security for the information and information systems that support the operations and assets under their control; and (iii) the organization has trained personnel sufficient to assist in complying with the information security requirements in related legislation, policies, directives, instructions, standards, and guidelines.

2.2 RISK EXECUTIVE FUNCTION

The NOAA Chief Information Officer (CIO) and Deputy CIO (DCIO) along with the NOAA Enterprise IT Risk Board, the NOAA Executive Council (NEC), the NOAA Executive Panel (NEP), the NOAA CIO Council and the NOAA Enterprise IT Risk Coordinator, are responsible for establishing the NOAA-wide approach for managing agency-wide data and system risk and help ensure that: (i) risk-related considerations for individual information systems, to include authorization decisions, are understood at an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and integrates IT security risk with the DOC Enterprise Risk Management process. The risk executive (function) coordinates with the senior leadership of an organization to:

- Provide a comprehensive, NOAA-wide, holistic approach for addressing risk an approach that provides a greater understanding of the integrated operations of the organization.
- Develop a risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole.
- Facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization.
- Provide oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent and effective risk acceptance decisions.
- Ensure that authorization decisions consider all factors necessary for mission and business success.
- Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation.

- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility.
- Ensure that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities; and
- Identify the organizational risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

2.3 NOAA CHIEF INFORMATION OFFICER

The NOAA Chief Information Officer (CIO) has oversight responsibility for the NOAA IT Security Program. The Security Program is implemented and maintained through interaction with NOAA's Line Office Assistant CIOs (ACIOS) and the LO Senior Agency Information Security Officers (SAISOs) or IT Security Officers (ITSOs). The NOAA CIO:

- Acts as the Authorizing Official (AO) for the authorization of all NOAA IT systems. This authority of the NOAA CIO may be delegated in writing to the Assistant CIOs of the involved Staff or Line Office or their Deputy. The NOAA CIO serves as Co-AO for all NOAA high systems. The Line Office Assistant CIOs will be the Co-AO for Low and Moderate systems.
- Ensures the appointment and/or designation of AOs and co-AOs as appropriate and in writing
- Ensures AOs and co-AOs, as applicable, authorize all systems and ensuring compliance with the Federal Information Security Management Act (FISMA), as well as DOC and NOAA policy requirements.
- Approves and enforces information security policies, procedures, and control techniques to address all applicable requirements.
- Oversees offices, groups, teams, or other organizations that are responsible for providing generic IT services identified in the NOAA-level IT Service Catalog, including personnel with significant responsibilities for information security; and ensures that the personnel are adequately trained.
- Assists other senior organizational officials concerning their security responsibilities
- In coordination with other senior officials, reports annually to the NOAA Administrator on the overall effectiveness of the organization's information security program, including progress of remedial actions.
- Provides advice and assistance to the NOAA Administrator and other senior Agency personnel to ensure NOAA IT security goals, priorities, and requirements are effectively and efficiently addressed to protect NOAA's investments in IT.
- Ensures sufficient funds are requested and allocated to sustain the NOAA wide IT security programs.

2.4 NOAA ASSISTANT CHIEF INFORMATION OFFICER

The Assistant Chief Information Officer (ACIO) will:

- Ensure that an IT Security Program is developed and implemented for their Staff or Line Office.
- Designate in writing a Senior Agency Information Security Officer (SAISO)/Cyber Security Program Manager (CSPM) to oversee and execute the Staff or Line Office Cyber Security Program and ensure that the SAISO/PM has the staff and resources necessary to carry out the program in accordance with FISMA.
- Act as the Co-Authorizing Official (AO) for the authorization of all low and moderate Line Office IT systems, and the AO for all low and moderate systems under their direct ownership authority. This authority may be delegated only to the Deputy ACIO. The Line Office ACIO will hold the Line Office AOs accountable for authorizing all systems to operate and ensuring compliance with the FISMA, the Line Office relevant policies, as well as DOC and NOAA policy requirements.
- Ensures the appointment and/or designation of AOs and co-AOs as appropriate and in writing
- Ensure that an adequate and appropriate IT security safeguards are in place for all Staff and Line Office systems.
- Ensure that the Staff and Line Office IT Security Program integrates fully into the Staff and Line Office's enterprise architecture and capital planning and investment control processes.

2.5 INFORMATION OWNER/STEWARD

See DOC Information Technology Security Program Policy, Section 3.3.3, IT Security Roles and Responsibilities.

2.6 PRIVACY ACT OFFICER/FREEDOM OF INFORMATION ACT (FOIA) OFFICER

The NOAA Bureau Chief Privacy Officer (BCPO) works with the DOC Office of Privacy and Open Government's (OPOG) and the Director of OPOG for the development and maintenance of privacy policies, procedures, and guidance essential to safeguarding the collection, access, use, dissemination, and storage of personally identifiable information (PII) and Privacy Act information in accordance with the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Management Act (FISMA), and policy and guidance issued by the President and Office of Management and Budget (OMB), and for the conduct of Privacy Impact Assessments on Information Technology that collects, maintains, or disseminates information in an identifiable form.

NOAA FOIA Officer in addition to responsibilities in NOAA FOIA Office below:

a. approves or denies fee waiver and expedited processing requests; and

b. act as Denial Official, as listed in Appendix B, 15 CFR Part 4 (http://www.corporateservices.noaa.gov/foia/title_15_commerce_and_foreign_trade/appendix-b.html)

NOAA FOIA Office will:

a. review and update FOIA policies, procedures, and guidance in coordination with the Department of Commerce (DOC) FOIA Office and NOAA Office of General Counsel (NOAA GC);

b. offer guidance, advice, and training to NOAA managers, program personnel, and FOIA Liaisons who respond to FOIA requests and provide basic training on NOAA FOIA procedures to all employees;

c. prepare and submit the NOAA contribution of the FOIA Annual Report to Department of Justice and Chief FOIA Officer report, and coordinate the submission of all other FOIA reports requested of NOAA;

d. maintain the NOAA FOIA home page;

e. retain copies of all FOIA requests and files in FOIAonline unless there is a documented strong business need to maintain outside of the web-based tool. Original copies of responsive records, whether released or not, are kept by the FOIA SO/LO Liaison or Action Office;

f. review all FOIA requests received by NOAA, including referrals from DOC and other federal agencies, and assign them to the appropriate FOIA Liaison whose office may have records responsive to the request and, when appropriate, suggest adding a task to additional office(s) at the time of assignment;

g. serve as agency lead for responding to all FOIA requests referred to NOAA from DOC;

h. maintain a list of all NOAA appeals and work with FOIA Liaisons to facilitate the appeals process;

i. function as the primary liaison between NOAA and DOC in resolving any FOIA issues; and

j. read each FOIA response to review metadata for completeness and mark as closed in FOIAonline.

2.7 SENIOR AGENCY INFORMATION SECURITY OFFICER (DIRECTOR, NOAA CYBER SECURITY DIVISION)

The NOAA Senior Agency Information Security Officer (SAISO) is the official responsible for carrying out the NOAA CIO's responsibility under FISMA. The NOAA SAISO shall:

- Issue through the NOAA CIO Council, NOAA-wide IT security policies, architectures, standards, best practices, and guidance that establish a framework for the IT Security program and ensures compliance with applicable federal statutes, regulations, policies and guidance.
- Designate in writing a NOAA OCIO IT Security Officer (ITSO) for the systems directly under the NOAA CIO as the primary AO.

- Serve as the principal advisor to the NOAA CIO on all matters (technical and otherwise) involving the security of the operating unit's IT systems.
- Maintain an accurate inventory of NOAA FISMA Systems.
- Monitor and evaluate the status of NOAA IT Security by overseeing Staff and Line Office security programs and system Authorizations to Operate.
- Track and report on NOAA-wide security posture including but not limited to weaknesses and POA&Ms to implement corrective actions.
- Ensure that all Staff and Line Office ACIOs appoint a Senior Agency Information Security Officer (SAISO)/Cyber Security Program Manager (CSPM) to establish, oversee, and execute the Staff or Line Office Cyber Security Program
- Ensure that the SAISO/PM has the staff and resources necessary to carry out the program in accordance with FISMA.
- Develop, implement, and maintain a computer incident response team within NOAA to ensure that NOAA has the expertise to manage security incidents.
- Maintain a security professional certification in accordance with the current DOC CITR.
- Ensure that an IT Security Awareness Training Program is developed, implemented, and managed, including procedures for all NOAA employees, contractors, and temporary personnel.
- Ensure that a risk management framework program is in place that provides support to authorization process for all NOAA IT systems.
- Ensure that NOAA systems are protected against malicious software through the acquisition and implementation of a NOAA-wide solution(s).
- Serve as the Chair of the NOAA IT Security Committee (ITSC) and hold regularly scheduled meetings to disseminate current information to Staff and Line Office ITSOs on issues relating to Federal, DOC/NOAA IT security law, policies, regulations, guidelines, or concerns.
- Coordinate with the DOC IT Security Program Manager and Critical Infrastructure Program Manager (CIPM), as well as the Office of Security (OSY),Office of the Inspector General (OIG) and NOAA Homeland Security, as appropriate, to address incidents, potential threats, and other IT security concerns.
- Maintain the Cyber Security Division Program web site.

2.8 NOAA IT SECURITY OFFICER

The assigned NOAA IT Security Officer (ITSO) will serve as backup to the Director, NOAA Cyber Security Division, function as the IT security liaison/focal point for Staff and Line Office ITSOs, and perform those duties assigned by the Director in support of the IT Security Program. In the absence of the NOAA ITSO the alternate NOAA ITSO will serve as the NOAA ITSO. The NOAA ITSO will:

- Serve as the central point of contact for the NOAA Cyber Security Division (CSD) and for NOAA security incidents.

- Implement NOAA wide IT security policies, architectures, standards, best practices, and guidance that establish a framework for the IT Security program and ensure compliance with applicable federal statutes, regulations, policies and guidance.
- Ensure all NOAA systems have in place effective and current security documentation, annual assessments, current and tested contingency plans, and current Assessments and Authorizations (A&As); via Staff and Line Office SAISOs/ITSOs
- Ensure the development of IT security policies, architectures, standards, best practices, and guidance which contributes to open, standard, scalable, interoperable, yet secure IT environments at the appropriate levels.
- Ensure 100% organizational participation in the NOAA IT Security Awareness Course (SAC). Review and monitor Staff and Line Office role-based security training programs to ensure compliance to the current DOC CITR.
- Ensure an inventory of FISMA systems in CSAM is maintained and coordinated with DOC to track compliance with DOC/NOAA IT Security Program requirements and provide updated inventories to the Director, NOAA Cyber Security Division as required.
- Advise NOAA SAISO of technological advances in IT security which can be used on an organizational scale and provide reduced cost for security efforts.
- Develop and track entity level remedial actions to mitigate risks in accordance with the DOC policies and procedures (e.g.: DOC CITR for plans of actions and milestone (POA&Ms) management).
- Recommend and adjudicate IT Security policy questions and requests for interpretation. Provide IT security guidance and technical assistance to the organizational IT security community.
- Disseminate information concerning potential security threats to NOAA IT information Staff and Line Office SAISOs and ITSOs, Network/System Administrator (N/SA) and IT Security community.
- Serve as directed on various committee and working groups and attend regularly scheduled meetings to disseminate current information on issues relating to federal, DOC/NOAA IT security law, policies, regulations, guidelines or concerns.
- Maintain a security professional certification in accordance with the current DOC CITR.

As appropriate, the ITSO may also take on the responsibilities of the Information System Security Engineer and Information Security Architect roles, as described in NIST SP 800-37.

Staff and Line Office ITSOs will serve similar roles, functions and responsibilities of the NOAA ITSOs within their respective offices.

2.9 LINE OFFICE SENIOR AGENCY INFORMATION SECURITY OFFICER/CYBER SECURITY PROGRAM MANAGER

The assigned Line Office Senior Agency Information Security Officer (SAISO)/Cyber Security Program Manager (CSPM) develops and oversees the LO cyber security program and manages staff of ITSOs who execute the LO cyber security program that consists of the responsibilities outlined below. In the absence of the Line Office SAISO/CSPM the Line Office ITSO will fill the role. The Line Office SAISO/CSPM will:

- Implement a risk-based security program.
- Serve as the AODR for unclassified Line Office information systems.
- Serve as the central point of contact for the Line Office IT Security program and for Line Office security incidents.
- Develop and implement Line Office IT security policies, architectures, standards, best practices, and guidance that establish a framework for the IT Security program and ensure compliance with applicable federal statutes, regulations, policies and guidance
- Ensure all Line Office systems have in place effective and current security documentation, annual assessments, current and tested contingency plans, and current Authorization to Operate (ATO).
- Develop IT security policies, architectures, standards, best practices, and guidance which contribute to open, standard, scalable, interoperable, yet secure IT environments at the appropriate levels.
- Ensure 100% participation of NOAA personnel in the NOAA IT Security Awareness Course.
- Review and monitor security training programs to ensure compliance to DOC CITR-006.
- Ensure that an inventory of FISMA systems in CSAM is maintained and coordinated with DOC to track compliance with DOC/NOAA IT Security Program requirements and provide updated inventories to the Director, NOAA Cyber Security Division as required.
- Advise appropriate levels of management of technological advances in IT security which can be used on an organizational scale and provide reduced cost for security efforts.
- Develop and track program level remedial actions to mitigate risks in accordance with the DOC CITR for plans of actions and milestone (POA&Ms) management.
- Recommend and adjudicate IT Security policy questions and requests for interpretation. Provide IT security guidance and technical assistance to the organizational IT security community.
- Ensure dissemination of information concerning potential security threats to Line Office IT information system owners, Network/System Administrator; (N/SA) and IT Security community.
- Serve as directed on various committees and working groups and attend regularly scheduled meetings to disseminate current information on issues relating to federal, DOC/NOAA IT security law, policies, regulations, guidelines or concerns.
- Maintain a security professional certification in accordance with DOC CITR-006.
- Serve as a voting member of the NOAA IT Security Committee and attend regularly scheduled meetings to obtain current information on issues relating to federal, DOC/NOAA IT security law, policies, regulations, guidelines or concerns.

As appropriate, the SAISO may also take on the responsibilities of the Information System Security Engineer and Information Security Architect roles, as described in NIST SP 800-37.

Line Office SAISOs/ITSOs will serve similar roles, functions and responsibilities of the NOAA ITSOs within their respective offices.

2.10 NOAA IT SECURITY COMMITTEE

The National Oceanic and Atmospheric Administration (NOAA) Information Technology Security Committee (ITSC) leads the NOAA wide development, implementation and maintenance of the enterprise IT Security Program. This is accomplished through the development and promulgation of policies and guidance, coordination of IT security activities, and strategic planning across all line offices. The ITSC also researches and develops recommendations to the NOAA Chief Information Officer's (CIO) Council on IT security issues.

The NOAA IT Security Committee is made up primarily of the NOAA SAISO/CSMP, Director of Cyber Security, NOAA ITSO, all Line Office SAISOs, all Line Office ITSOs, and/or their alternates.

The NOAA ITSC will:

- Provide governance for the NOAA IT Security Program.
- Recommend NOAA-wide policies to the NOAA CIO Council.
- Identify activities and specific coordination to be proposed for the DOC IT
- Facilitate an open forum for the sharing and discussion of IT security issues and concerns.
- Review enterprise-wide IT security products and services.

2.11 AUTHORIZING OFFICIAL

An Authorizing Official (AO) must be at least a senior official or executive with the authority to formally assume responsibility and risk for operating an information system and associated data at an acceptable level of risk.

Within NOAA, the NOAA CIO will serve as the Co-Authorizing Official (Co-AO) for all high systems. For all low and moderate systems, the Line Office Assistant CIO serves as Co-AO as delegated by the NOAA CIO. A Co-AO is necessary when the AO is not in the chain of command of the NOAA CIO.

The NOAA CIO delegates AO authority to the LO AA (or Deputy AA) with the privilege of delegating that authority further within the LO the LO AA (or Deputy AA) being required to notify the NOAA CIO in writing of any re-delegation. For high-impact systems, the AO must be a member of the Senior Executive Service (SES). The AO must ensure that adequate resources are allocated to A&A activities from system security categorization to post-authorization continuous monitoring.

The AO will:

- Execute the budget and business operations of the information systems within their area of responsibility.
- Collaborate with the Co-AO for an acceptable level of risk to operations, assets, or individuals by executing risk-based decision supported by an ATO. The ATO decision must be based on an annual assessment that includes the key components as outlined in NIST SP 800-37.
- Appoint a system owner (SO) for each IT system in concert with the Co-AO, as appropriate, and in writing.

- Review all A&A packages for compliance to requirements. Ensure risk acceptances are valid and justified.
- Approve the FIPS 199 security categorization, FIPS 200 Security Control Selection, documentation of security controls baseline tailoring risk acceptance, and any other Risk Acceptance documentation, including acceptance of risk, and the Authorization to Operate memoranda and all ATO supporting documentation for those systems for which they are responsible. AOs also are required to sign any external agreement such as an ISA or MOU/A. An AO may also approve the system's security plan (SSP) and other key documents, but may delegate this approval to the AO Designated Representative (AODR).
- For high impact systems, the Co-AO and AO must both approve the delegation of risk acceptance to the AODR.

2.12 CO-AUTHORIZING OFFICIAL

Within NOAA, the NOAA CIO will serve as the Co-Authorizing Official (Co-AO) for all high systems. For all low and moderate systems, the Line Office Assistant CIO serves at Co-AO as delegated by the NOAA CIO. This role provides oversight and serves to provide a consistent application of risk management and tolerance principles across NOAA and within individual Staff and Line Offices. This role is not the same as a primary AO, and is not required to be operationally involved throughout the day to day management and decision making for an IT system.

The Co-AO along with the primary AO, a Co-AO must agree and sign the following key security documents including: the FIPS 199 Security Categorization, FIPS 200 Security Control Selection and any Risk Acceptance documentation, such as an acceptance of risk, and the Authorization to Operate memoranda and all ATO supporting documentation.

2.13 COMMON CONTROL PROVIDER

The NOAA common control provider is the NOAA OCIO IT Security Office, which is responsible for the development, implementation, assessment, and monitoring of common control designations for NOAA systems. Please see Section 3.3.8 Common Control Provider in the *DOC ITSPP*, 2014.

2.14 NOAA IT RISK MANAGEMENT OFFICER

The NOAA IT Risk Management Officer (ITRMO) is appointed by the NOAA CIO.

The NOAA IT Risk Management Officer helps ensure:

I. Risk-related considerations for individual information systems, to include authorization decisions, are viewed from an NOAA-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and

II. Managing information system-related security vulnerabilities and risks is consistent across NOAA, reflects NOAA risk tolerance and is considered along with other types of risks in order to ensure mission/business success.

The ITRMO coordinates with the senior leadership of NOAA Cyber Security Division to:

- Provide a comprehensive, NOAA-wide, holistic approach for addressing IT Security risk an approach that provides a greater understanding of the integrated operations of the organization.
- Identify and manage information security risks to achieve mission objectives.
- Develop an IT Security risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole.
- Facilitate the sharing of IT Security risk-related information among authorizing officials and other senior leaders within the organization.
- Provide oversight for all IT Security risk management-related activities across the organization (e.g., security categorizations) to ensure consistent and effective risk acceptance decisions.
- Ensure authorization decisions consider all factors necessary for mission and business success.
- Provide a NOAA-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation.
- Ensure the shared responsibility for supporting NOAA mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities.
- Identify the organizational IT Security risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

2.15 NOAA COMPUTER INCIDENT RESPONSE TEAM

The Director, NOAA Cyber Security Division manages the NOAA Computer Incident Response Team (N-CIRT) that serves as the focal point for NOAA on all matters relating to any type of IT security-related incidents or violations. The N-CIRT has authority to make all decisions during the incident response process. The N-CIRT will:

- Coordinate all reported incidents with the DOC IT Security Program Manager (ITSPM), DOC Office of Inspector General (OIG), DOC Office of Security (OSY), Federal Bureau of Investigation (FBI), and Department of Homeland Security (DHS) US Computer Emergency Readiness Team (US-CERT).
- Establish procedures for reporting and receiving information regarding incidents affecting NOAA. This will include establishing a hotline for reporting, tracking, and coordinating incident data, and maintaining a database of incidents to analyze and assess overall threats.
- Provide incident response services to NOAA as defined in NIST SP 800-61, DOC policy, federal policy, and US-CERT Concept of Operations.
- Perform and coordinate organizational computer forensic information gathering as required in support of legal activities for NOAA.

- Monitor the resolution of all incidents and prescribe corrective actions pursuant to incident containment and recovery.
- Provide other organizational support services that may include (in a directed manner) provisions for the Vulnerability Monitoring and Regression Testing activity that includes an ad-hoc end-user liaison function, tools, education, auditing, consulting, product evaluation, and security testing in product evaluation.
- Provide the organizational community guidance and technical assistance on NOAA anti-virus software.
- Assist in the development of policy and guidance for N-CIRT and N/SAs.
- Participate in NOAA ITSC meetings.
- Monitor NOAA campuses for wireless networks. Wireless networks found to be in noncompliance will be reported to the Staff and Line Office ITSO, the relevant Authorizing Official (AOs), the ACIO for the Line Office, or, as appropriate, the NOAA Cyber Security Division or NOAA CIO office for action.

2.16 SECURITY OPERATION CENTER

The NOAA Security Operation Center (SOC) serves as a central clearinghouse for all reported organizational incidents. The SOC will provide appropriate security alerts, bulletins, and other security related material as well as disseminate to all NOAA IT Systems Owners and Managers prompt advisories of system threats, operating system vulnerabilities, and tracking information related to reported incidents, trends, and impacts.

2.17 CERTIFICATION AGENT/SECURITY CONTROL ASSESSOR/CERTIFIER

The Security Control Assessor (SCA) (also referred to as “Certifier” or “Certification Agent”) is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). SCAs also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. In addition to the above responsibilities, Security Control Assessors prepare the final security assessment report containing the results and findings from the assessment.

For assessments that require independence (moderate and high systems), the AO or AODR must approve the designation of the SCA. For these systems, the SCA will not be in the same chain of command as the primary SO but is in the same chain as the primary AO.. For control assessments that do not require independence (low systems), the SO may appoint the SCA.

The SCA role may be filled by a variety of methods. A Staff and Line Office may choose to contract out to a vendor to obtain the services. Or they may use a NOAA Staff and Line Office assessment team Staff and Line Office that is not within the same chain of command as the

primary AO Official of the system under assessment. The SCA lead must comply with the professional certification requirements of DOC CITR-006.

2.18 INFORMATION SYSTEM OWNER

As described in the NIST SP-800-37, Appendix D.4, the Information System Owner (SO) (System Owner/Project Manager) has many responsibilities in addition to the day-to-day operation and maintenance of their systems as well as direct oversight of the system/network administrators and operations staff. The information SO is the NOAA or Staff and Line Office manager responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system, and relies on the assistance and advice of the appropriate Staff and Line Office SAISO/ITSO and other IT staff in the implementation of the following security responsibilities. For IT systems (classified and/or unclassified) under their responsibility, System owners will:

- Ensure that security considerations are included in the systems lifecycle management.
- Develop and maintain the system's SSP and perform continuous monitoring to ensure that the system is deployed and operated at an acceptable risk level in accordance with the AO-approved security controls baseline.
- Develop and maintain specific procedures for implementing security policies and requirements for systems under their preview.
- In coordination with the information owner/steward, the SO will decide who has access to the system (and with what types of privileges or access rights) and ensure system users and support personnel receive the requisite security awareness training (e.g., instruction in rules of behavior) and role-based training.
- Based on guidance from the AO or AODR, the SO will inform appropriate organizational officials of the need to conduct the security authorization, ensure the necessary resources are available for the effort, and provides the required information system access, information, and documentation to the SCA as agreed in the Security Assessment Plan.
- Assemble the security authorization package, recommend draft POA&Ms or risk acceptance, and submit the package to the authorizing officials for approval.
- Ensure all controls are effective and operating as intended, and for those with POA&Ms, ensure actions are taken and POA&Ms are closed on schedule.
- Ensure system users, system administrators and ISSOs receive system specific security awareness training and education as appropriate and acknowledge acceptance of responsibility as required.
- Ensure personnel designated in the SSP control AT-3 as having a role with significant IT security responsibilities comply with DOC CITR-006.
- Maintain an updated list of hardware and software inventory operated/used by the system.
- Ensure that IT system security documentation such as contingency plans are maintained and tested as required.
- Routinely perform security impact analysis as part of system configuration changes ensuring the awareness of the system's security posture.

- Appoint an ISSO, and if necessary an Alternate ISSO, in writing and ensure the ISSO maintains a professional certification as required by DOC-CITR-006.
- Identify, in writing, a(n) Account Manager(s)/Network and System Administrators, responsible for the creation, deletion and change of user IDs.

2.19 INFORMATION SYSTEM SECURITY OFFICER

Each Information System Security Officer (ISSO), supported by an Alternate ISSO if appropriate, will design, implement, and maintain IT system security controls continuous monitoring program consistent with DOC/NOAA, and government-wide laws, regulations, policies, procedures, and standards. The ISSO implements controls and executes the Program as required by DOC, NOAA, and SO/LO policies. The ISSOs are appointed in writing by the SO and must implement the system-level controls and maintain system documentation. The ISSO is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information system owner. The ISSO also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The ISSO has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned by the SO the responsibility for the continuous monitoring of day-to-day security operations of a system. This responsibility may also include, but is not limited to, physical and environmental protection, personnel security, incident handling, and security training and awareness. The ISSO may be called upon to assist in the development of the security policies and procedures and to ensure compliance with those policies and procedures. In close coordination with the Information System Owner, the ISSO often plays an active role in the monitoring of a system and its environment of operation to include developing and updating the security plan, managing and controlling changes to the system, and assessing the security impact of those changes.

The ISSO will:

- Advise the System Owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e., life cycle management).
- Assist in the determination of an appropriate level of security commensurate with the level of security categorization of the system.
- Assist in the development and maintenance of security and contingency plans for all FISMA ID systems under their responsibility.
- Participate in security impact analysis for system changes and annually review the security categorization of the system, risks, and risk mitigation strategies.
- Serve as the point of contact for all security incidents within their area of responsibility and reports as appropriate to the NOAA Computer Incident Response Team (N-CIRT). Handles and investigates incidents in cooperation with and under direction of the Staff and Line Office ITSO and N-CIRT.
- Participate in vulnerability scanning and penetration testing of systems/networks.
- Not function as the network and/or systems administrator for any Moderate- or High-impact system they are assigned to as the ISSO unless a waiver with justification is

requested from the Staff and Line Office ACIO. Separation of duties dictates that an ISSO cannot be a systems administrator for the same IT system.

- Ensure that all user accounts are disabled within 24 hours of notification of user's separation from employment and immediately for individuals being separated for adverse reasons.
- Monitor and review system security policy, practices, and procedures at least annually, and update as necessary.
- Ensure the security of all interfaces between the IT system and external systems by developing, maintaining, and enforcing interconnection agreements (ISA, SLA, MOU, and MOA).
- Maintain a security professional certification as specified by DOC CITR-006.

2.20 INFORMATION SECURITY ARCHITECT

The Information Security Architect is an individual, group, or organization within a Staff or Line Office who will ensure the selection of security controls is consistent with the enterprise architecture, including reference models and segment and solution architectures. They will ensure that the information security requirements necessary to protect NOAA's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. The information security architect will serve as the liaison between the enterprise architect and the information system security engineer and also coordinate with information system owners, common control providers, and information system security officers on the allocation of security controls as system-specific, hybrid, or common controls. In addition, the information security architect, in close coordination with information system security officers, will advise authorizing officials, chief information officers, senior information security officers, and the risk executive (function), on a range of security-related issues including, for example, establishing information system boundaries, assessing the severity of weaknesses and deficiencies in the information system, plans of action and milestones, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

The ITSO/SAISO may also take on the responsibilities of the Information Security Architect.

2.21 INFORMATION SYSTEM SECURITY ENGINEER

The Information System Security Engineer is an individual, group, or organization that will conduct information system security engineering activities including:

- Provide advice on the continuous monitoring of the information system
- Provide advice on the impacts of system changes to the security of the system
- Participate in the configuration management process
- Participate in any acquisition/development activities that are required to implement a system change
- Implement approved system changes

The ITSO/SAISO may also take on the responsibilities of the Information System Security Engineer.

2.22 NETWORK/SYSTEM ADMINISTRATOR (N/SA)

Each system and or network(s) within NOAA will have administrators to perform IT security implementation through installation and configuration of IT resources. The N/SAs will:

- Take action for specific aspects of system security, such as adding and deleting user accounts as authorized by the system owner or ISSO, patching systems, implementing secure configurations as prescribed in the system security plans, and normal operations of the system in keeping with job requirements.
- Implement DOC, NOAA, and Staff and Line Office security policies, procedures, and guidelines on local systems and networks.
- Assist in the development and maintenance of security and contingency plans for FISMA ID systems under their responsibility.
- Participate in security impact analysis of system configuration changes and in the annual review of the system security categorization , risks, and mitigation strategies.
- Participate in continuous monitoring assessments of system safeguards and program elements and in annual authorization and assessment of the system.
- Evaluate proposed technical security controls to assure proper integration with other system operations.
- Identify requirements for resources needed to effectively implement technical security controls.
- Assures the integrity of technical security controls.
- Report all incidents to the system ISSO and system owner and assist in the investigation of incidents as directed.
- Develop system administration and operational procedures and manuals.
- Evaluate and develop procedures that assure proper integration of service continuity with other system operations.
- Know which systems or parts of systems for which they are directly responsible (e.g., network equipment, servers, LAN, etc.).
- Know the sensitivity of the data they handle and take appropriate measures to protect it.
- Will not function as the ISSO on any system he/she functions as the system administrator unless there has been security baseline controls tailoring to the AC-5 control requirements, with justification is requested from the Staff and AOs/Line Office ACIO.
- Maintain the system(s) baseline(s), coordinating changes with the ISSO, SO and Change Control Board (CCB) and obtaining approval for baseline deviations.

2.23 EMPLOYEES, CONTRACTORS AND TEMPORARY PERSONNEL (END USERS)

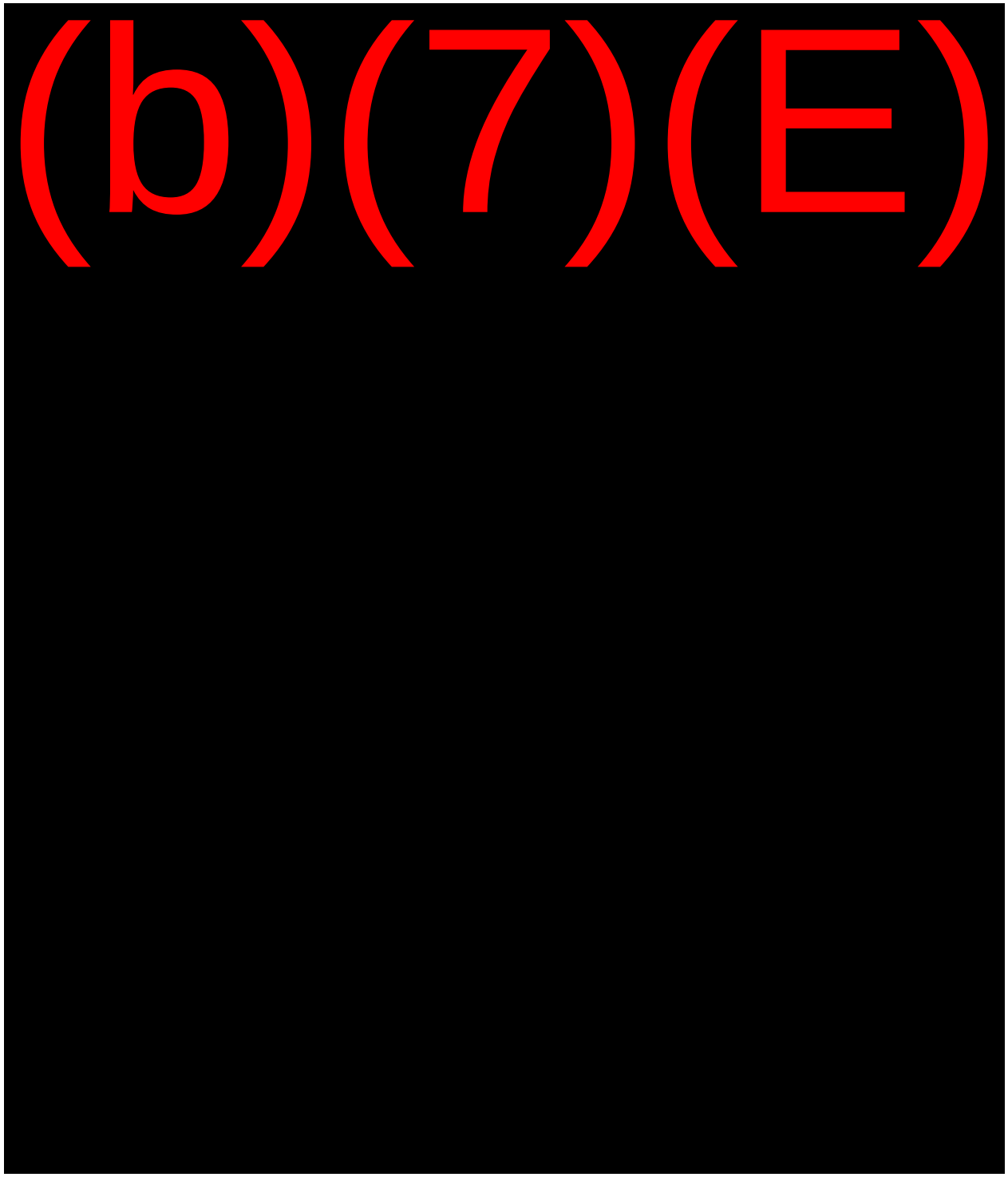
Each employee, including contractors and temporary personnel, is responsible for the adequate protection of IT resources based on the security category of the information within their control or possession, e.g., laptops, devices, passwords. End users will also be vigilant in performing necessary security procedures in order to maintain the confidentiality, integrity, and availability of the information. End users will:

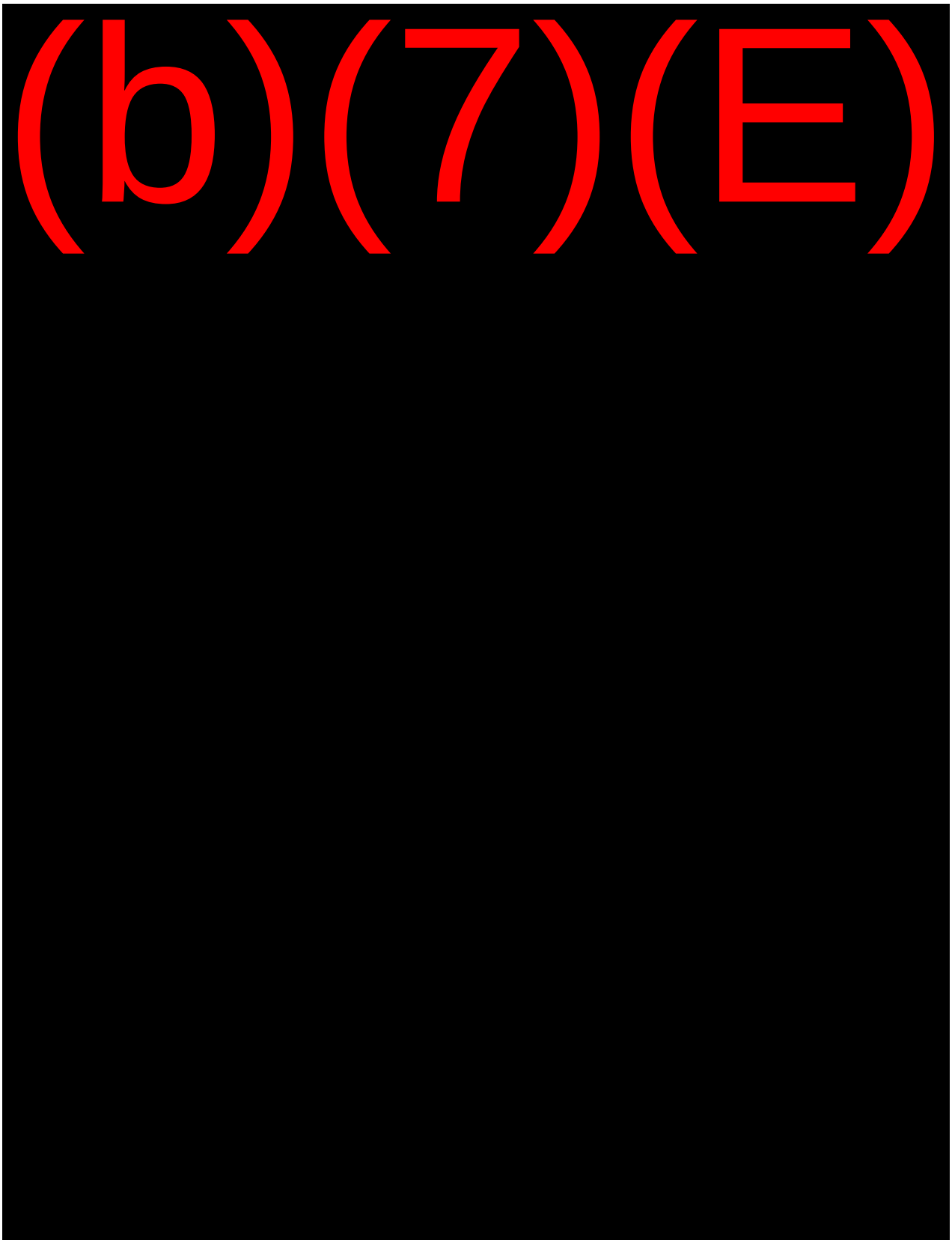
- Participate in the IT Security Awareness Program by completing the NOAA IT security awareness training annually as required;
- Follow installation procedures and requirements for the protection of information resources to which access is granted;
- Report IT security incidents according to established policies and in a timely manner to appropriate managers or supervisors and to the ISSO and cooperate in the investigation of incidents;
- Comply with all NOAA security program policy, passwords, rules of behavior, and appropriate use policy requirements regarding use or abuse of operating unit IT resources; and
- Protect sensitive information and data that resides on mobile devices and/or portable storage devices (USB drives, CD-ROMs, etc.) that are under the users control.

SECTION 3: SECURITY POLICIES

This page is intentionally blank.

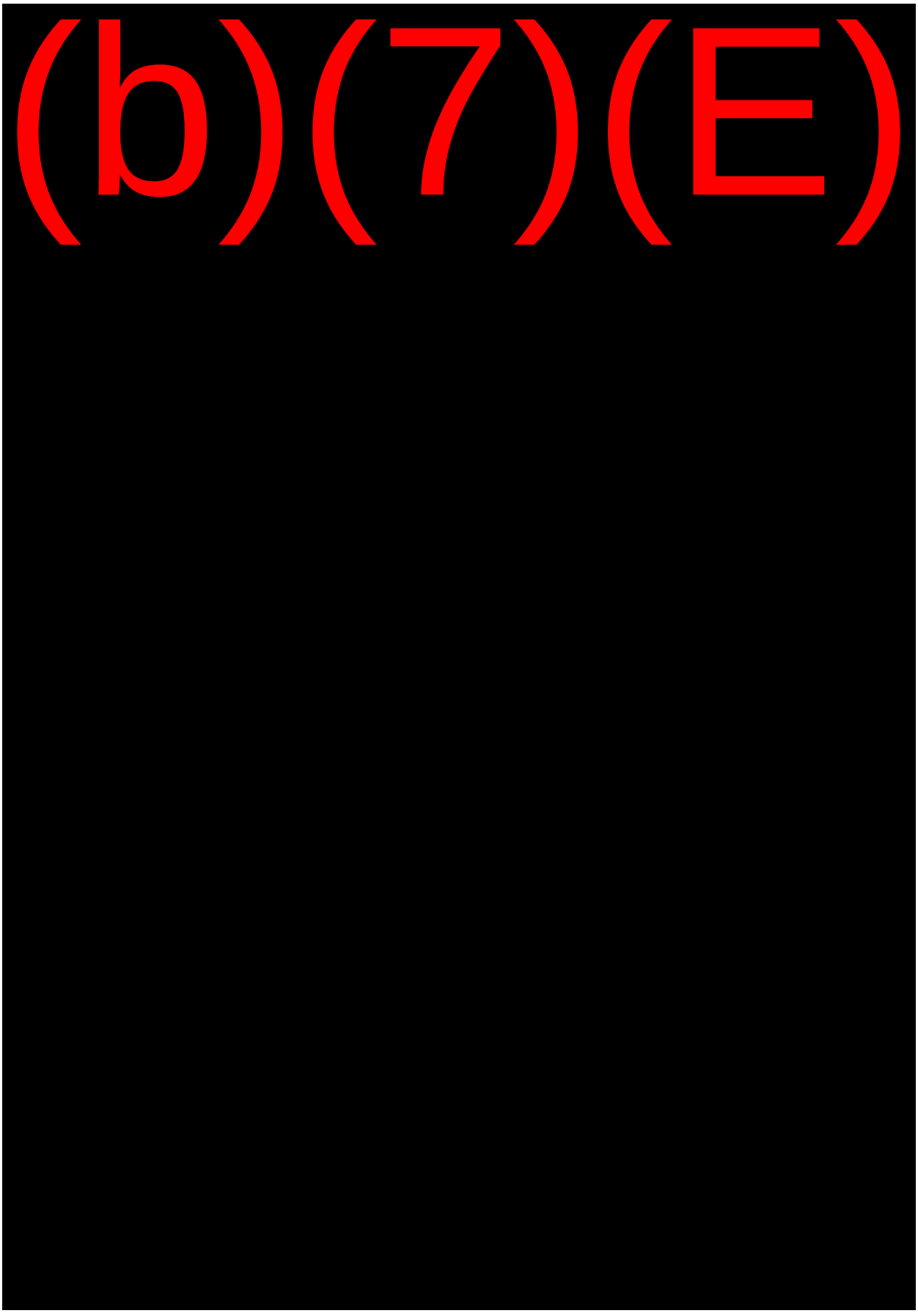
3 SECURITY CONTROLS POLICIES

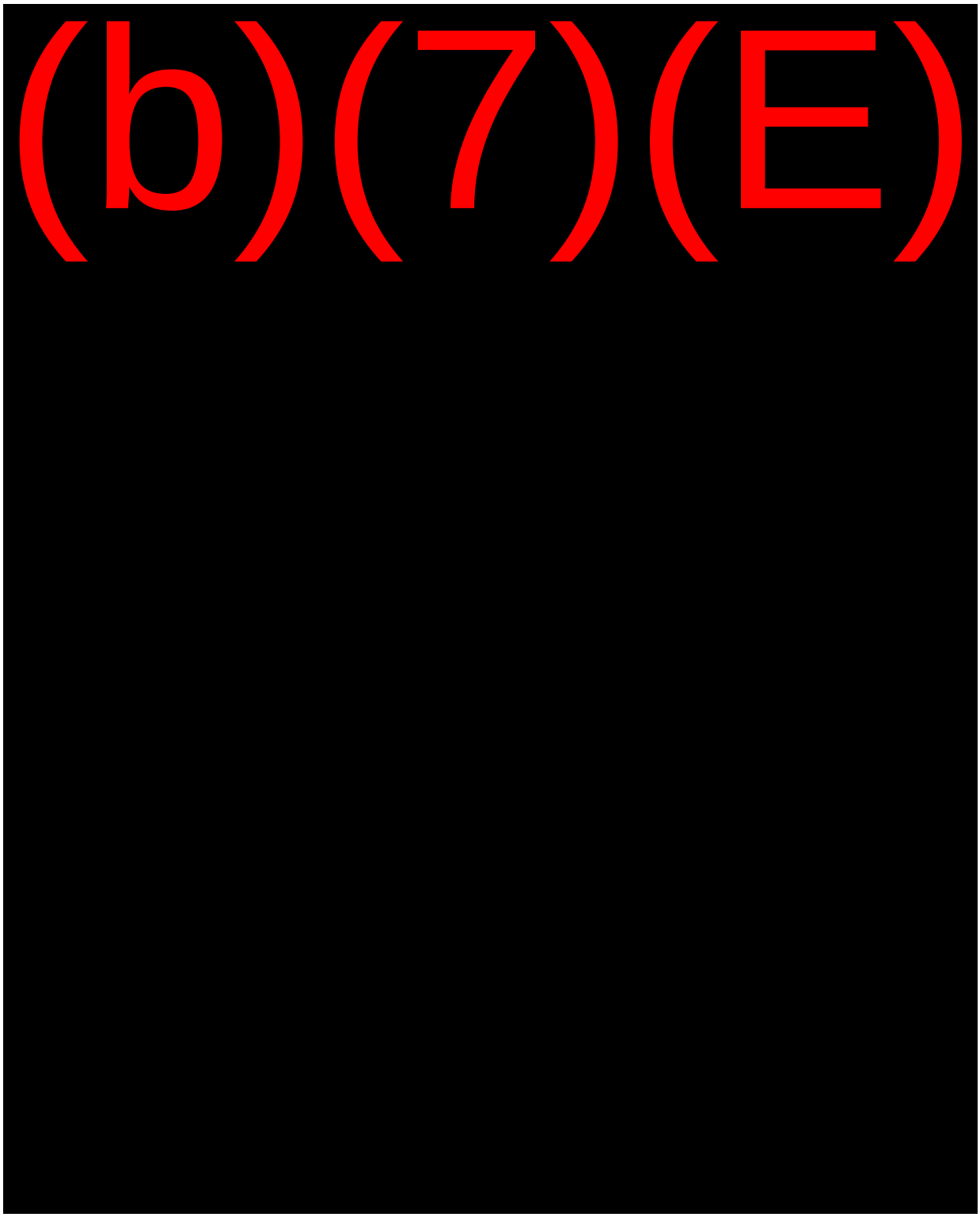



(b)(7)(E)

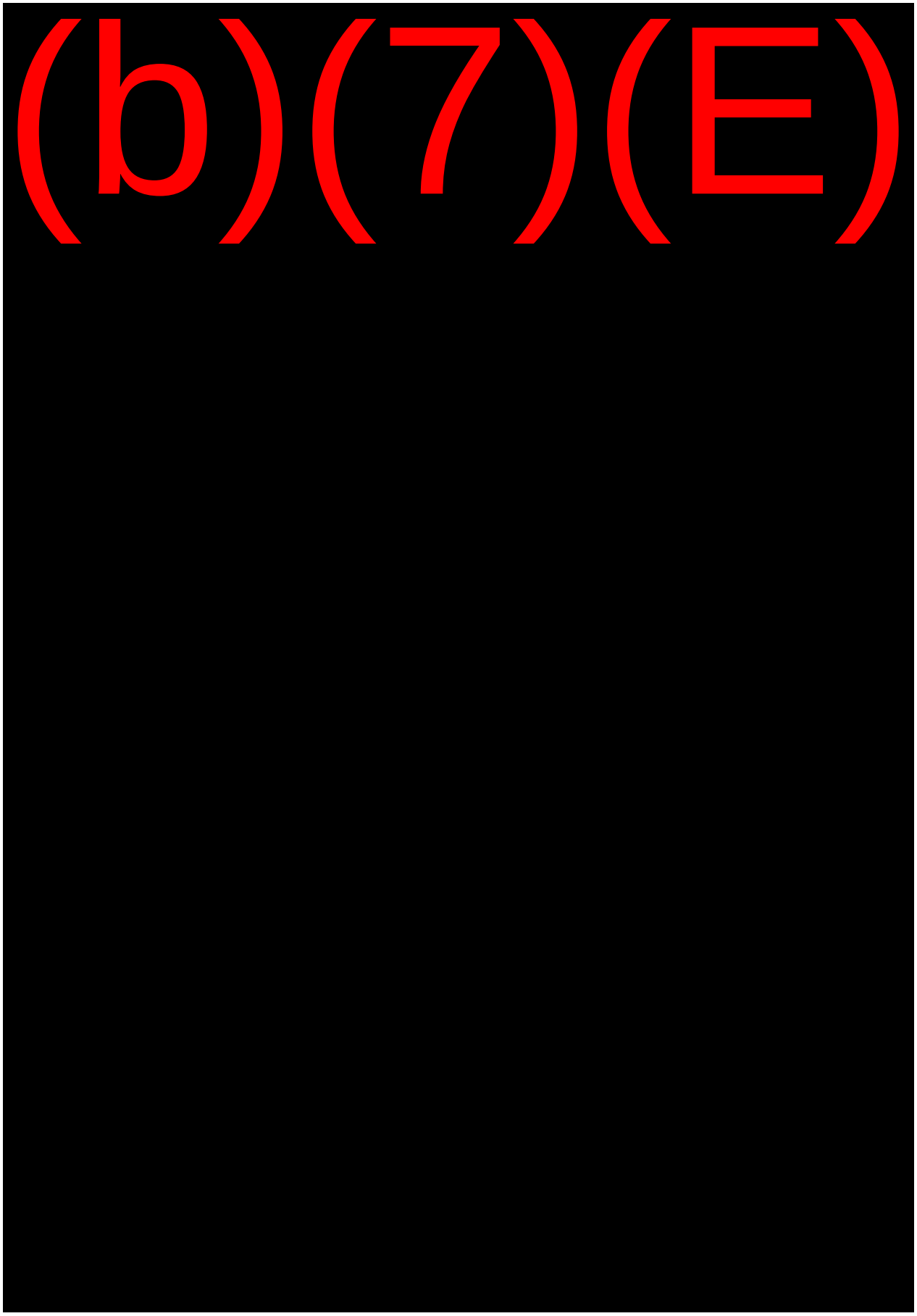

(b)(7)(E)

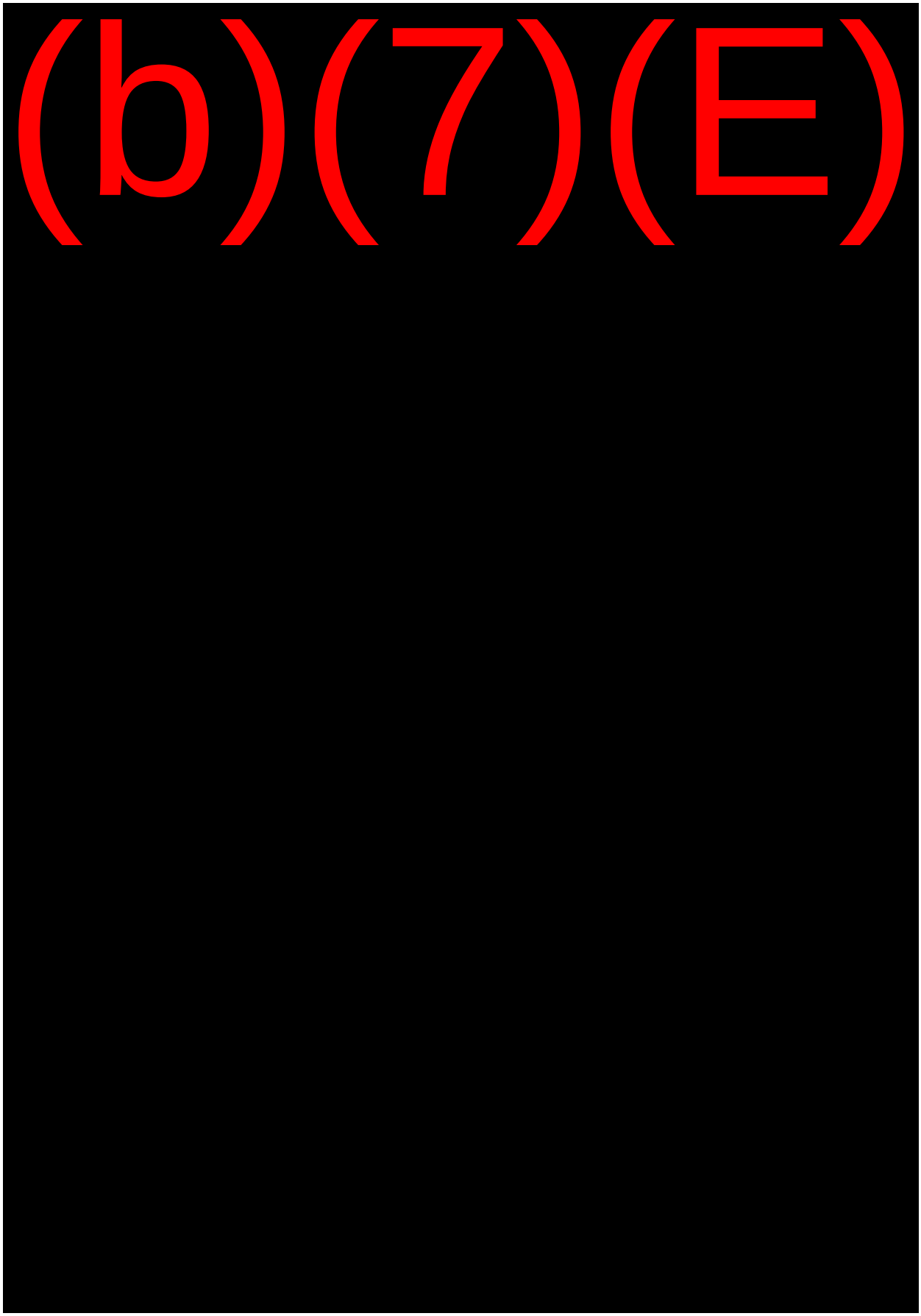

(b)(7)(E)

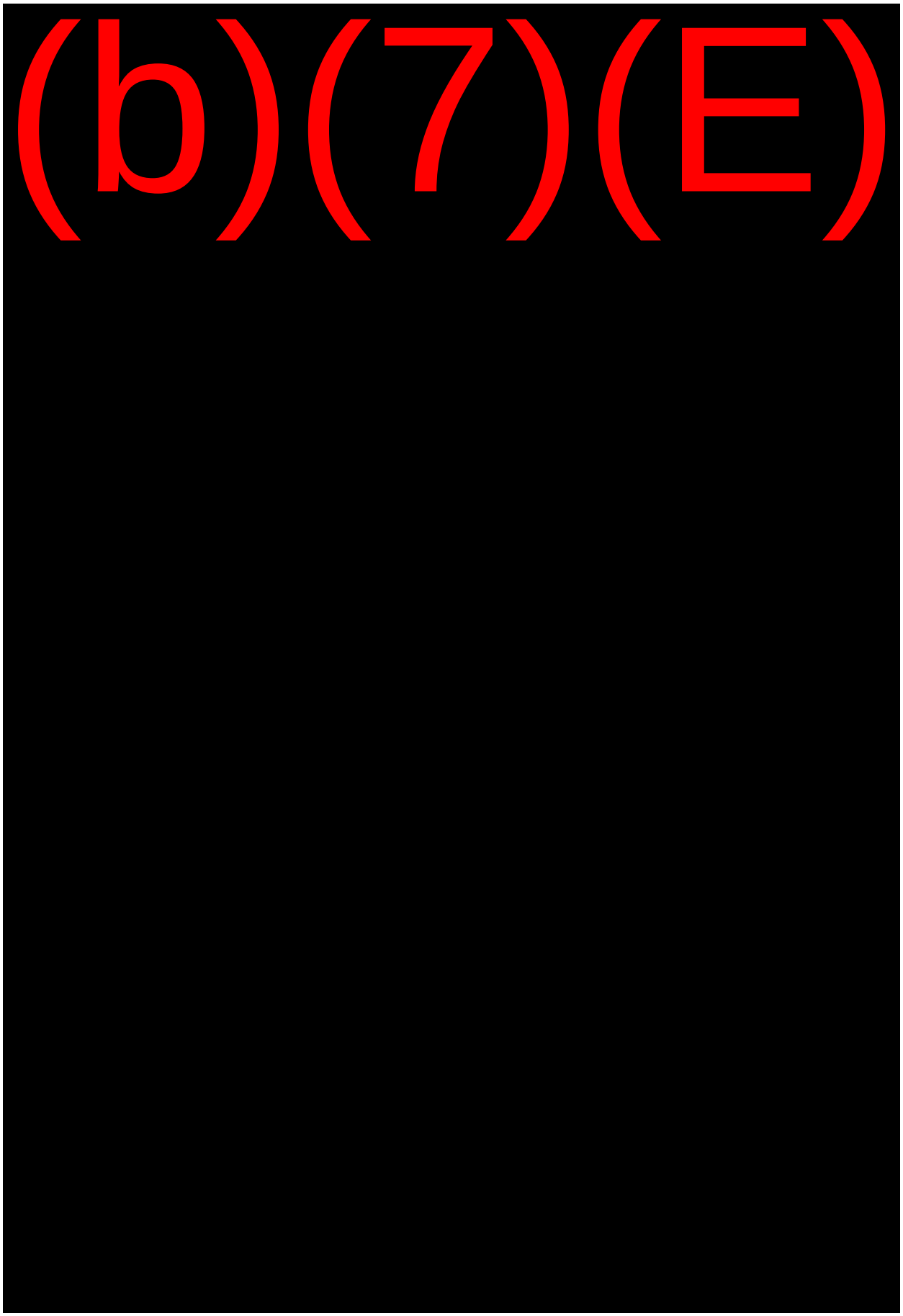

(b)(7)(E)

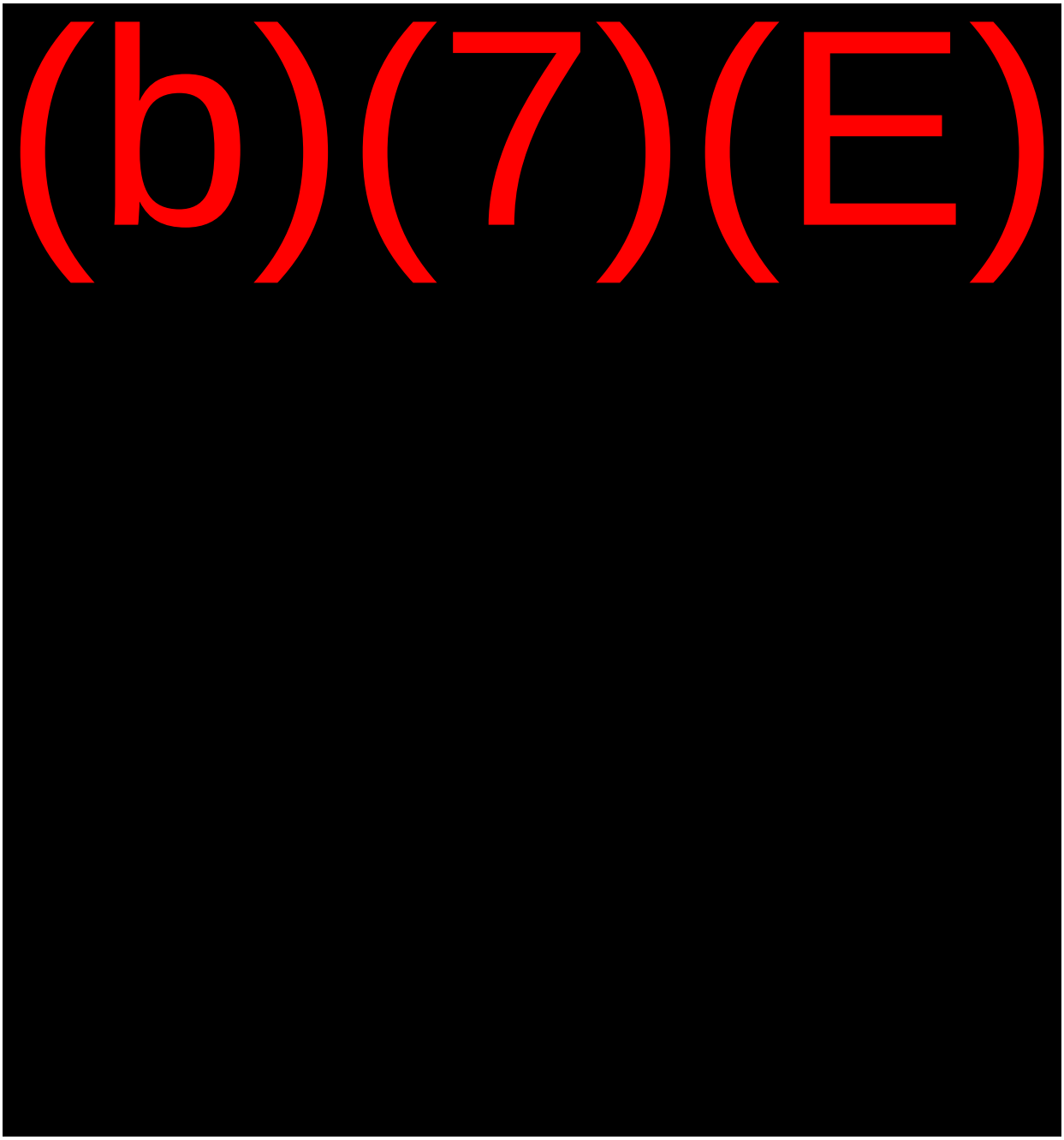

(b)(7)(E)


(b)(7)(E)

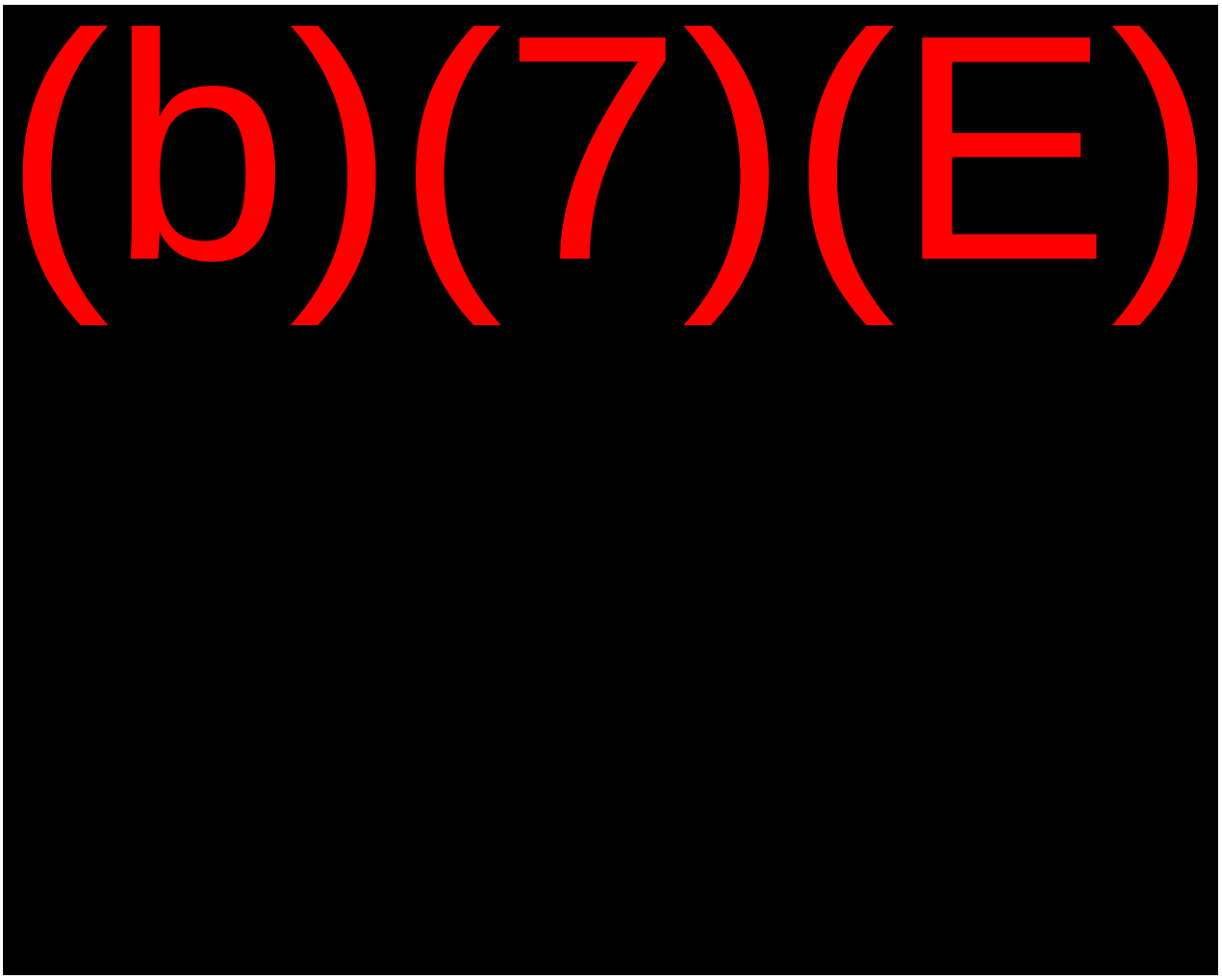

(b)(7)(E)

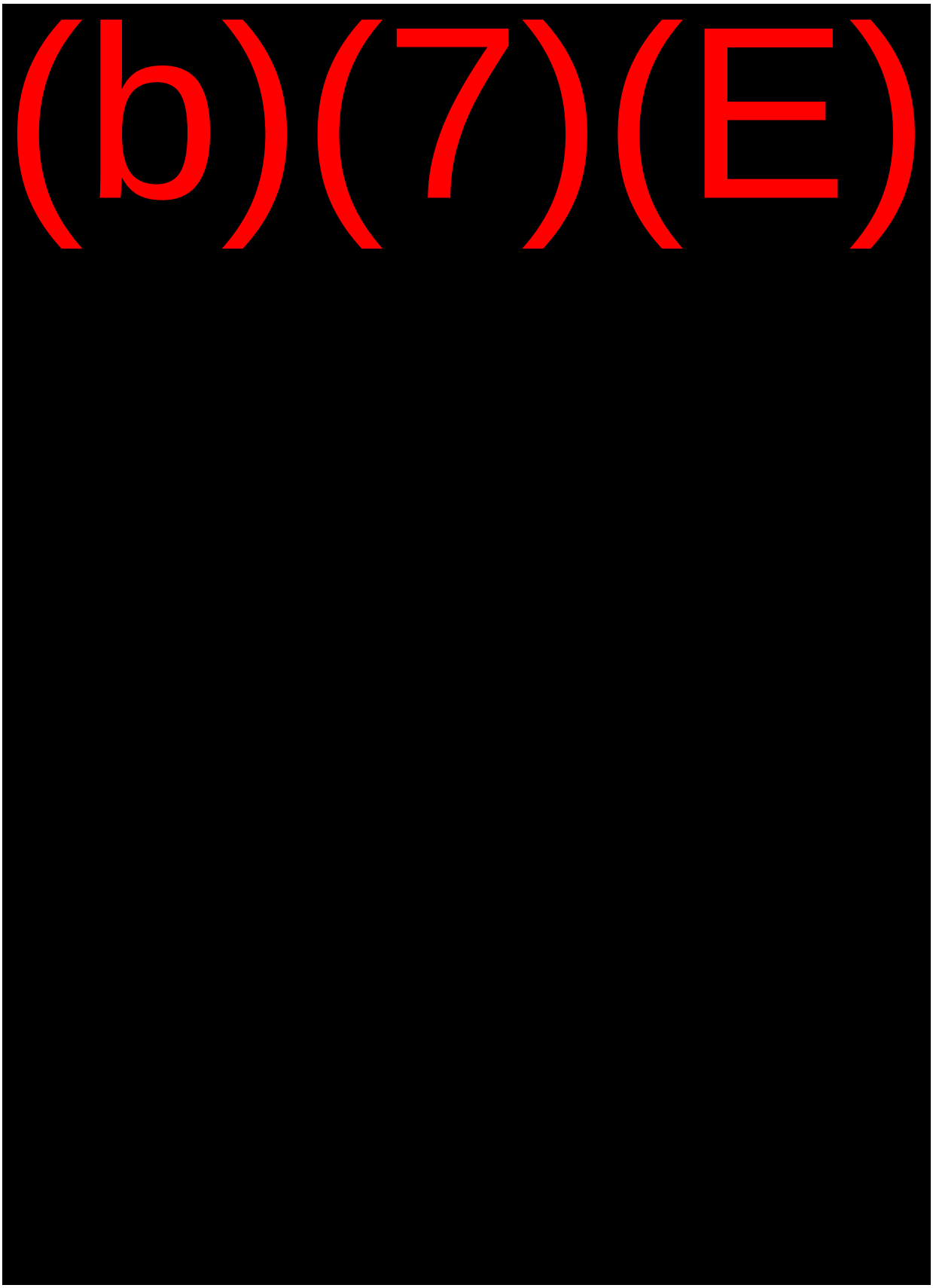

(b)(7)(E)


(b)(7)(E)

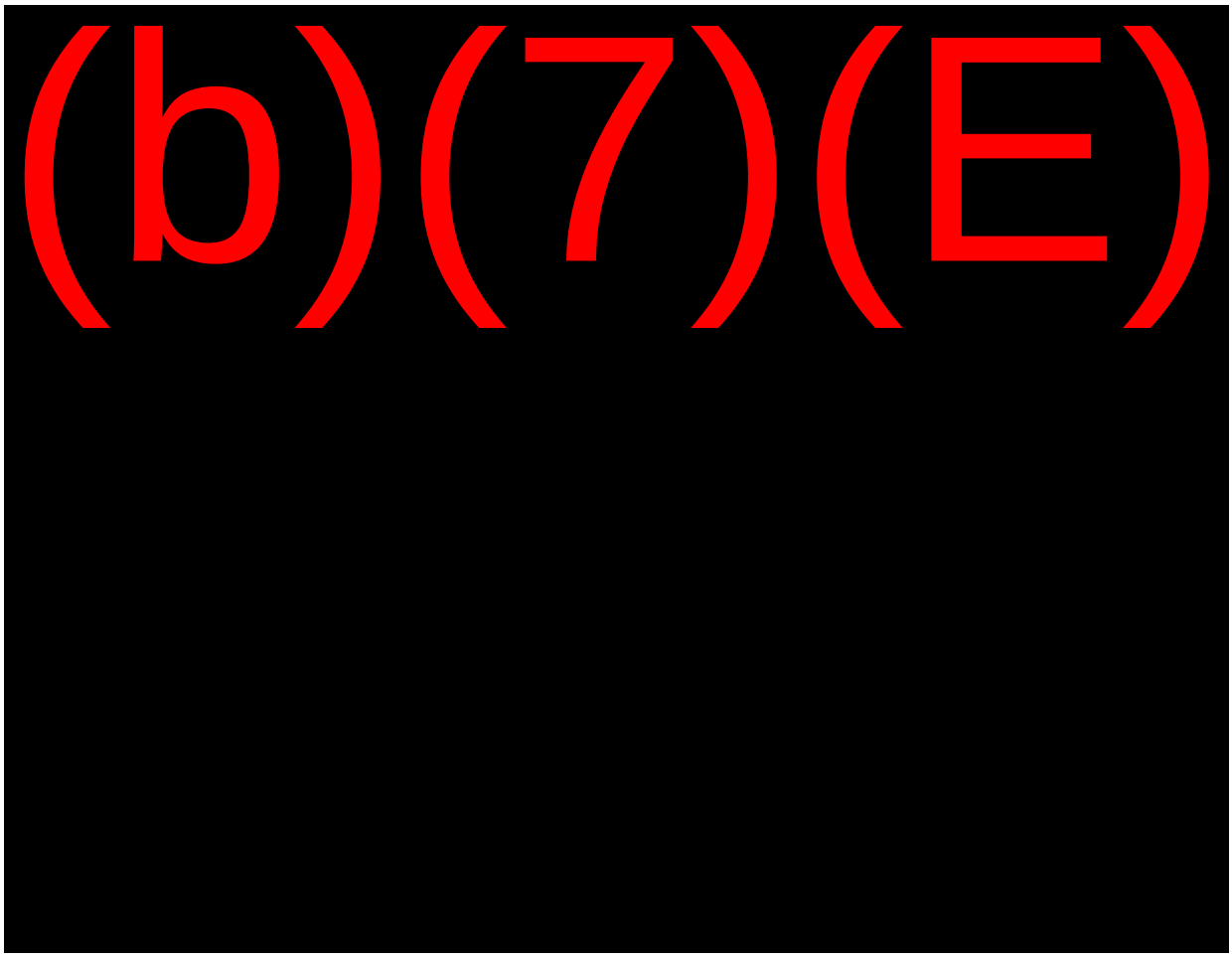

(b)(7)(E)

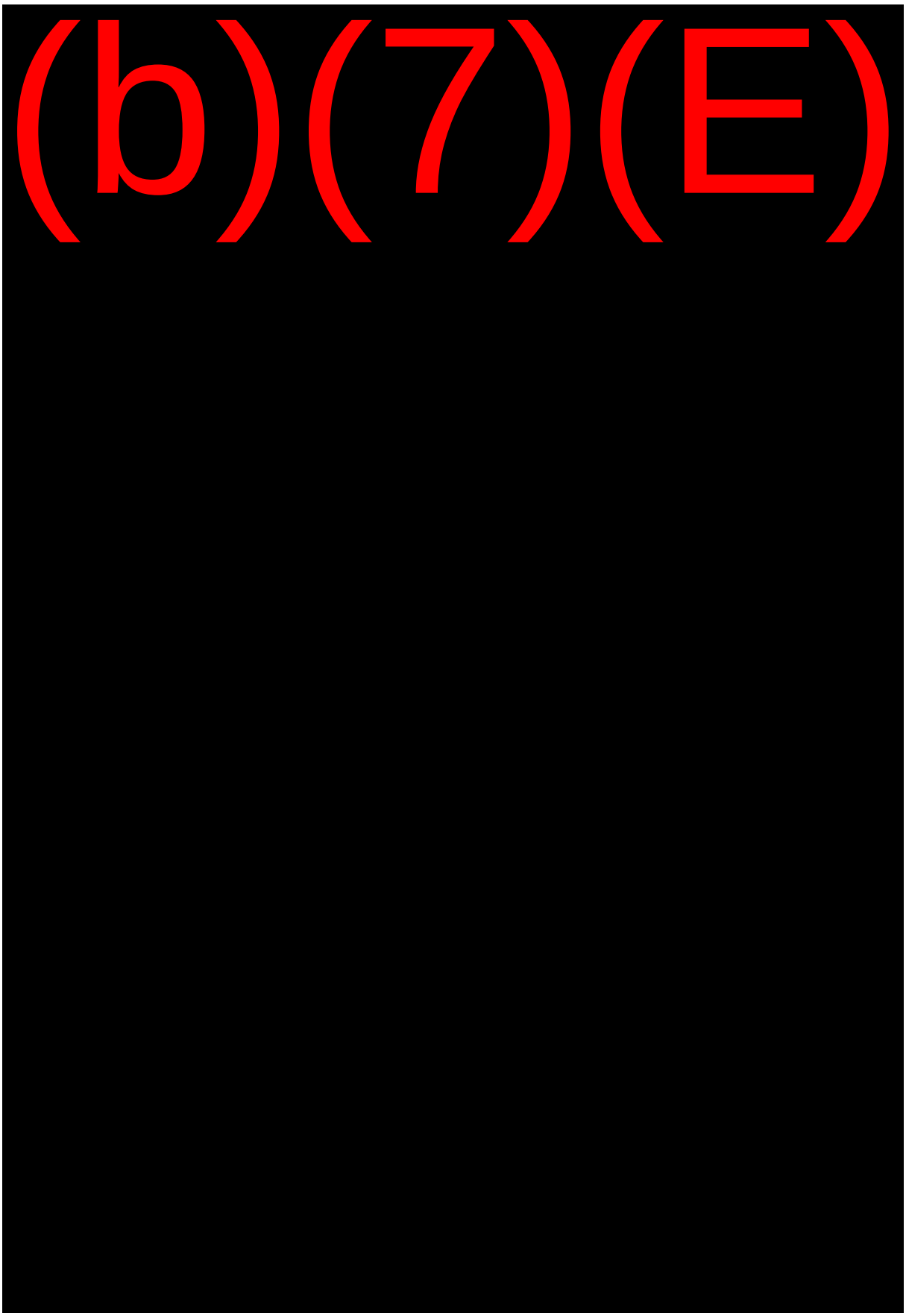

(b)(7)(E)

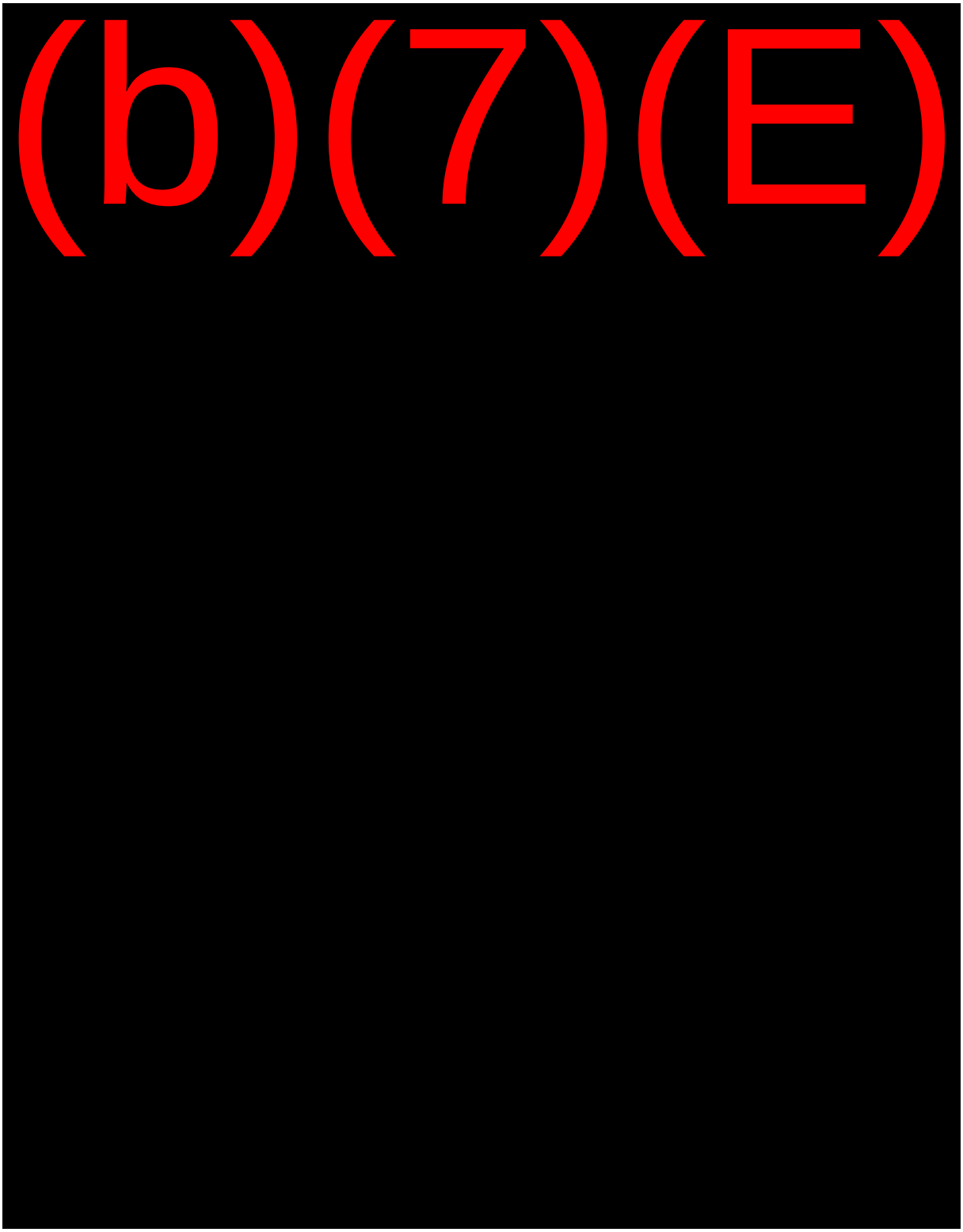

(b)(7)(E)

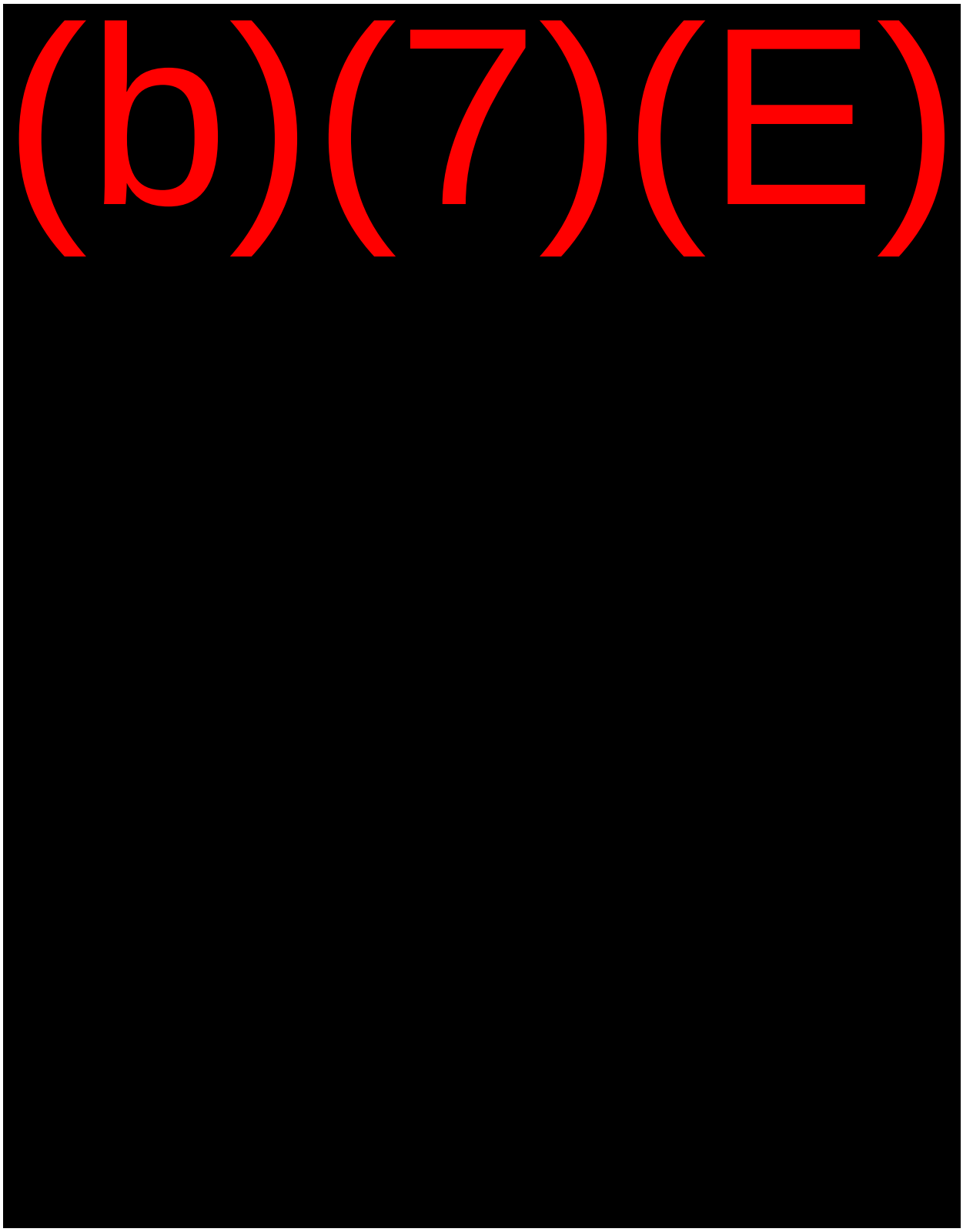

(b)(7)(E)

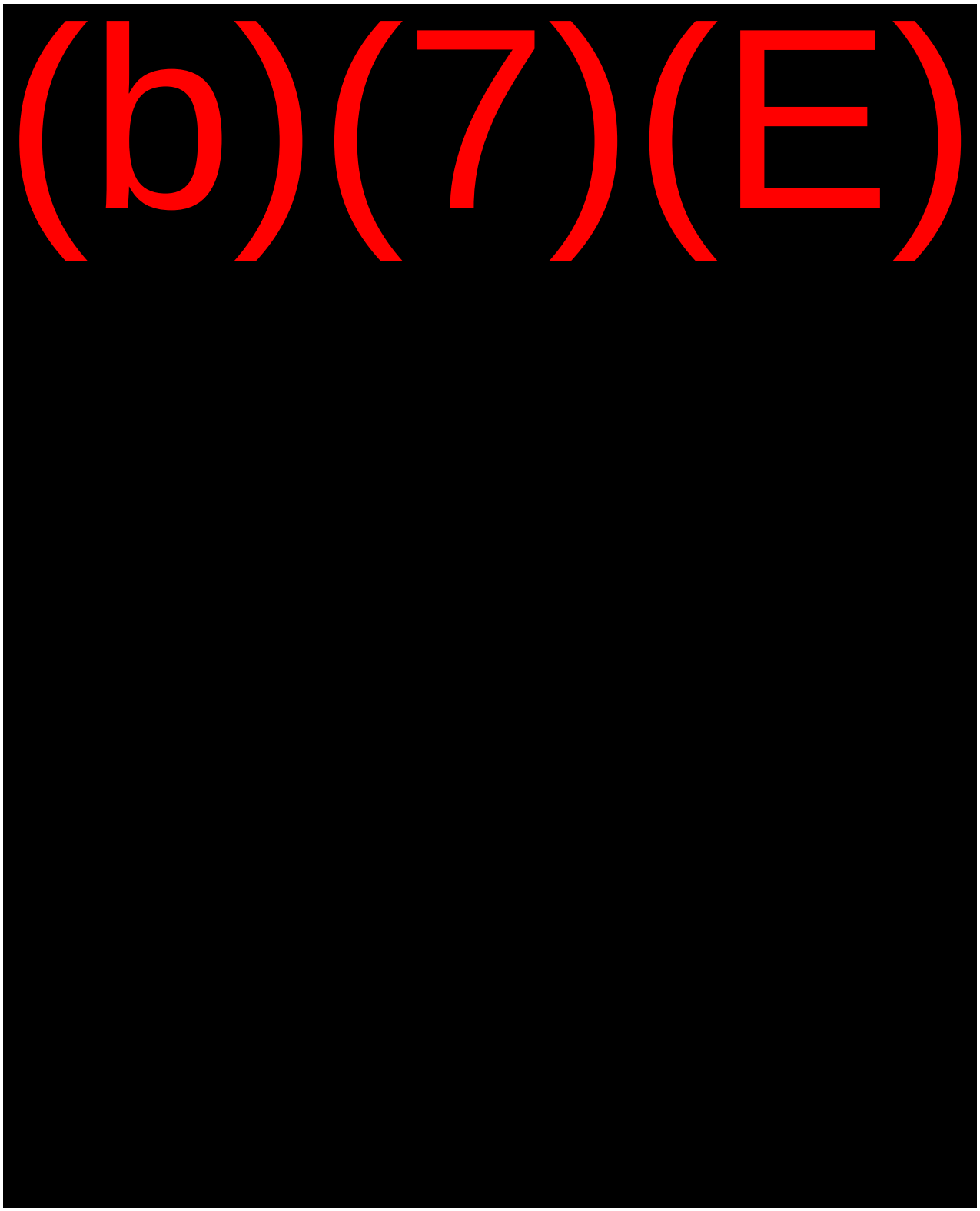

(b)(7)(E)

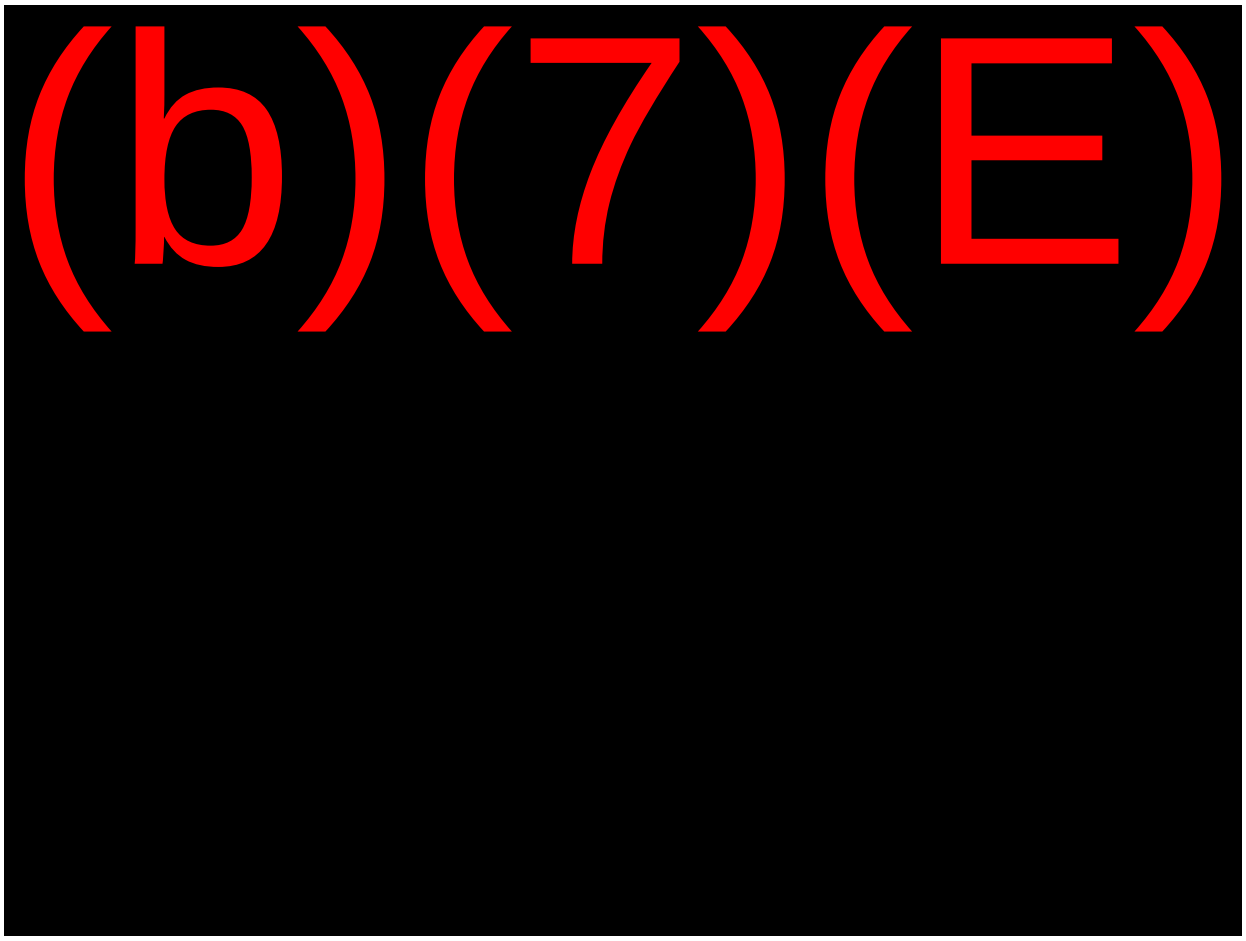

(b)(7)(E)

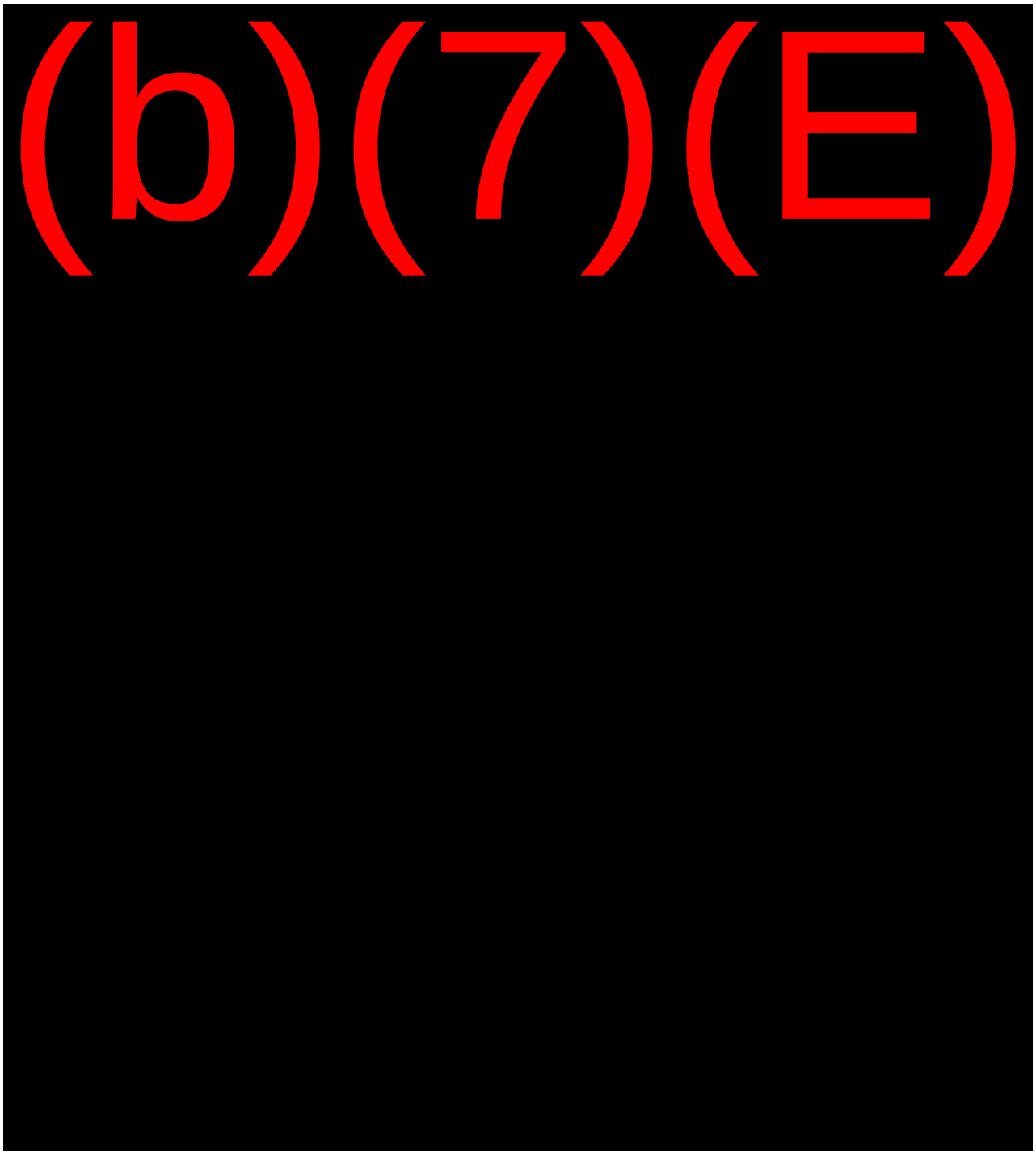

(b)(7)(E)


(b)(7)(E)

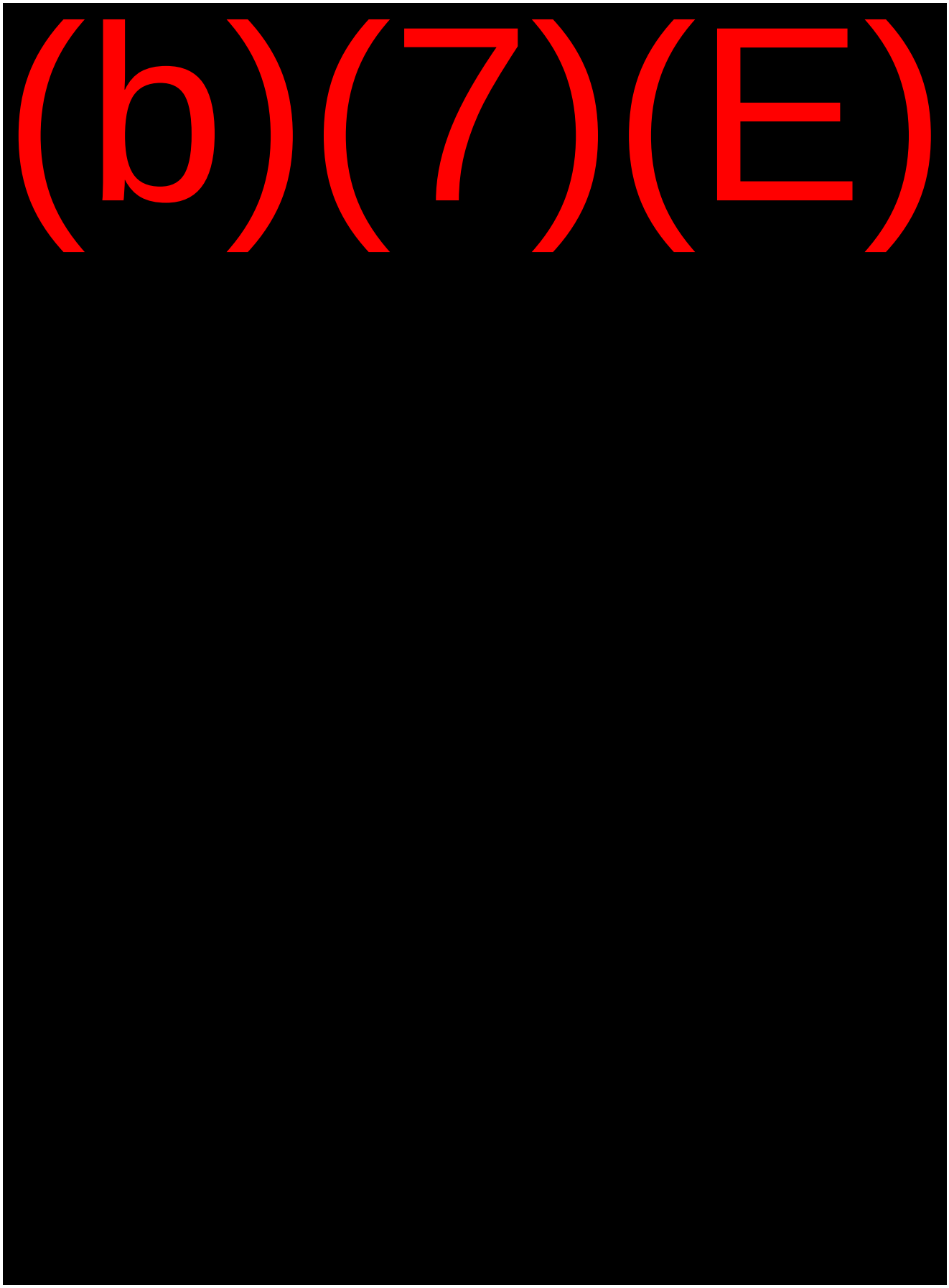

(b)(7)(E)

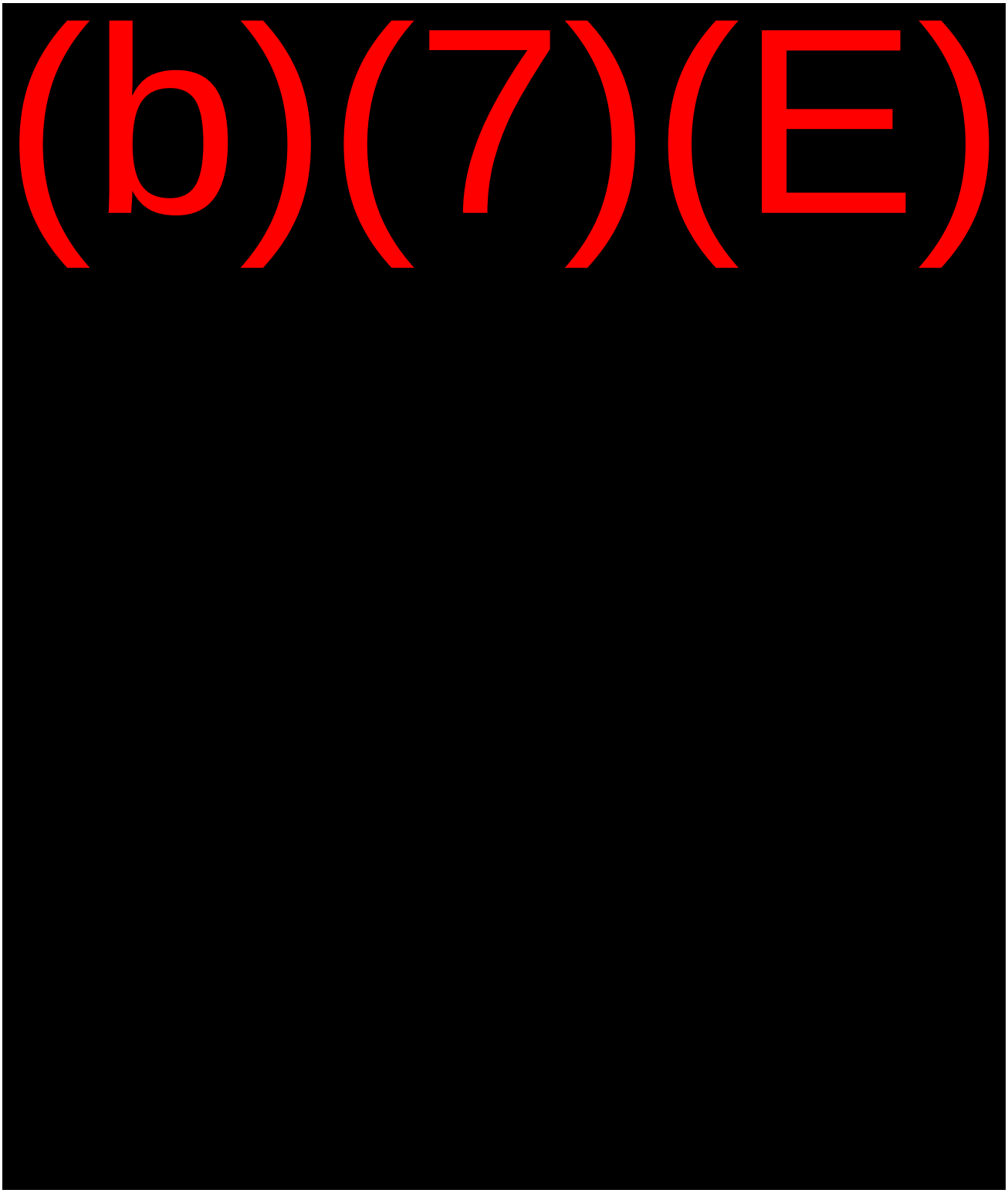

(b)(7)(E)


(b)(7)(E)

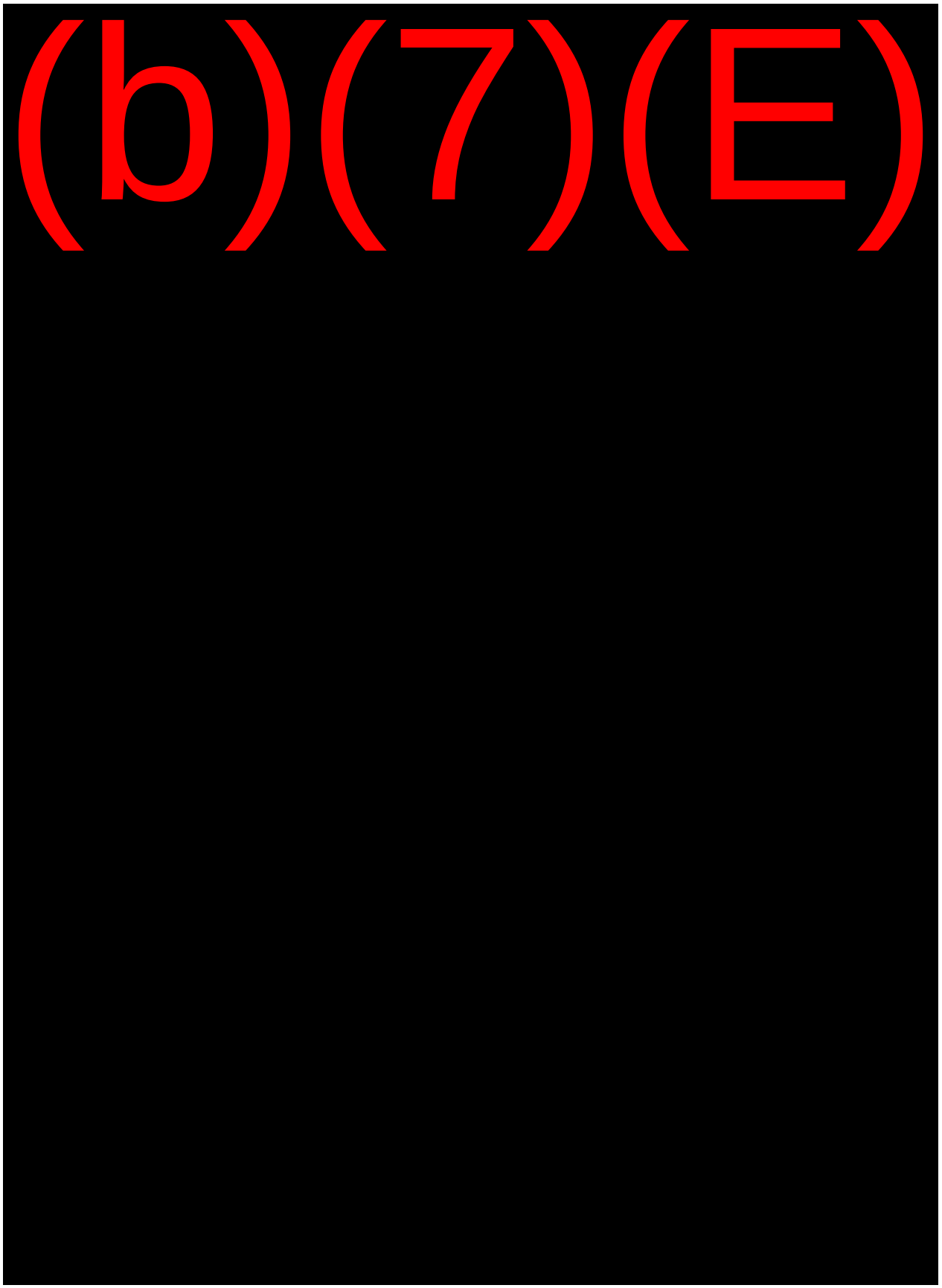

(b)(7)(E)

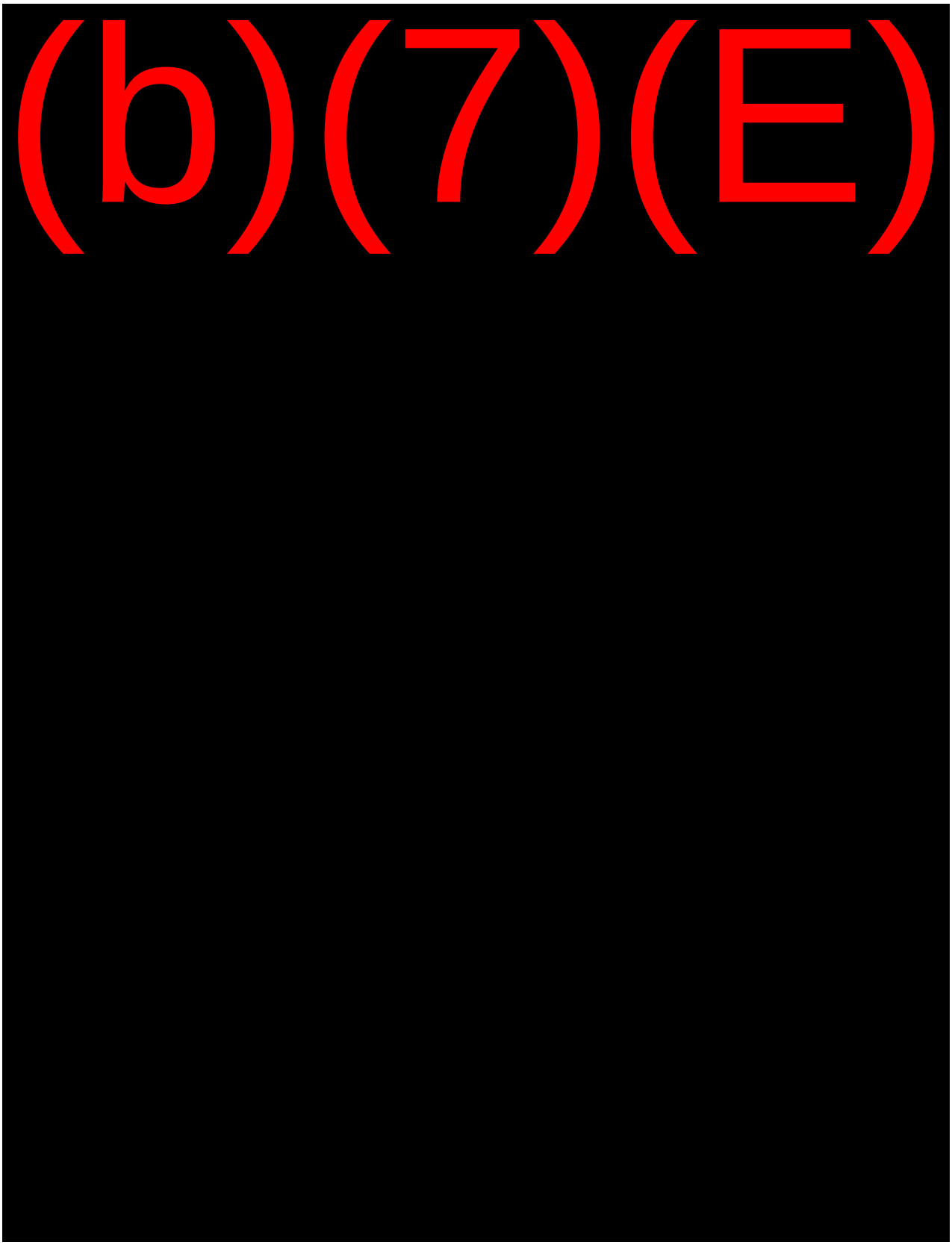

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

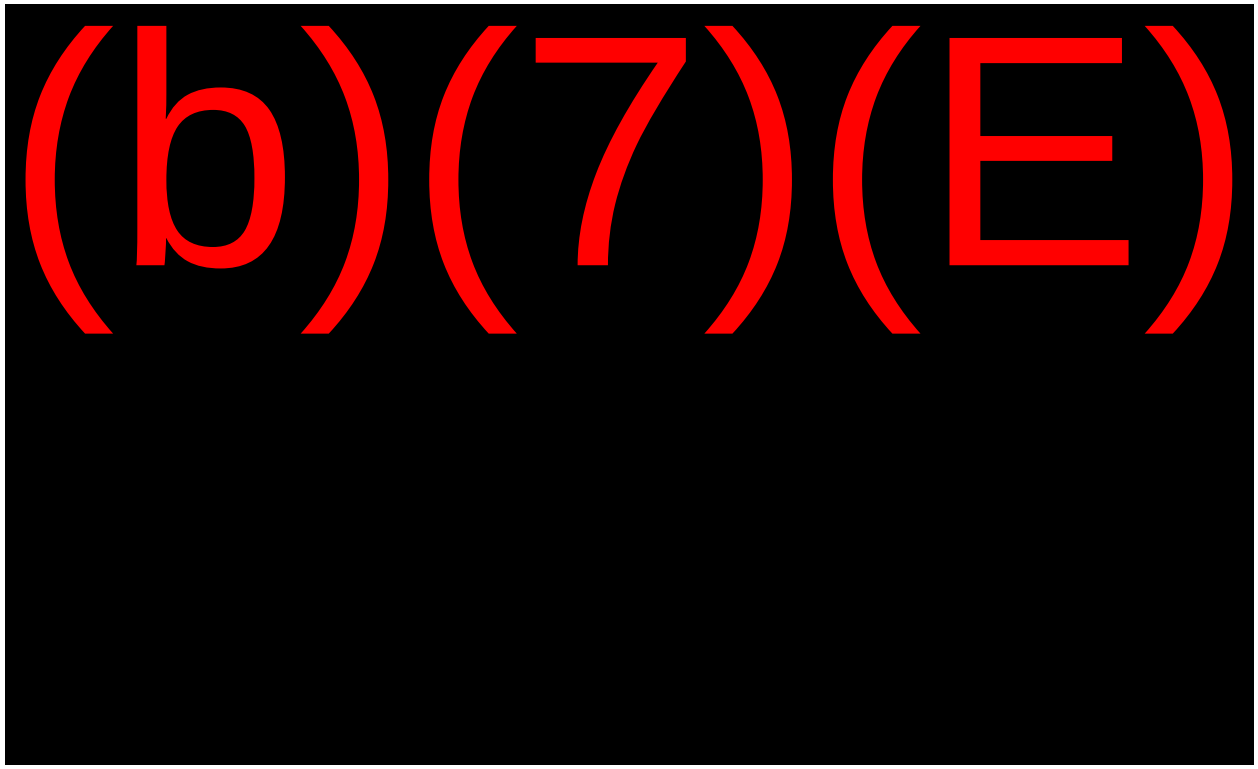

(b)(7)(E)

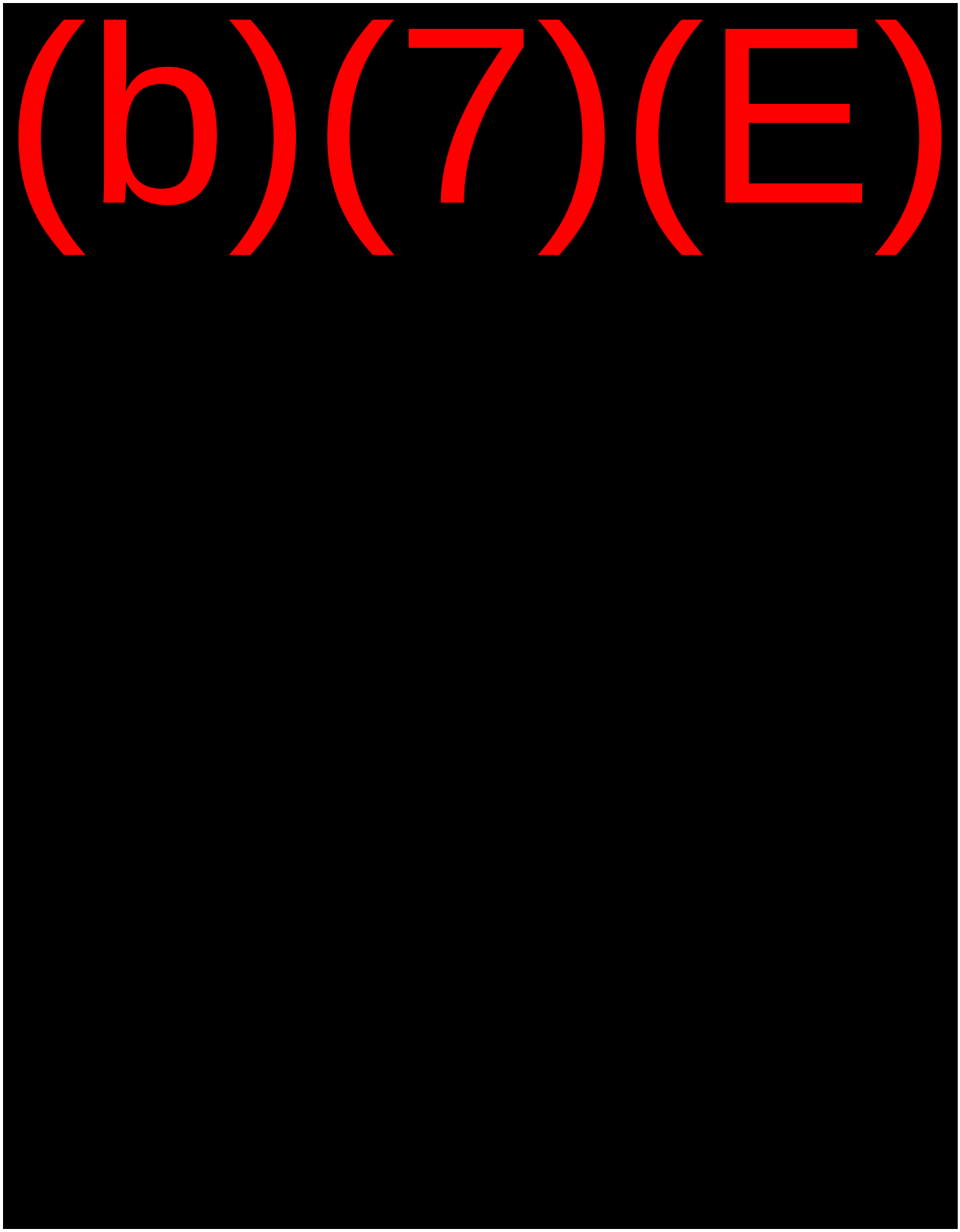

(b)(7)(E)

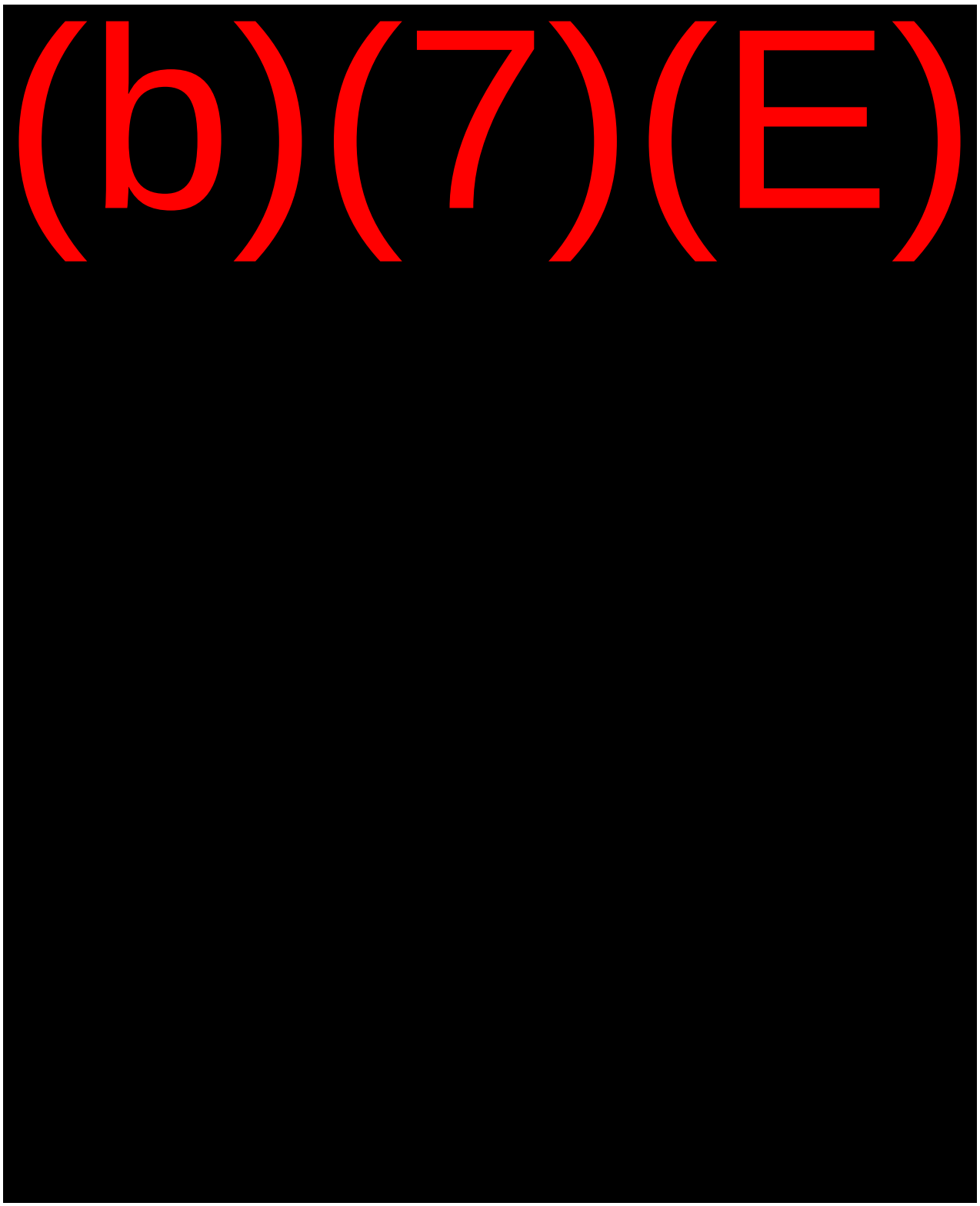

(b)(7)(E)

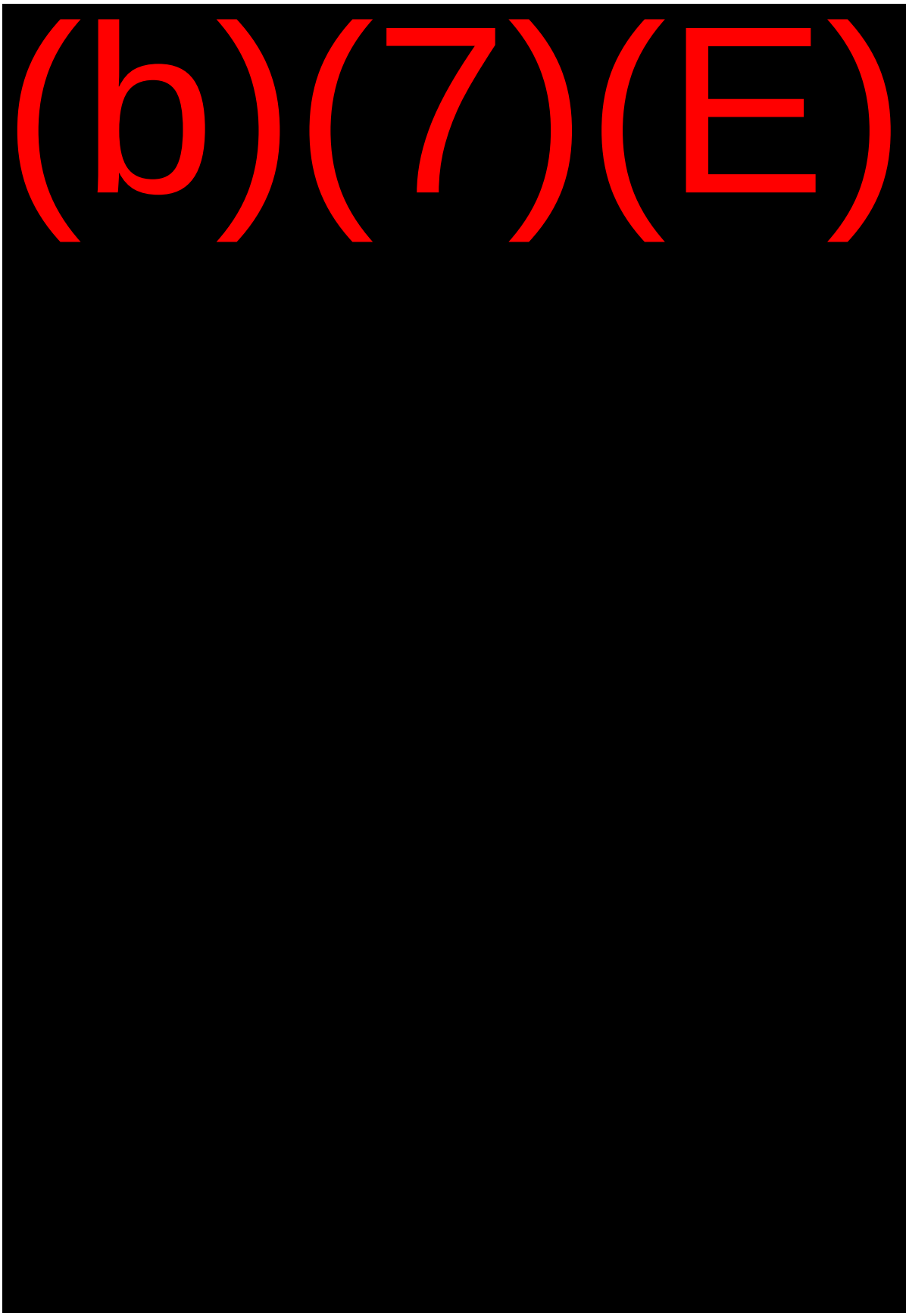

(b)(7)(E)

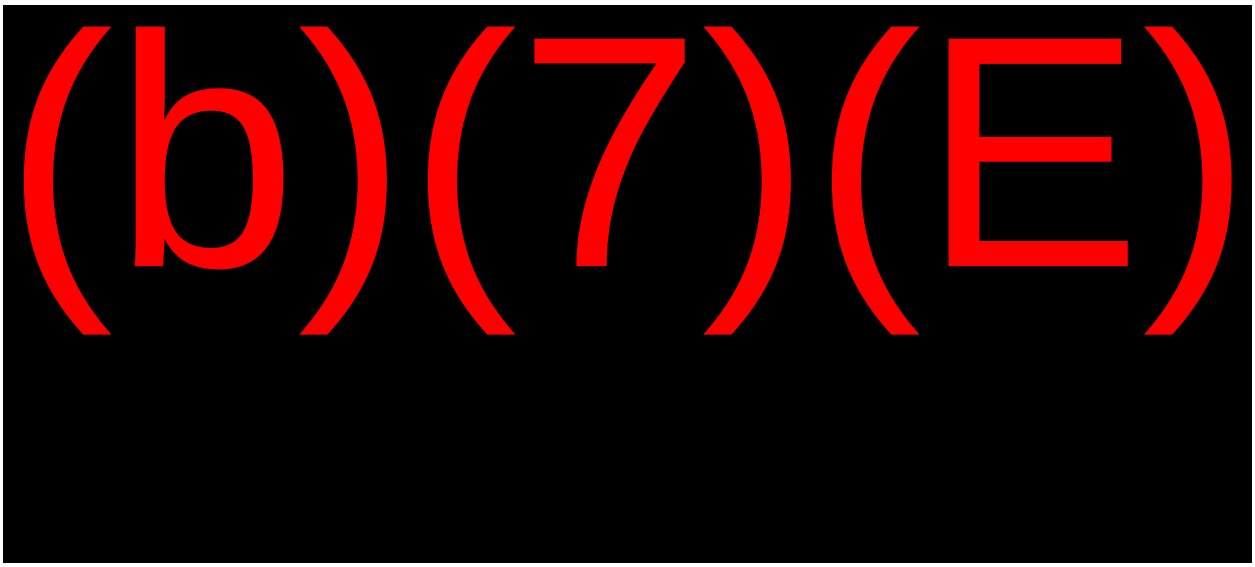

(b)(7)(E)

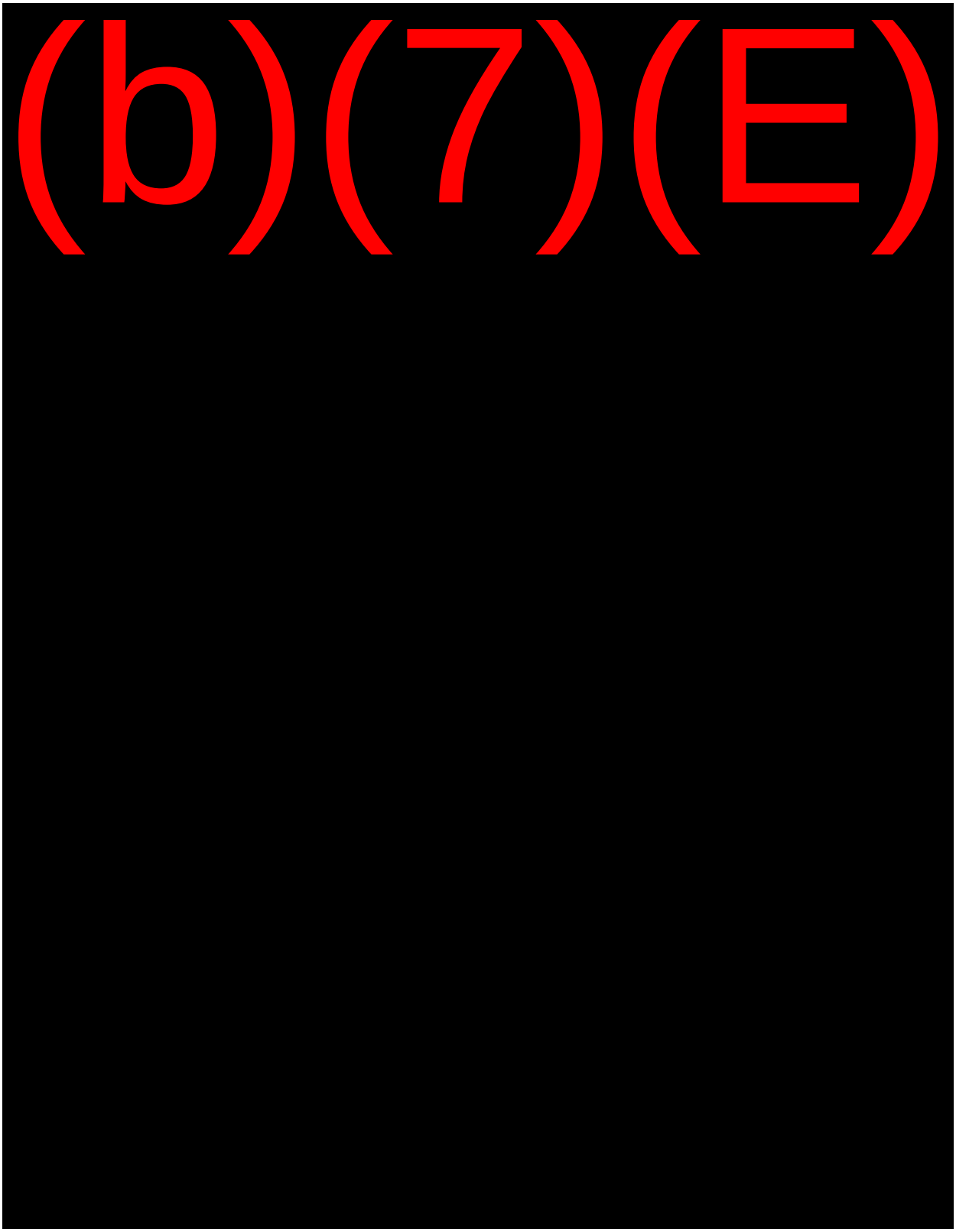

(b)(7)(E)

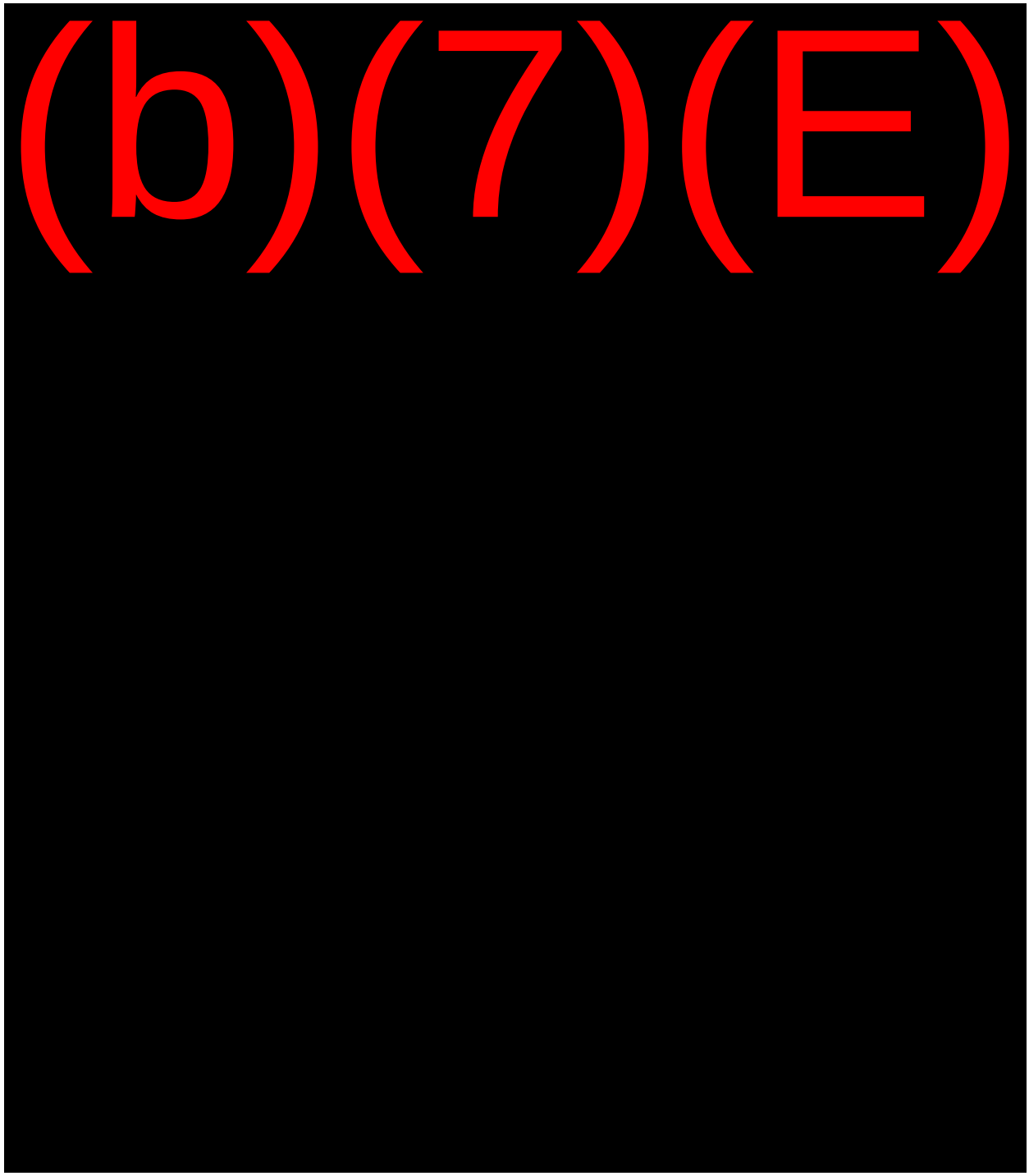

(b)(7)(E)

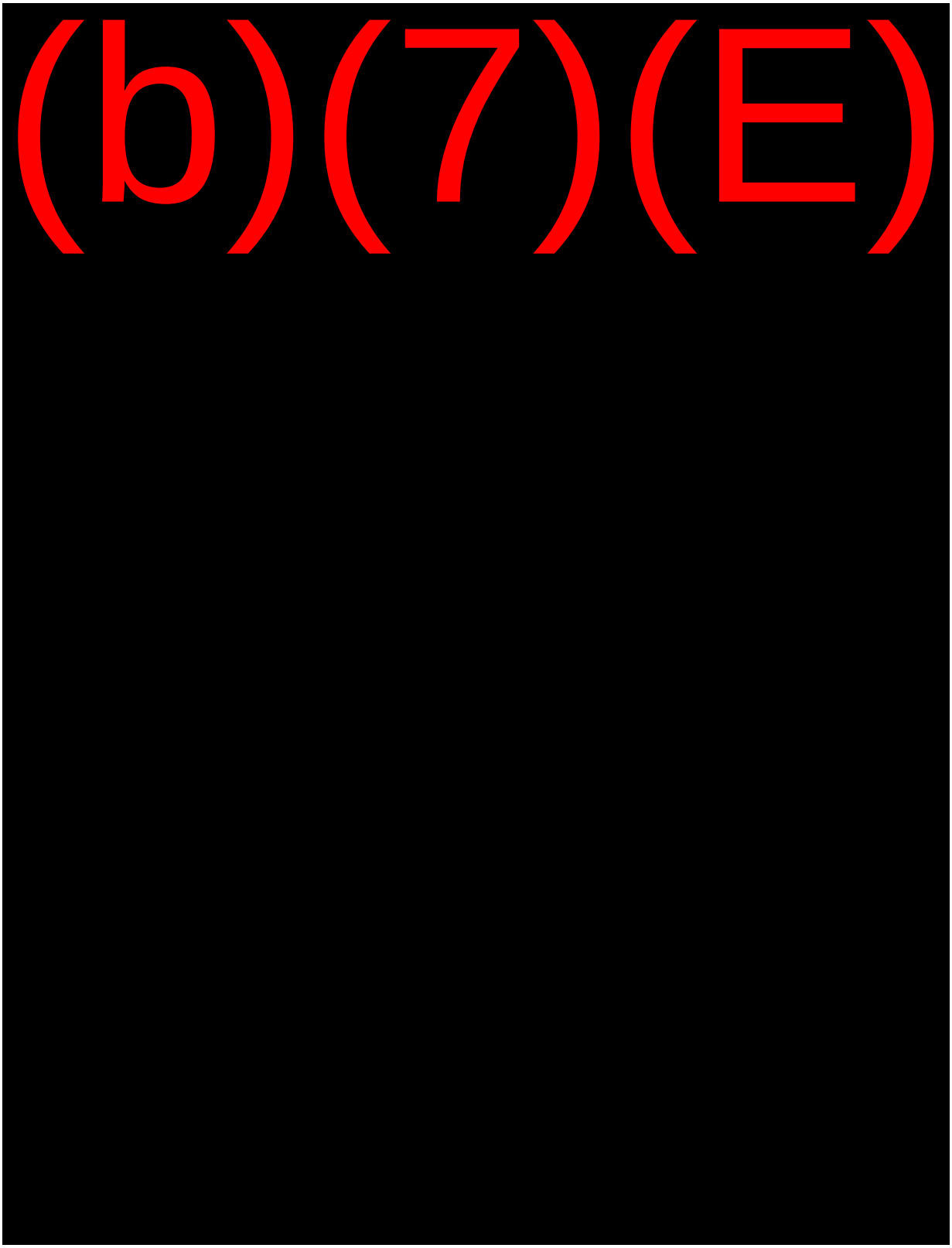

(b)(7)(E)

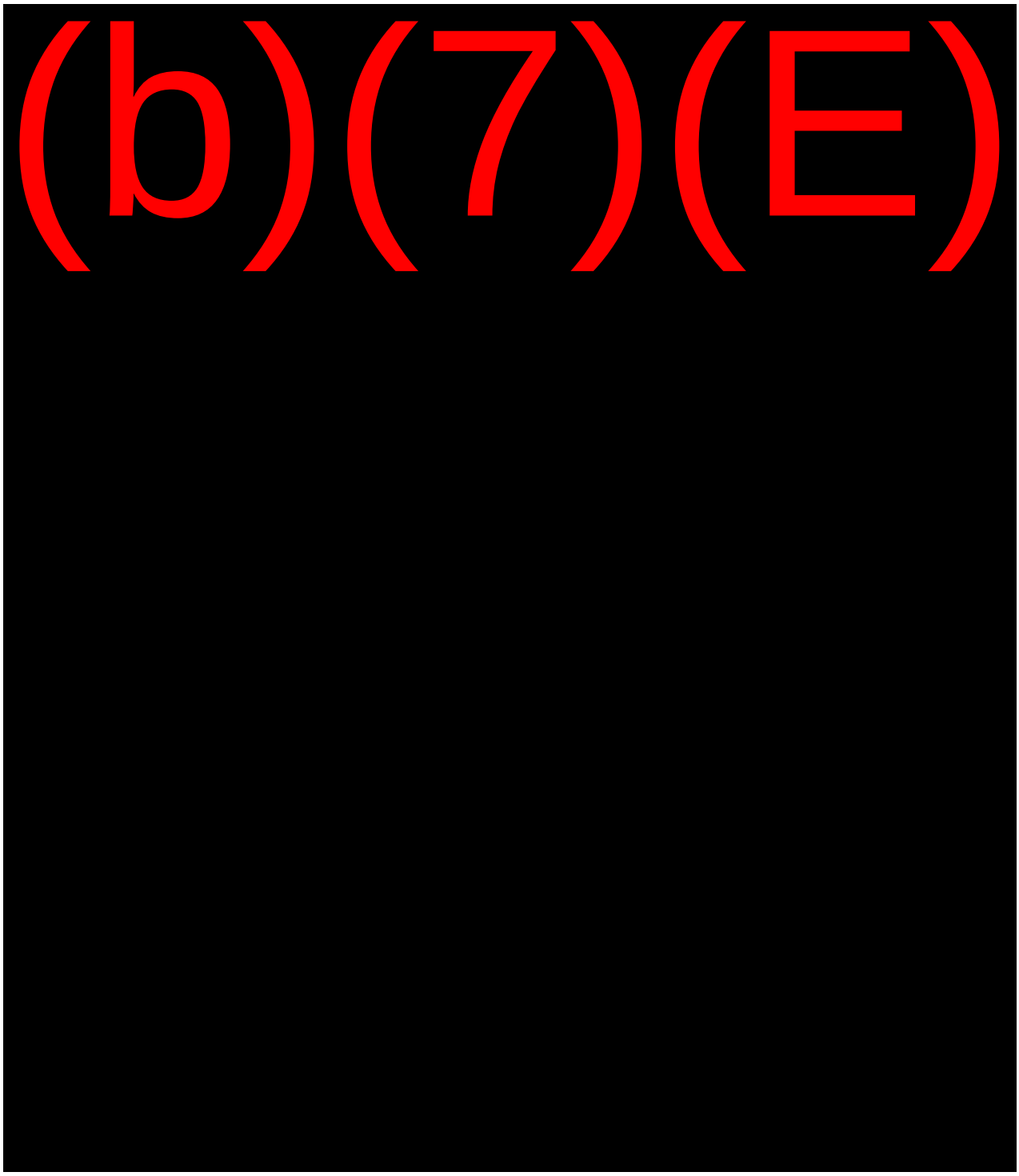

(b)(7)(E)

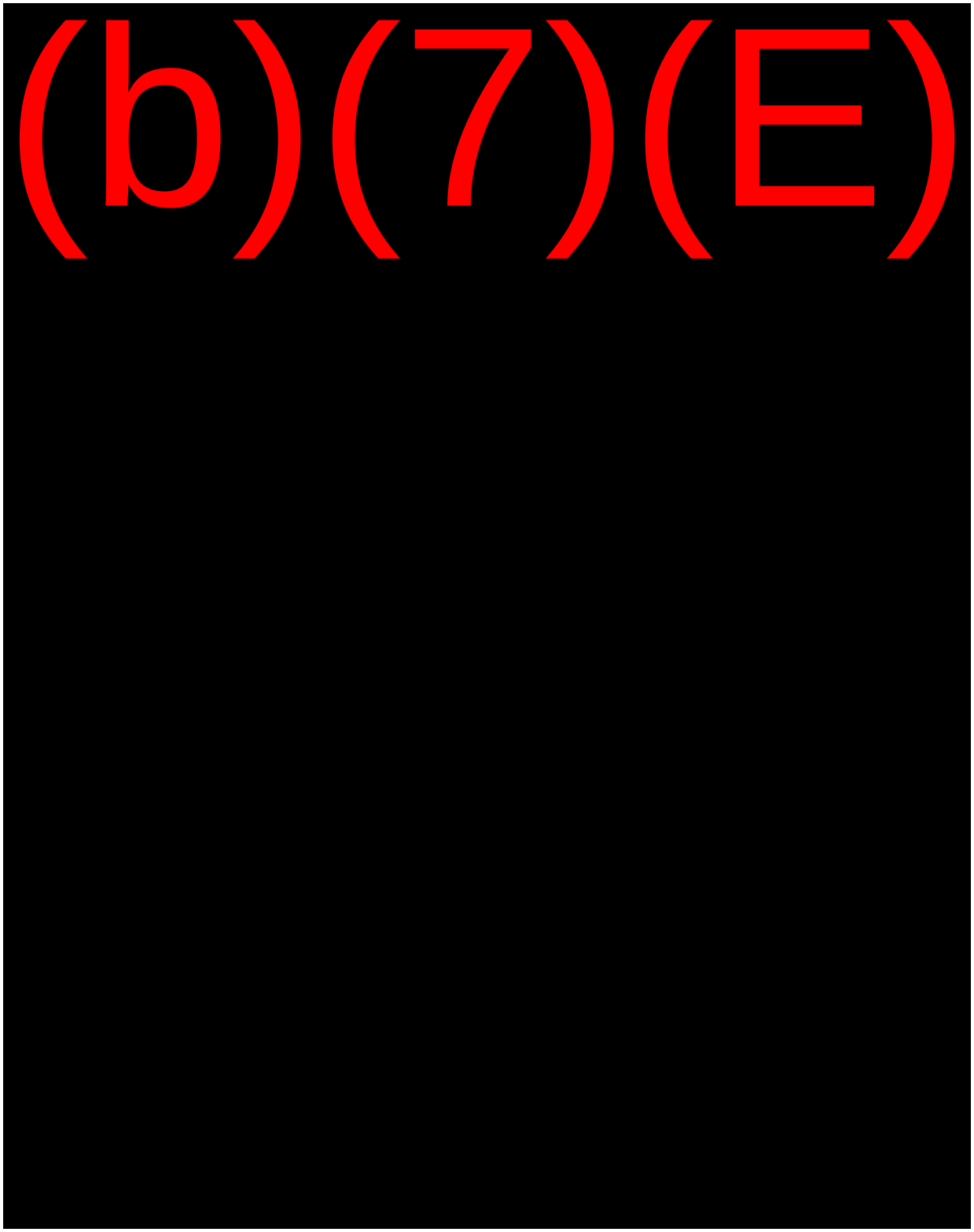

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)


(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

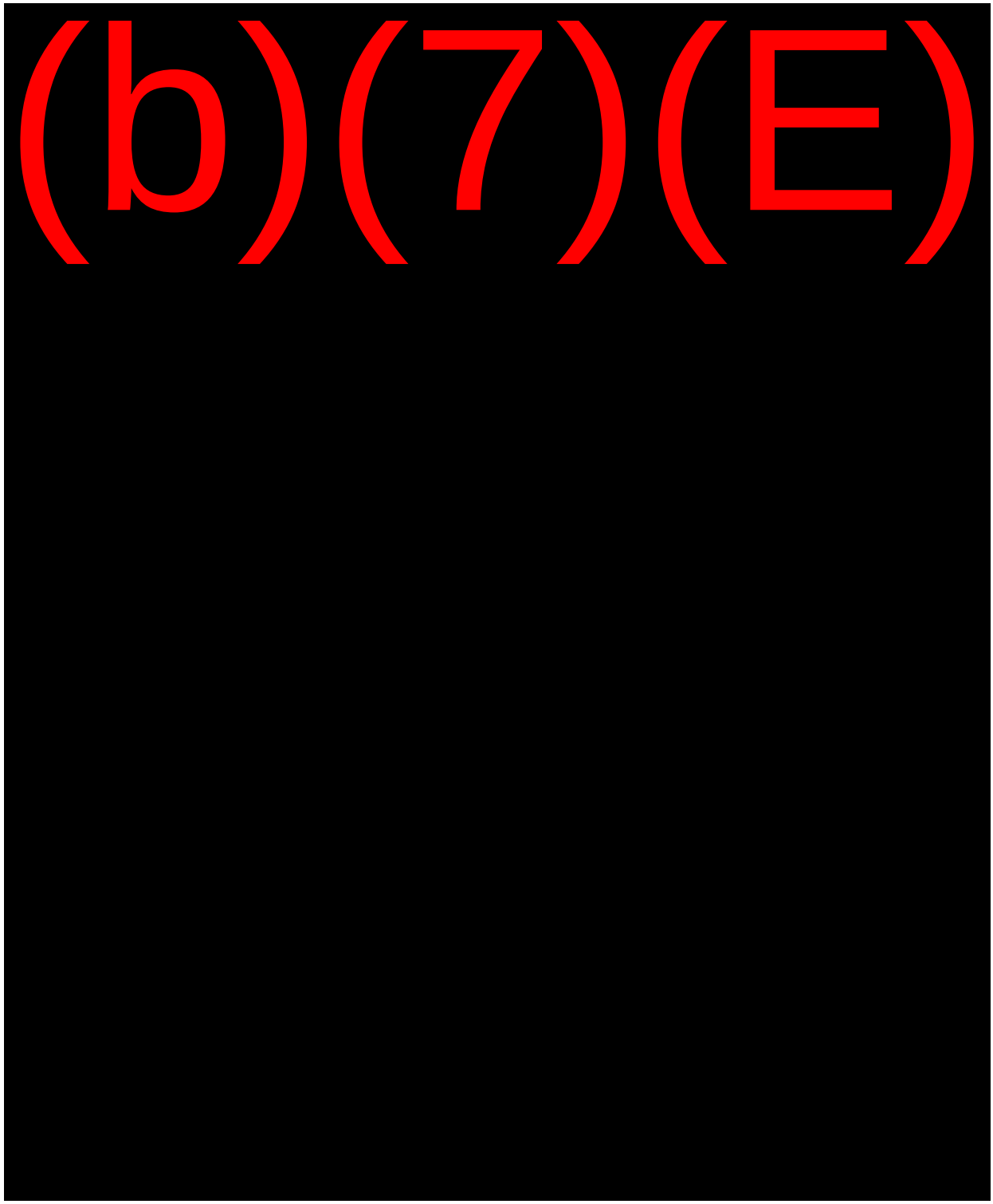

(b)(7)(E)

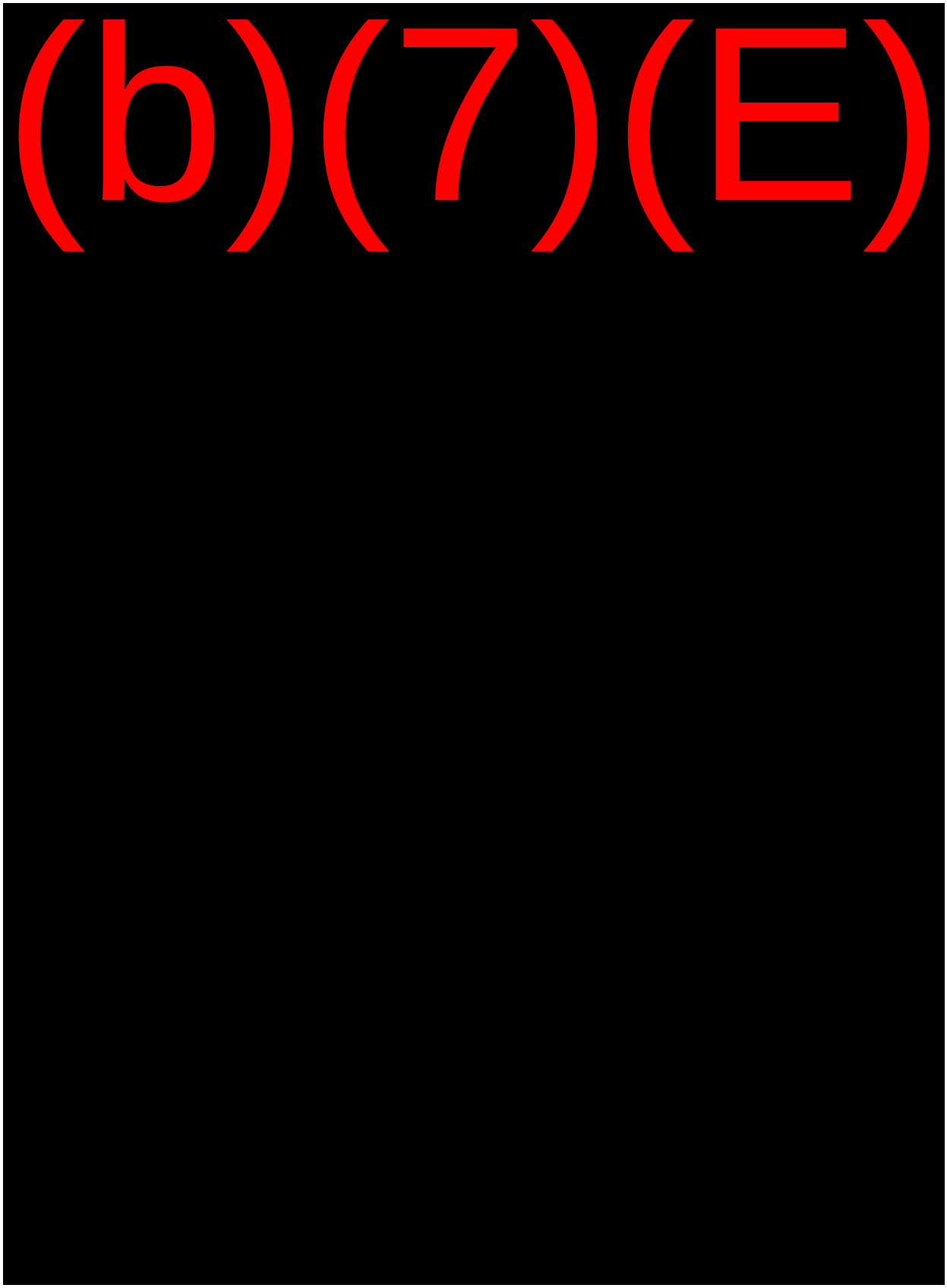

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

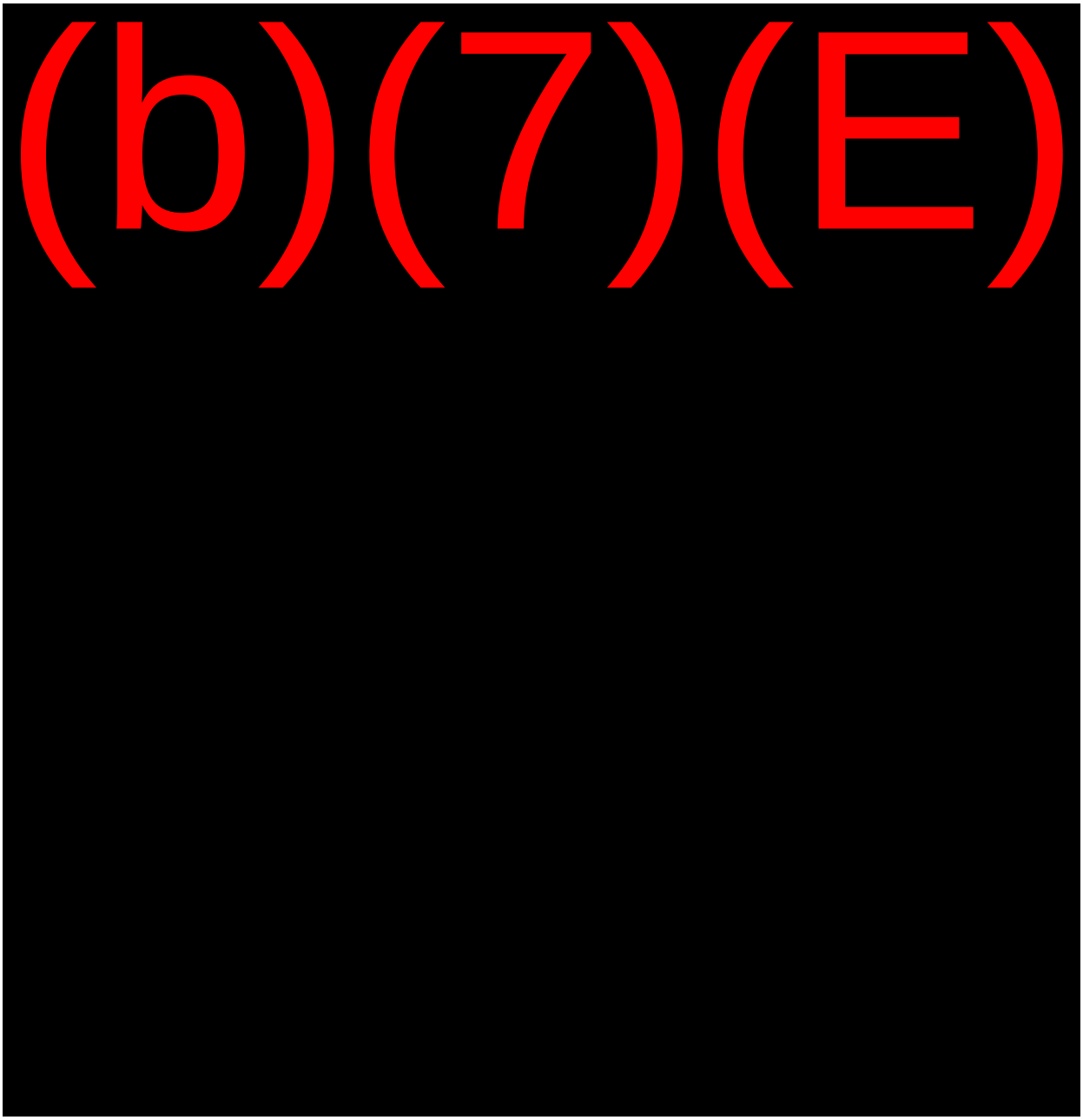

(b)(7)(E)

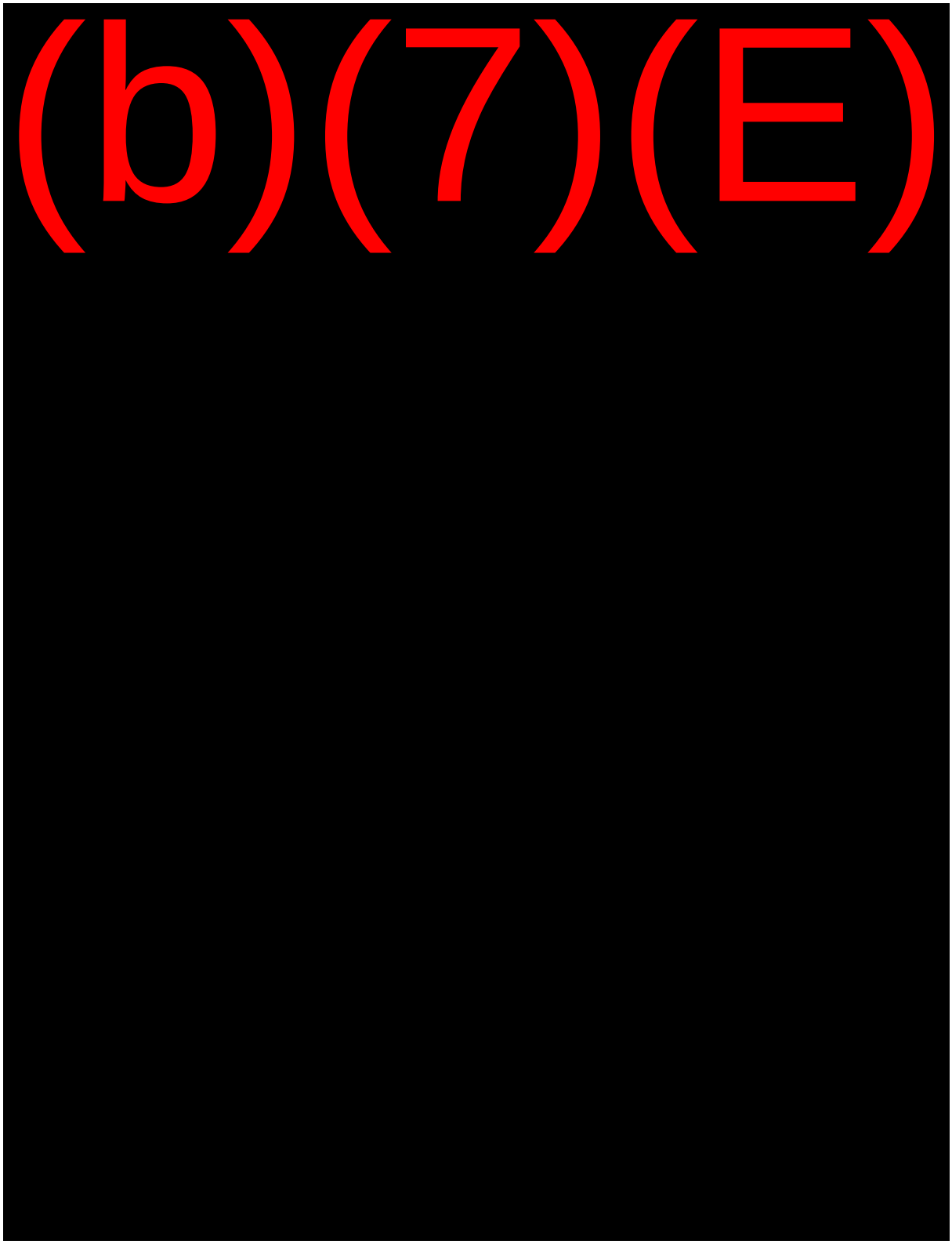

(b)(7)(E)


(b)(7)(E)

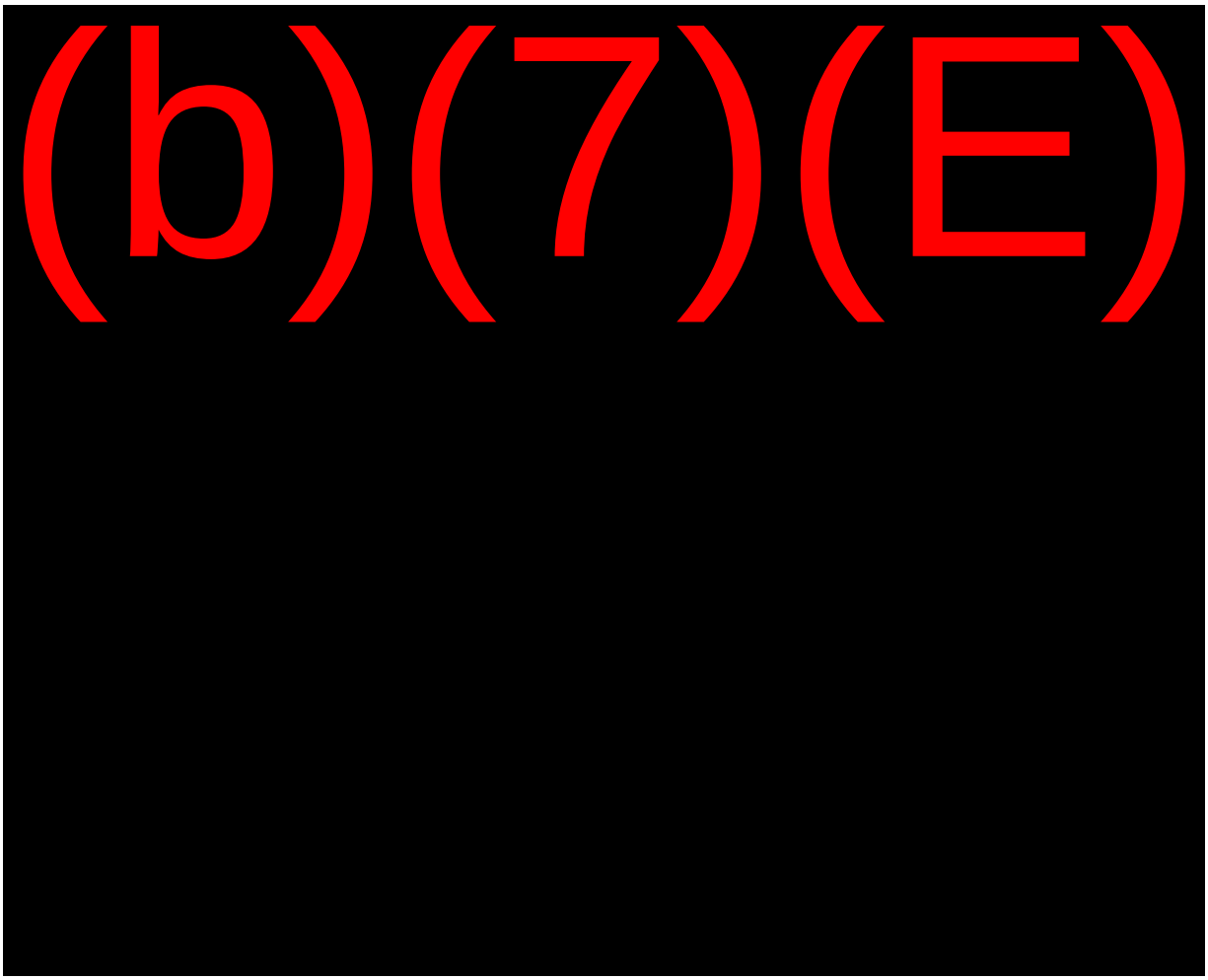

(b)(7)(E)

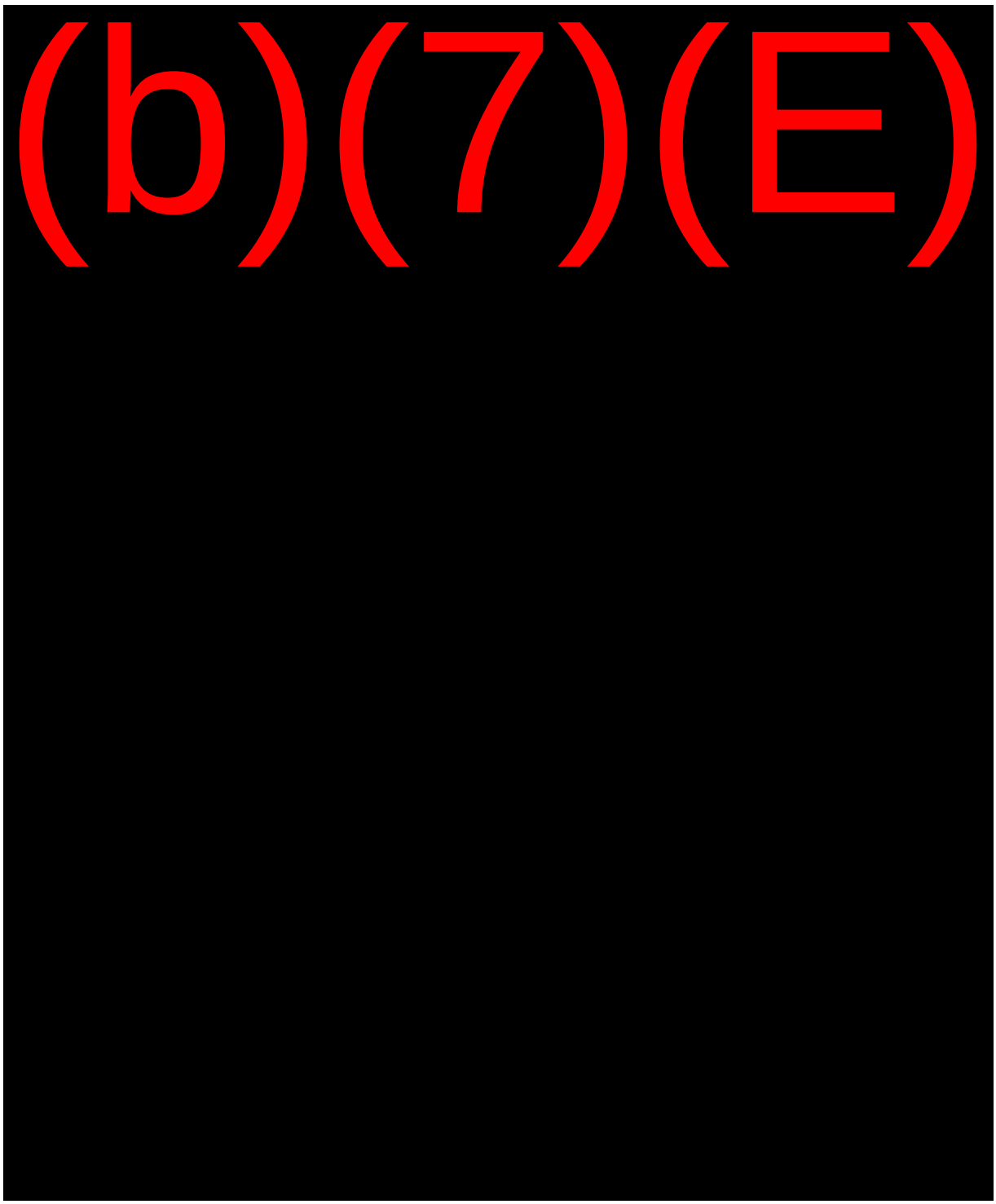

(b)(7)(E)


(b)(7)(E)

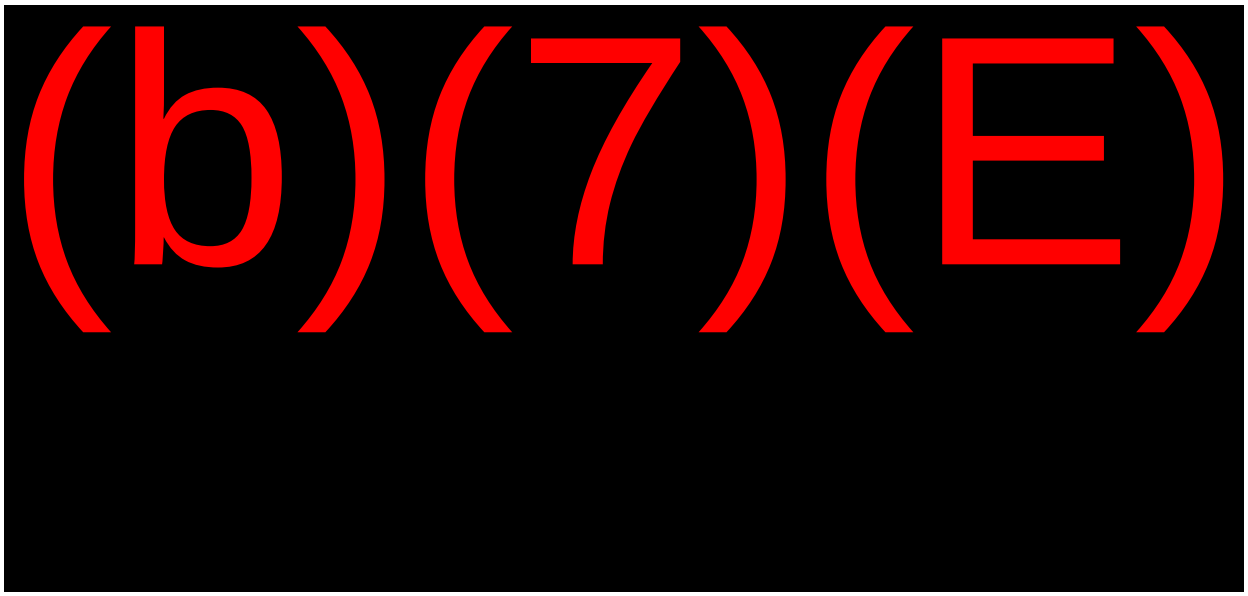

(b)(7)(E)

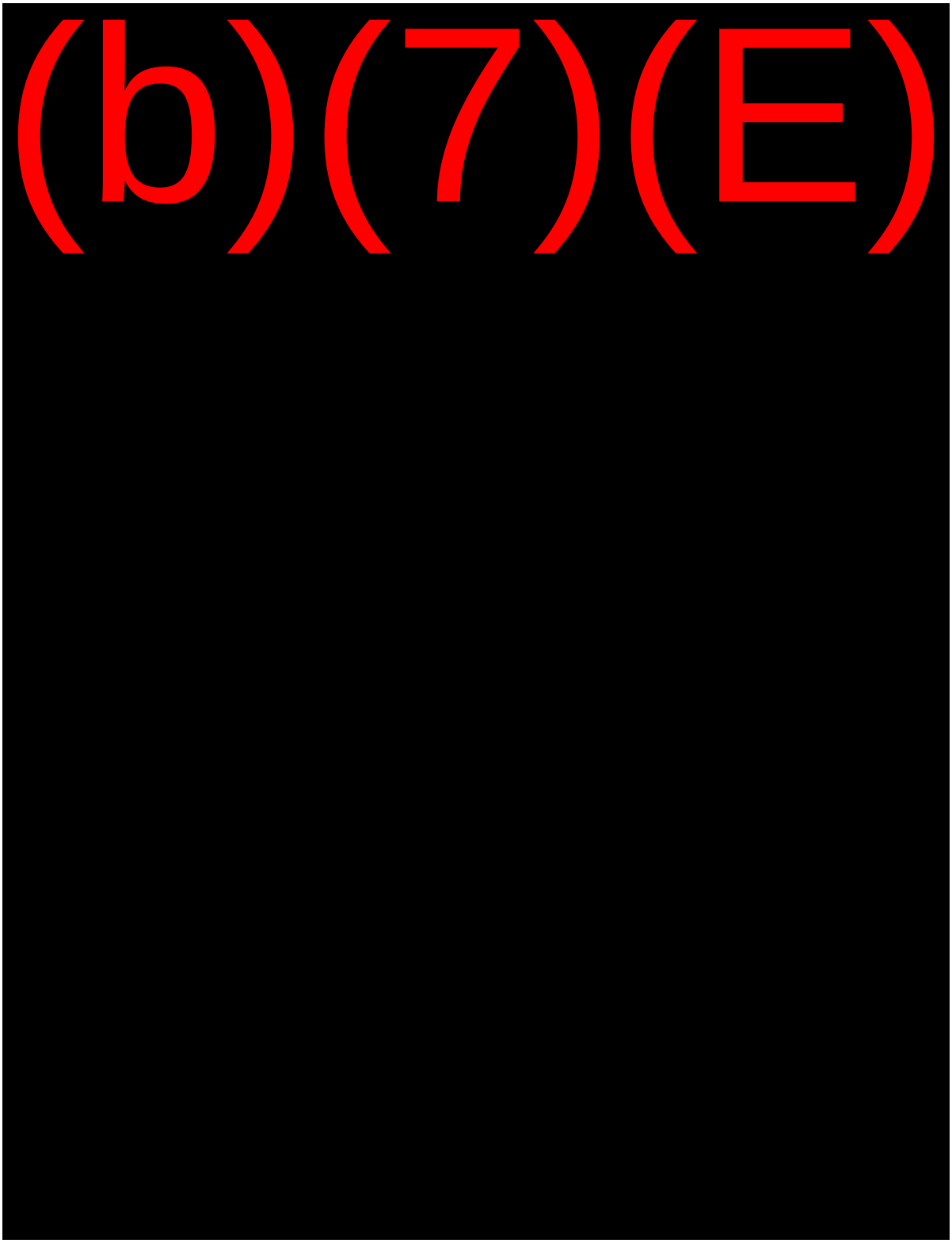

(b)(7)(E)

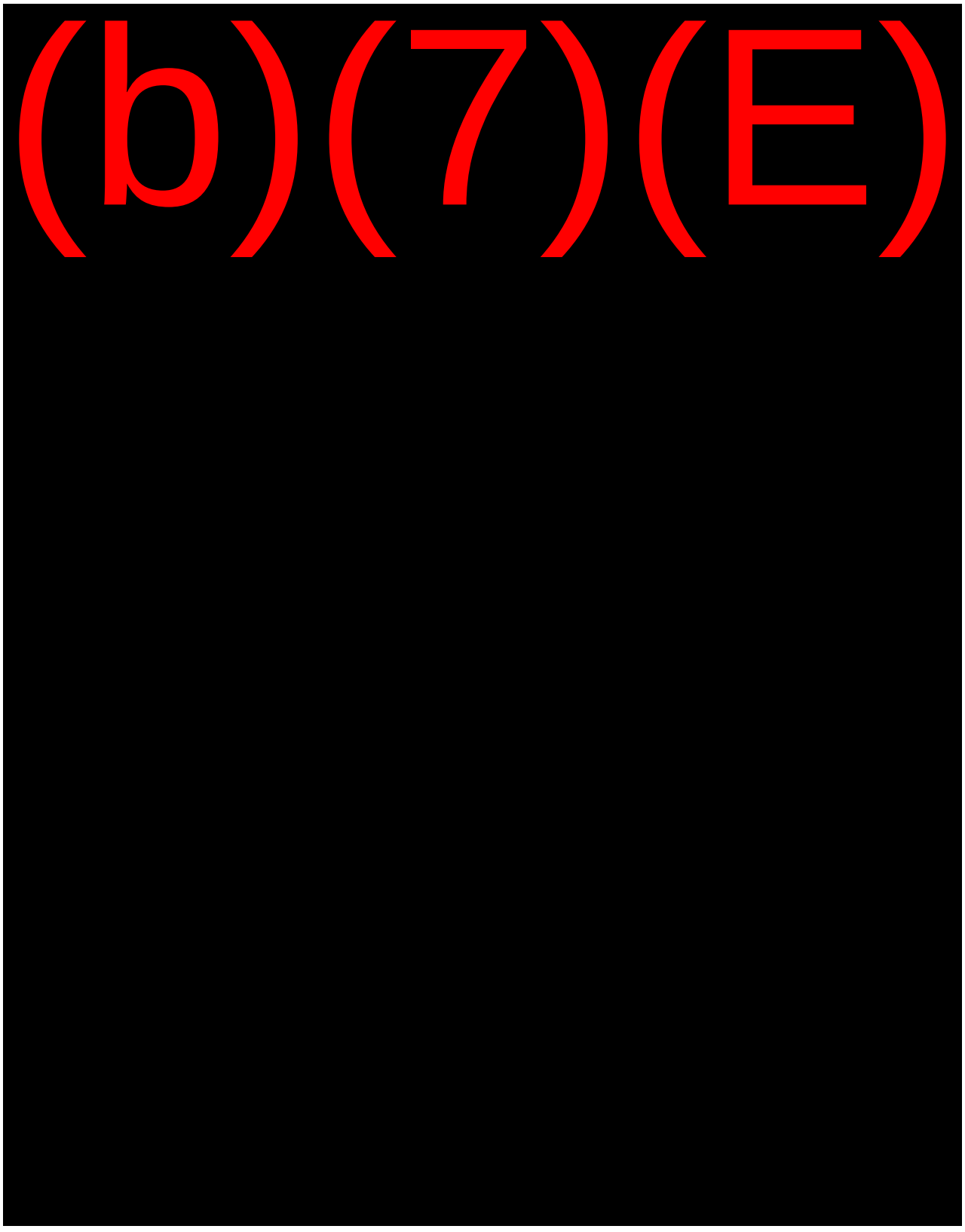

(b)(7)(E)

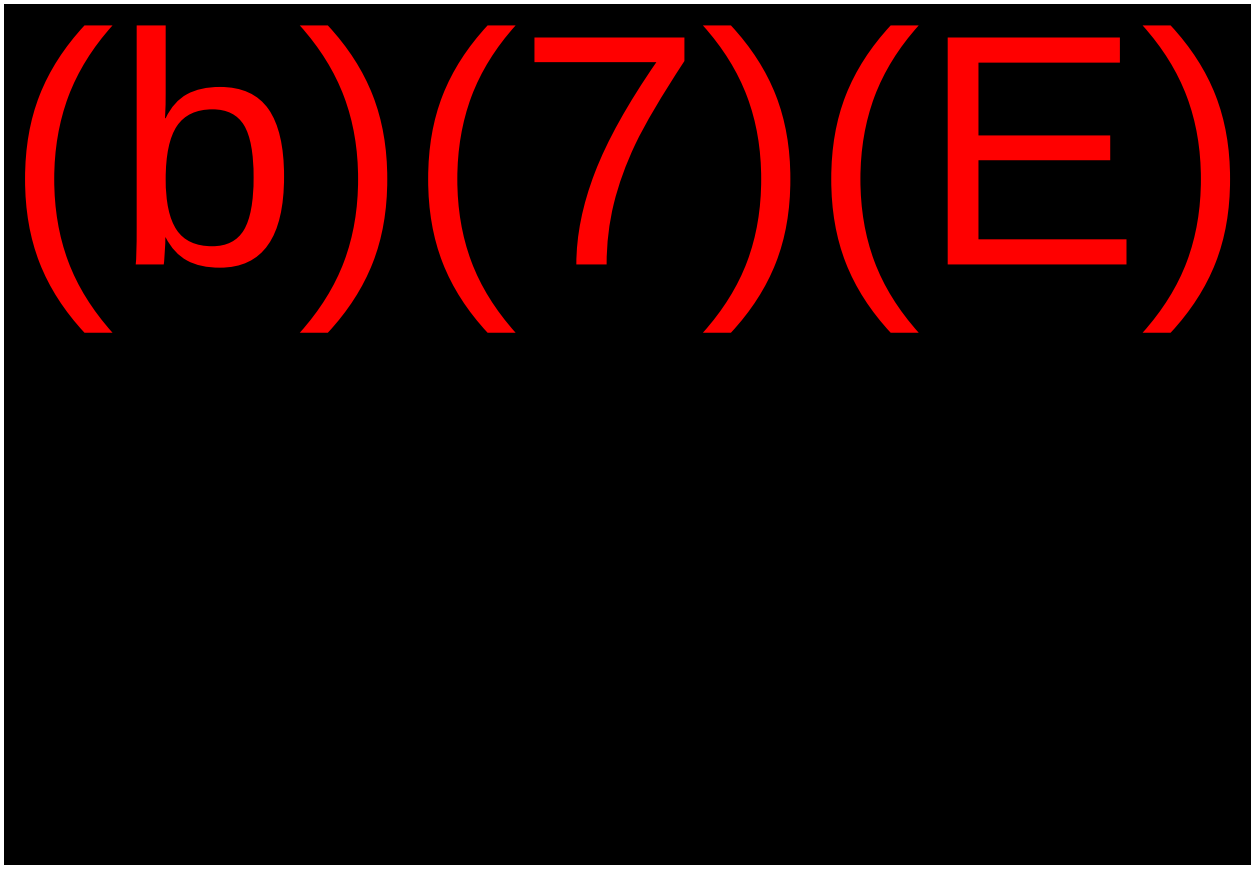

(b)(7)(E)

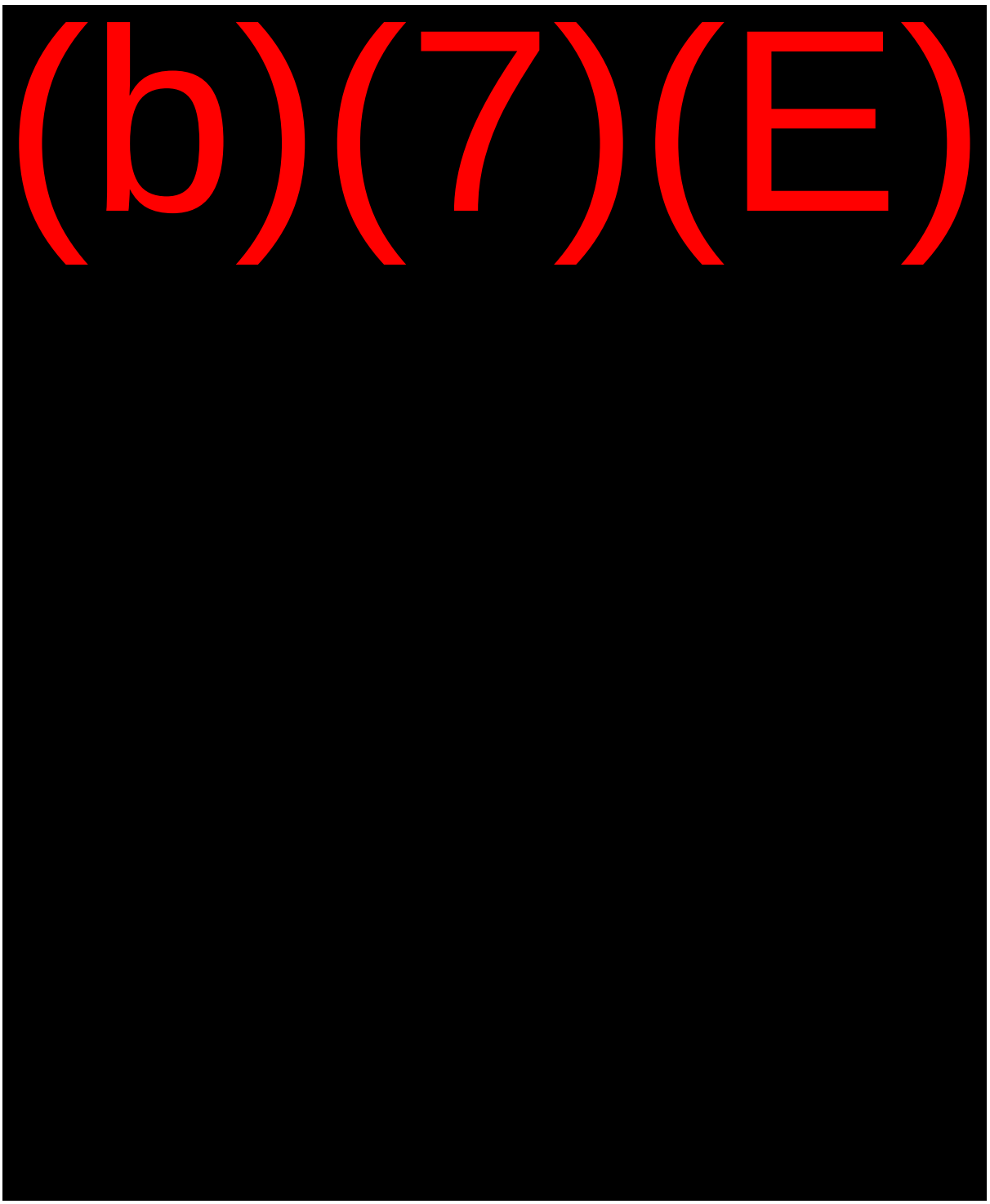

(b)(7)(E)

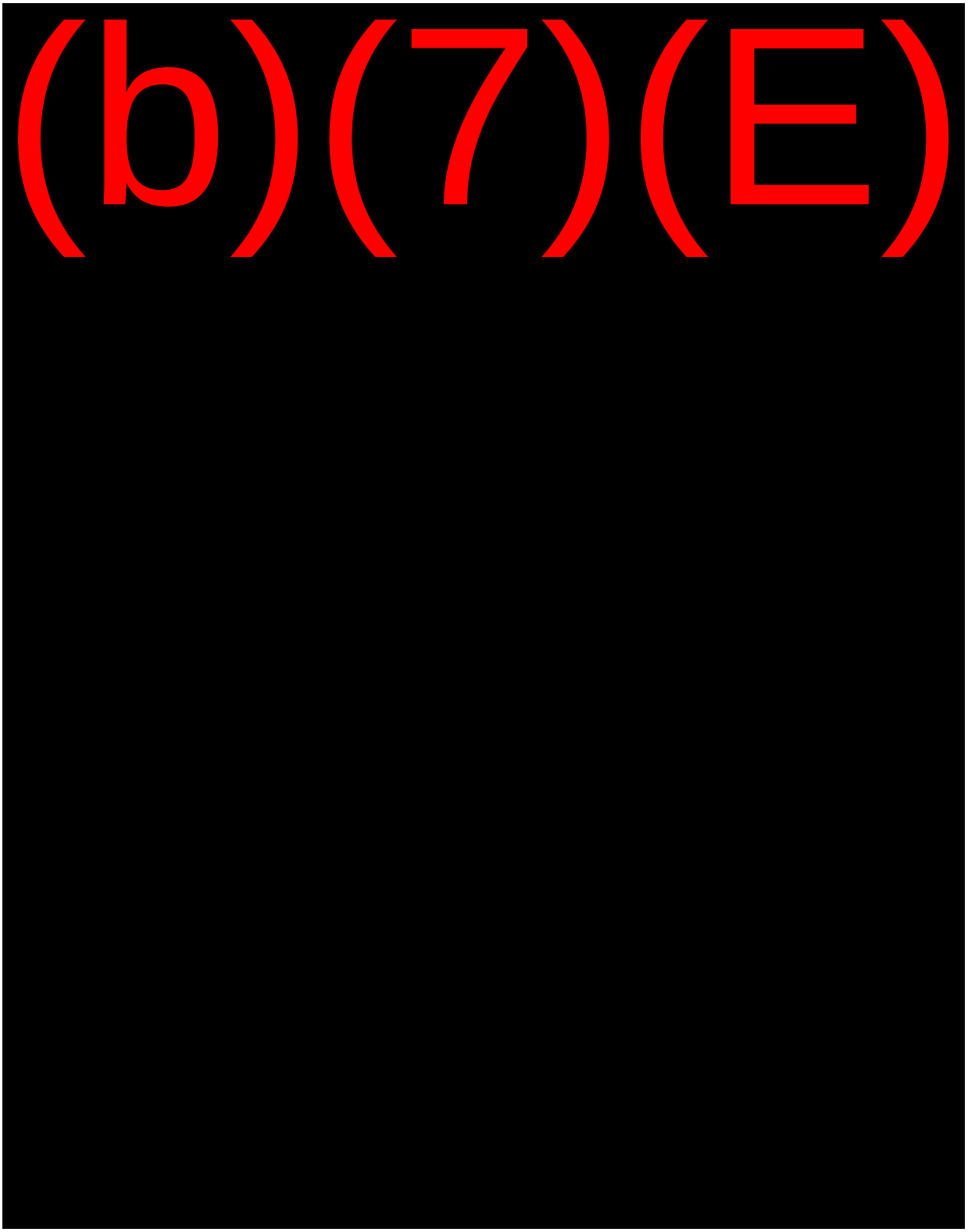

(b)(7)(E)


(b)(7)(E)

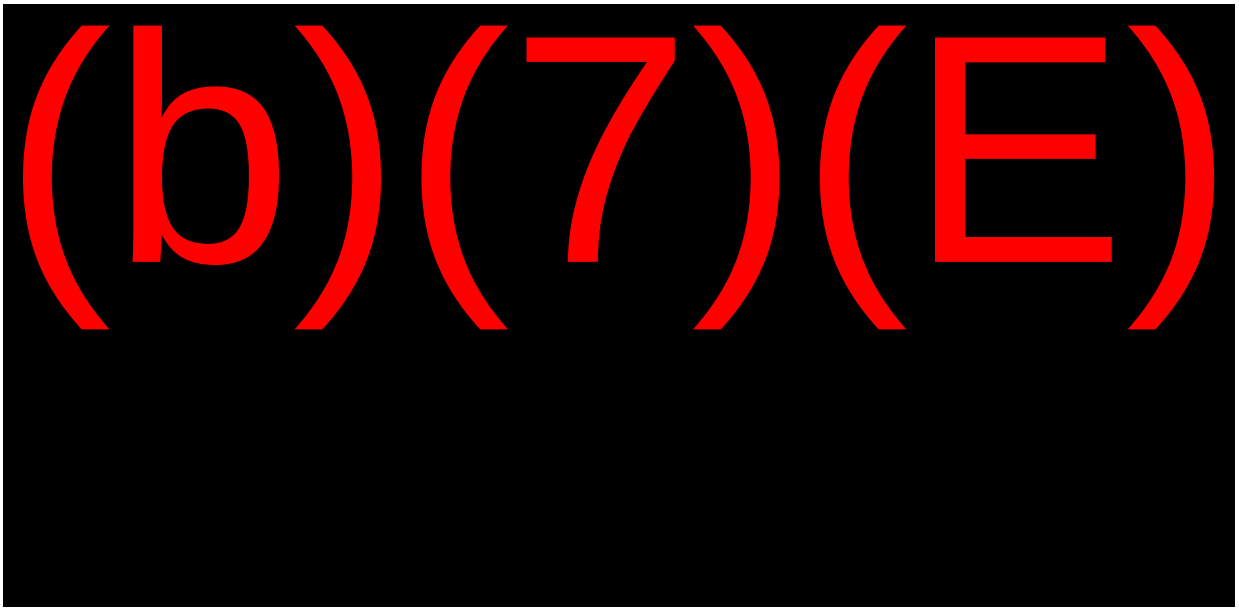

(b)(7)(E)

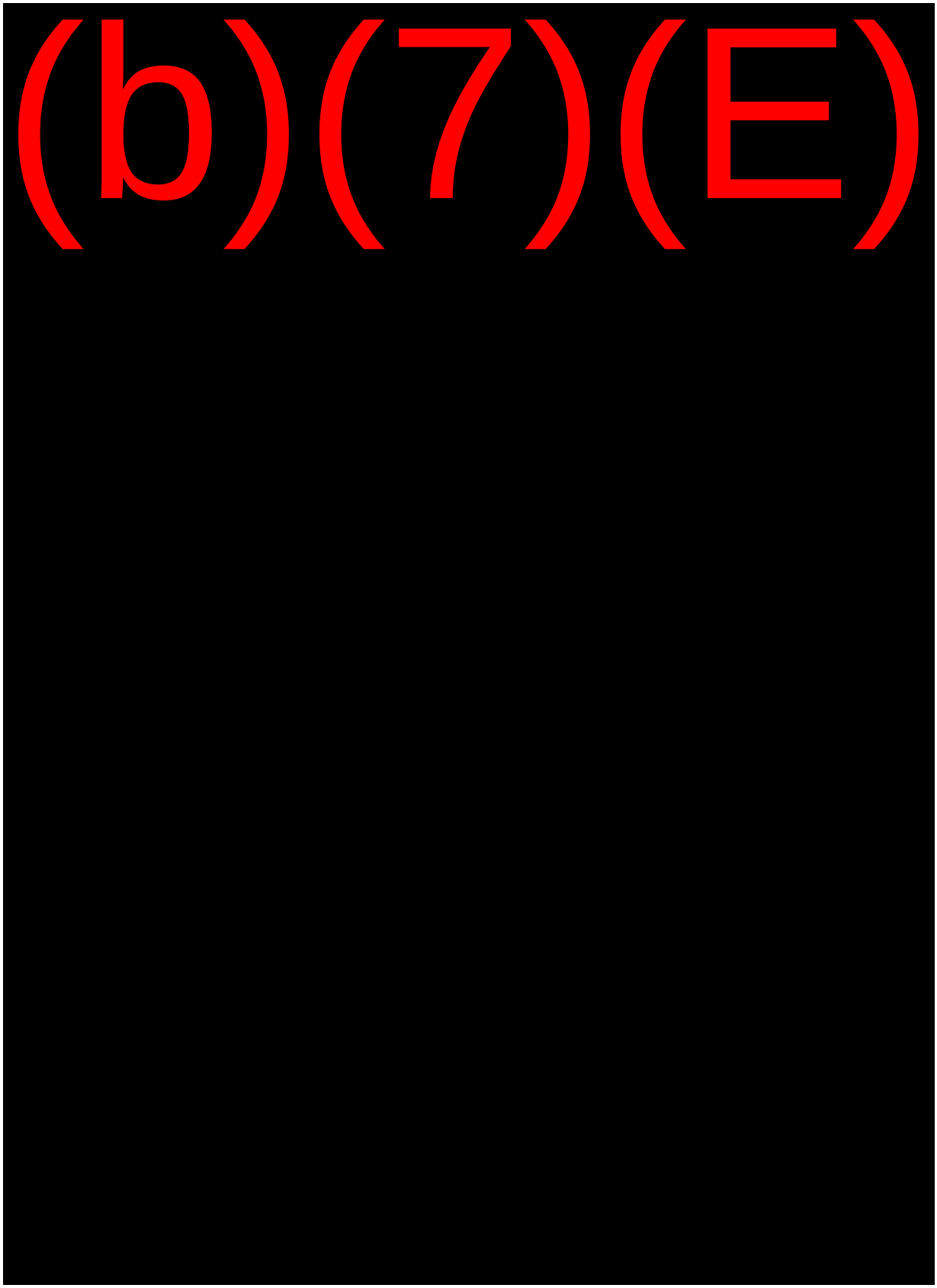

(b)(7)(E)


(b)(7)(E)

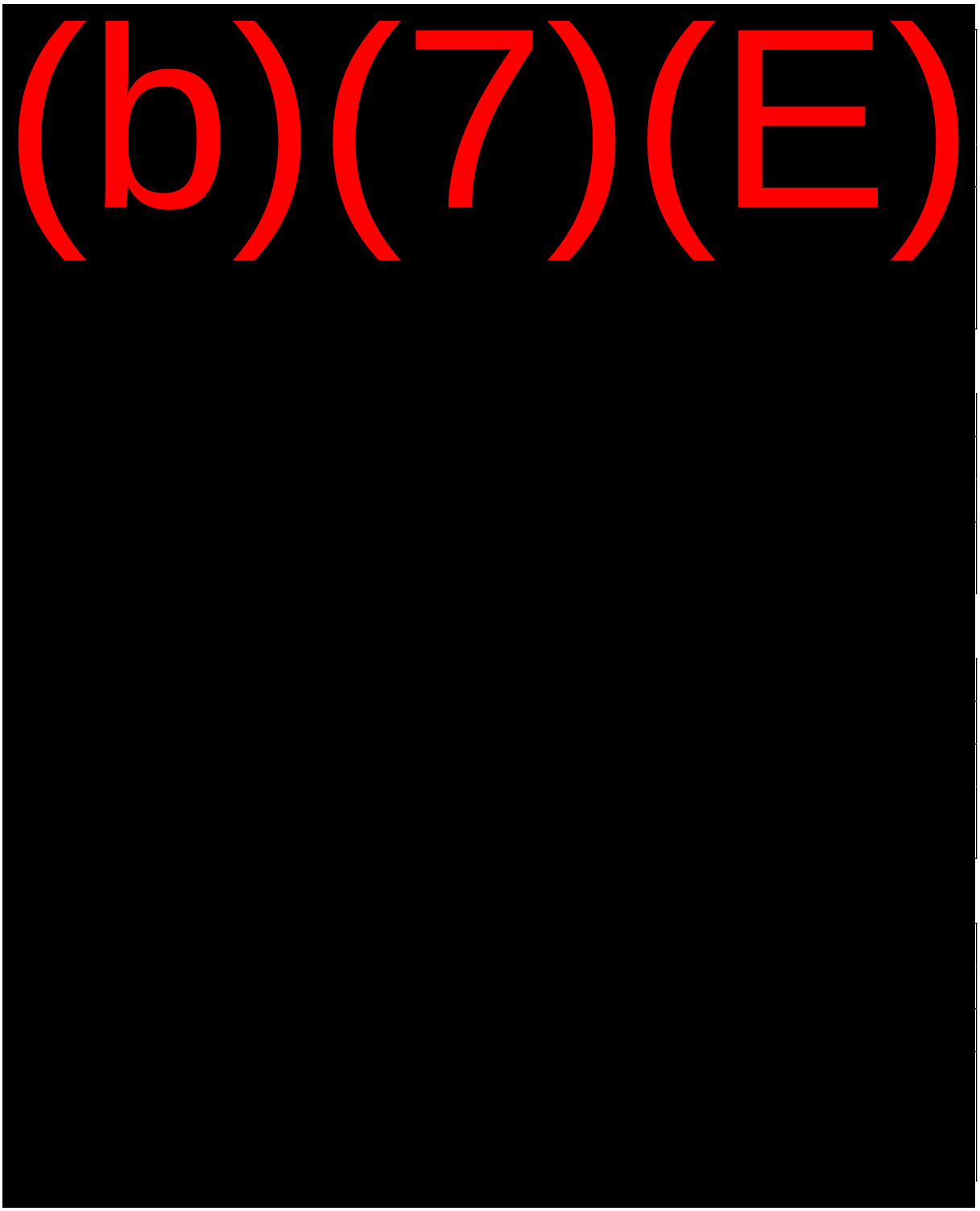

(b)(7)(E)


(b)(7)(E)


(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

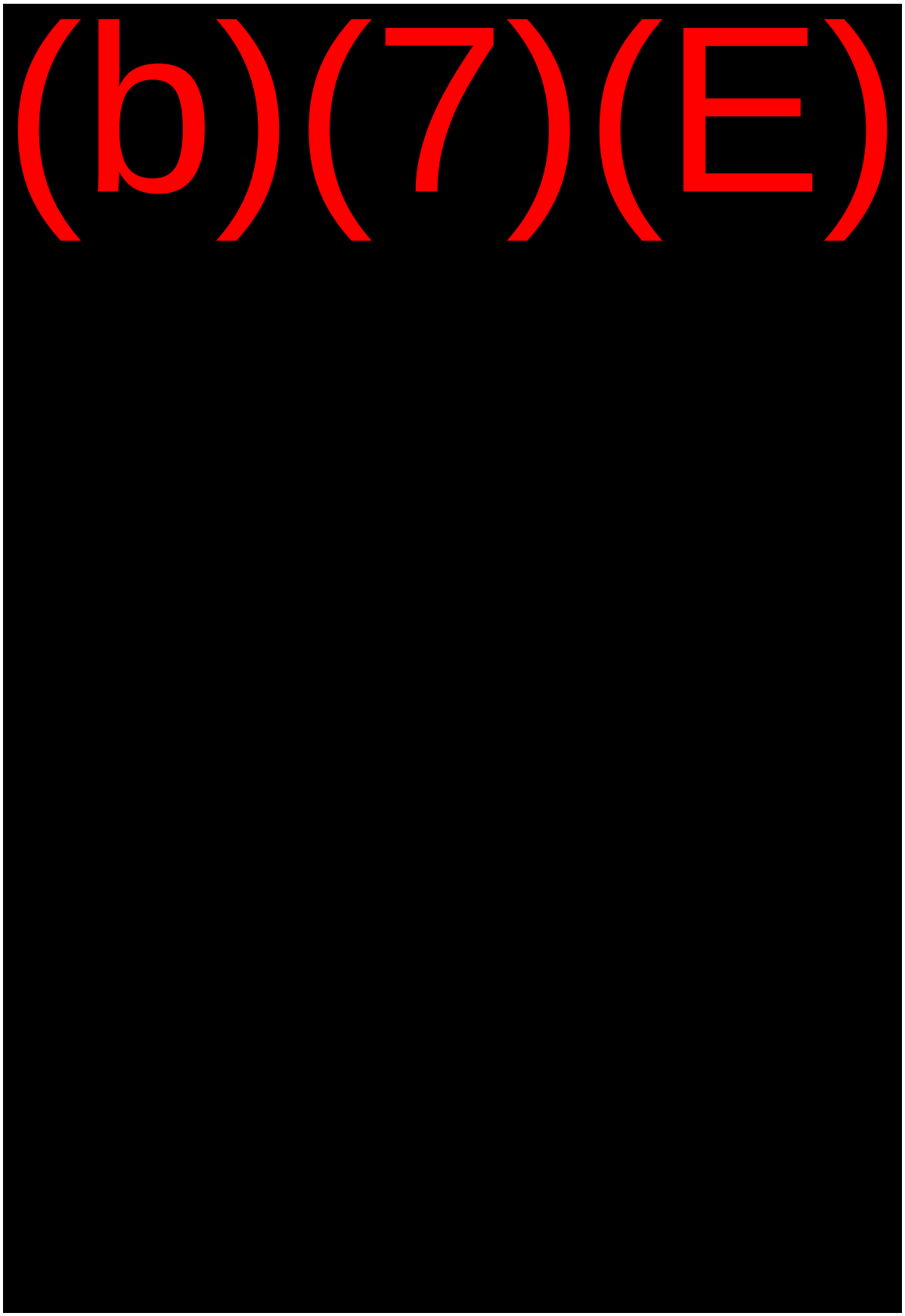

(b)(7)(E)

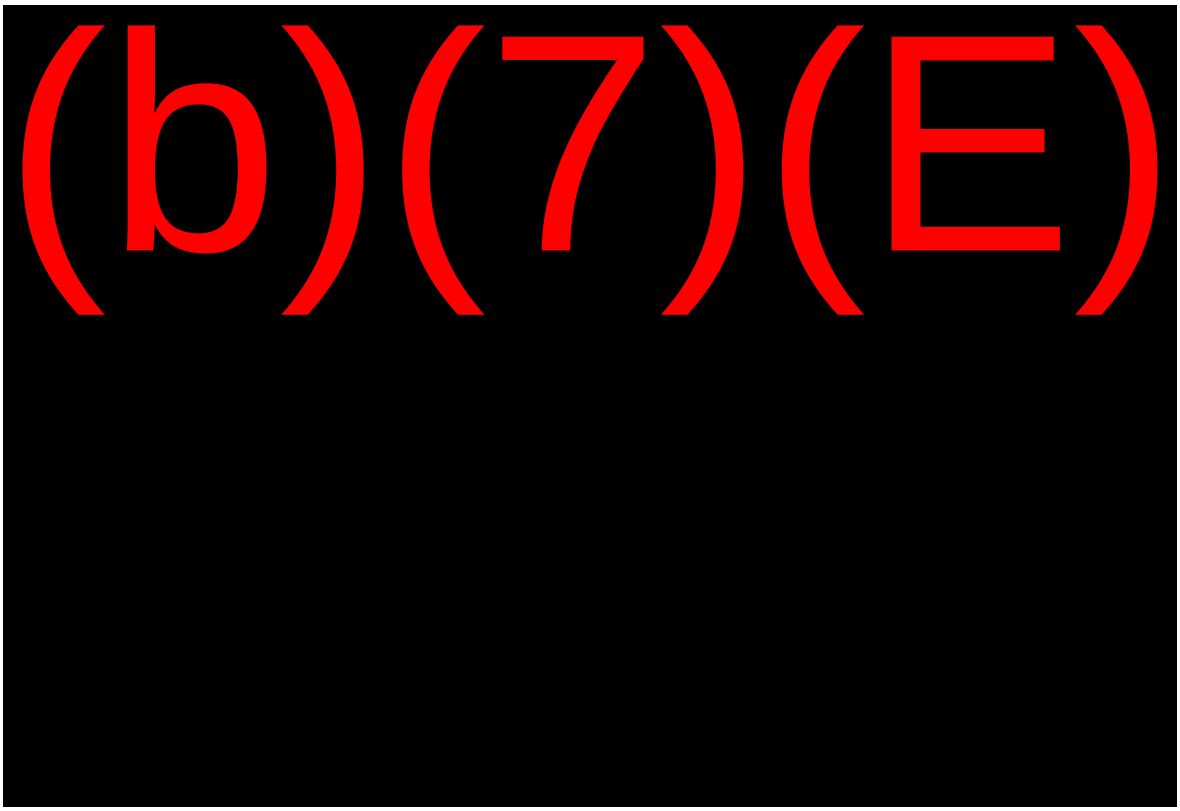
ITSM APPENDICES

This page is intentionally blank.

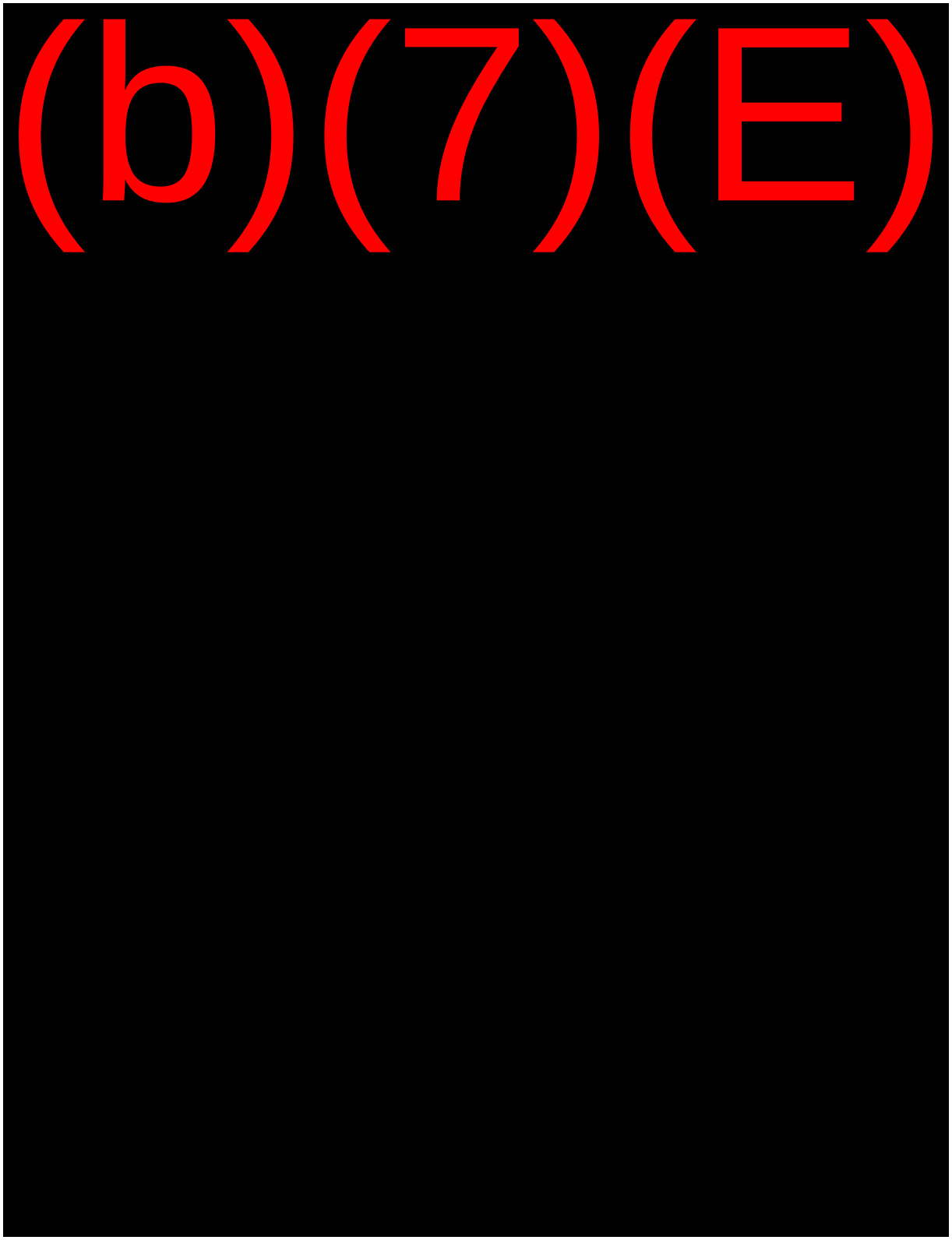
Appendix A: NOAA Common Controls


(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

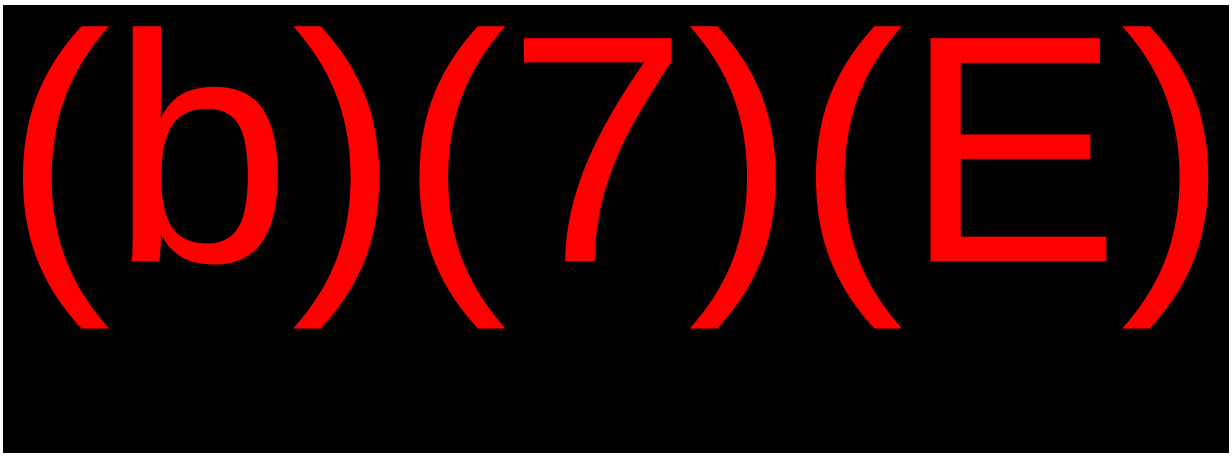
Appendix B: Wireless Security




(b)(7)(E)

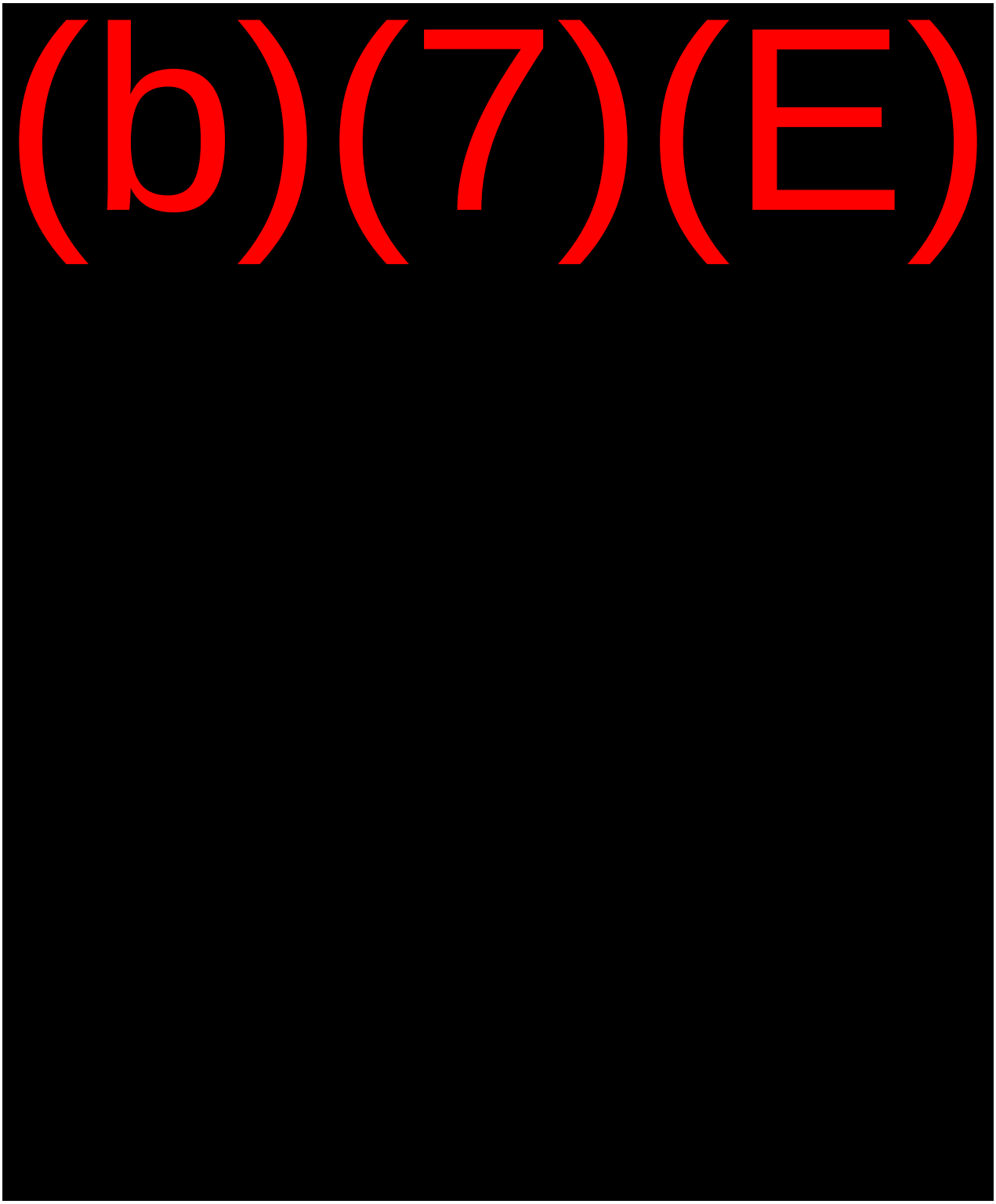

(b)(7)(E)

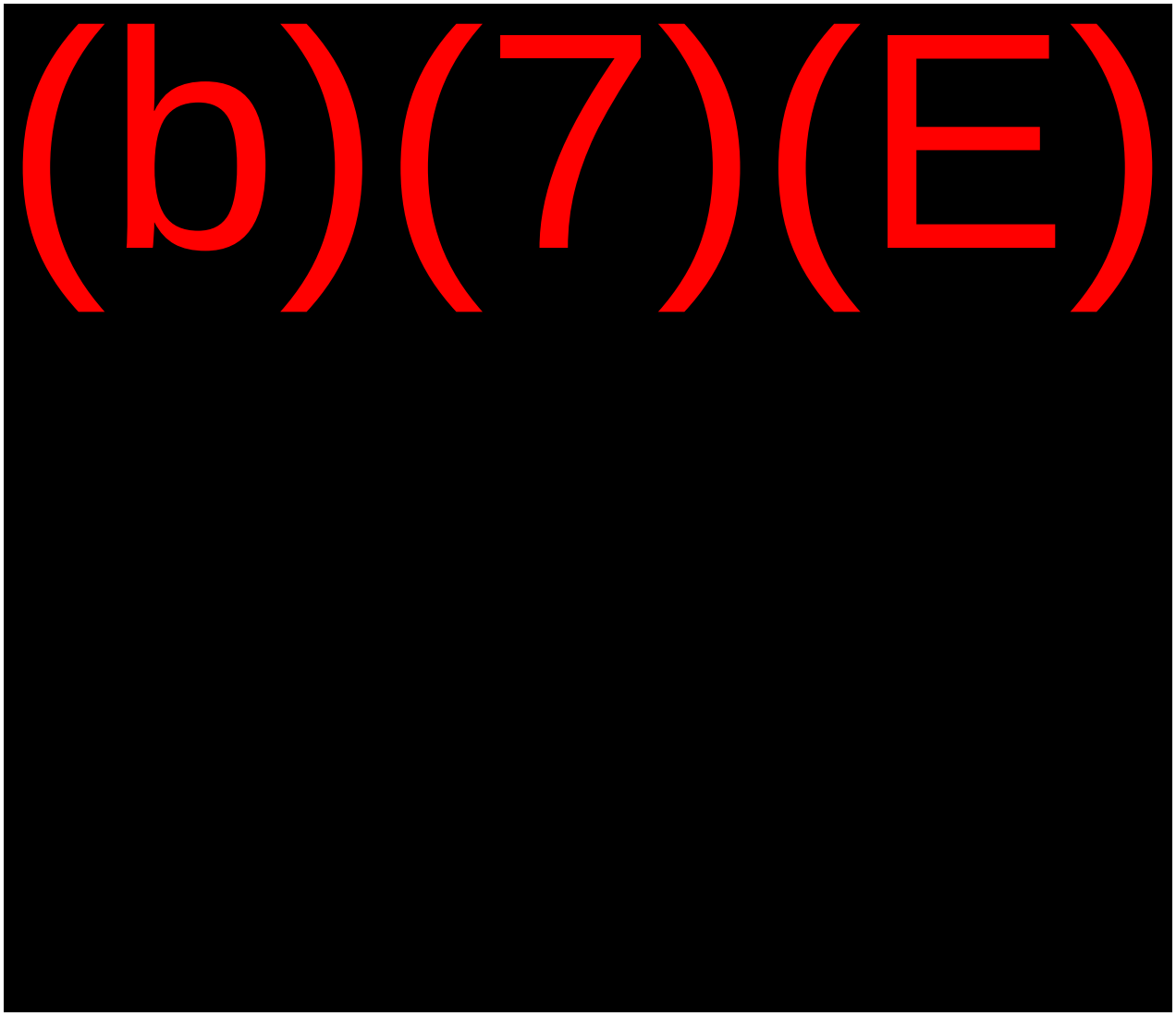

(b)(7)(E)


(b)(7)(E)

Appendix C: Remote Access Agreement

National Oceanic and Atmospheric Administration (NOAA)
Unclassified System Remote Access Approval and User Agreement
(Example)





User's Printed Name/Signature _____ Date

APPROVAL:

Remote access, as described in this agreement, is approved_____ disapproved_____

Printed Name/Signature, Information System Owner _____

Date

Appendix D: Voice over Internet Protocol

K

L. (b)(7)(E)

Appendix E: Security Training

NOAA Augmented Security Awareness and Training: FISMA, this document and higher level policies require mandatory periodic training for all employees involved in the management, use or operation of Federal computer systems. This includes contractors as well as employees of the agency. NOAA Security training shall conform to guidance provided in the NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role-and Performance-Based Model*, and will consist of training in basic computer security, security planning and management, computer security policy and procedures, contingency planning and systems life cycle management.

System owners shall determine the level or extent of such security training required to support the security posture and delineate which training shall be mandatory to grant access to their systems. All NOAA Employees including Contractors and Affiliates will complete the NOAA IT Security Awareness Training at https://www.csp.noaa.govwithin 3 days of entry and agree to abide by the NOAA rules of behavior prior to being granted access to NOAA IT resources. This shall be considered minimum mandated security training for access. System Owners will enforce mandatory training by requiring its completion within the specified time frame or revoking system access if not completed after 3 days of entry on duty and if annual refresher training is not completed by the specified deadline for continued access.

All IT Security Awareness training must be recorded in the NOAA Learning Management System (LMS).

IT Security Awareness, Training, and Education. The types of security learning activities applicable to the NOAA environment include:

1. **Awareness**: Programs and products designed to convey general security information to all NOAA systems users. Such activities range from conducting new employee orientation briefings to security alert services, web-based courses for introduction to government computer security requirements, ad hoc awareness events, creating security literature, and promoting good security through the NOAA IT Security Website.
2. **Training**: Programs and products designed to provide more specific information to enable NOAA systems users functional support and needed security skills and competency relevant to their job role. Training topics include: Security Planning and Management activities covering risk assessment, threat analysis, security training ("train the trainers"), and technical information for systems staff in security configuration and security compliance monitoring.
3. **Education**: Programs and products designed to integrate all security skills and competencies into a common body of knowledge, adding a multi-disciplinary study of concepts, issues and principles. Formalized education for individuals seeking professional certifications in IT security is included in this group.
4. **Refresher Activities**: Programs and products designed to provide continuing education to the NOAA community on relevant security topics. Such programs include annual briefings, distance education refresher products, and related items.

NOAA Augmented IT Security Awareness, Training, and Education Program Requirements. The NOAA IT Security Awareness, Training, and Education Program shall ensure a consistent level of understanding that complies with Law, DOC and NOAA IT security training policies. Mandatory requirements are:

A. All new employees are required to attend the New Employee Orientation Briefing on IT Security. In addition, they are required to complete the web-based security training course within 3 days of entrance on duty.

B. IT security training above the awareness level shall be provided to personnel who manage, design, implement or maintain systems.

C. LO SOs shall ensure that all network and system administrators having responsibility for performing installation, configuration and maintenance of systems and networks are identified and receive appropriate training in systems security. ACIOs will ensure system owners implement and manage tailored IT security training for individuals with privileged access

D. All NOAA system-specific training includes:

1) Awareness specific to the system (patch bugs and fix message distribution, posters, booklets, and trinkets);

2) Documentation of the type and frequency of system-specific security training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the-job training); and

3) Procedures for assuring that employees and contractor personnel have been provided and completed system-specific training shall be documented in the SSP (control AT-1).

E. LOs and systems shall augment of the NOAA training program as required to ensure awareness of locally sensitive security issues. An example might be specific daily requirements for IT security on board NOAA ships. Security Awareness, Training and Education Programs will be designed and provided to meet the mandatory general and specialized requirements (based on the employee's role/job function) as identified in Table 1, Mandatory IT Security Awareness, Training, and Education Requirements.

F. Additional IT security training annually that maintains a level of proficiency to support the evolving security needs of the system. This may be a mix of technical and security awareness training offered by many sources (e.g., SANS Institute, N-CIRT workshops, DOC and NOAA E-Learning etc). Additional SANS courses may be available to NOAA employees at a discount. Information on those SANS courses can be found at: https://www.csp.noaa.gov/tea/

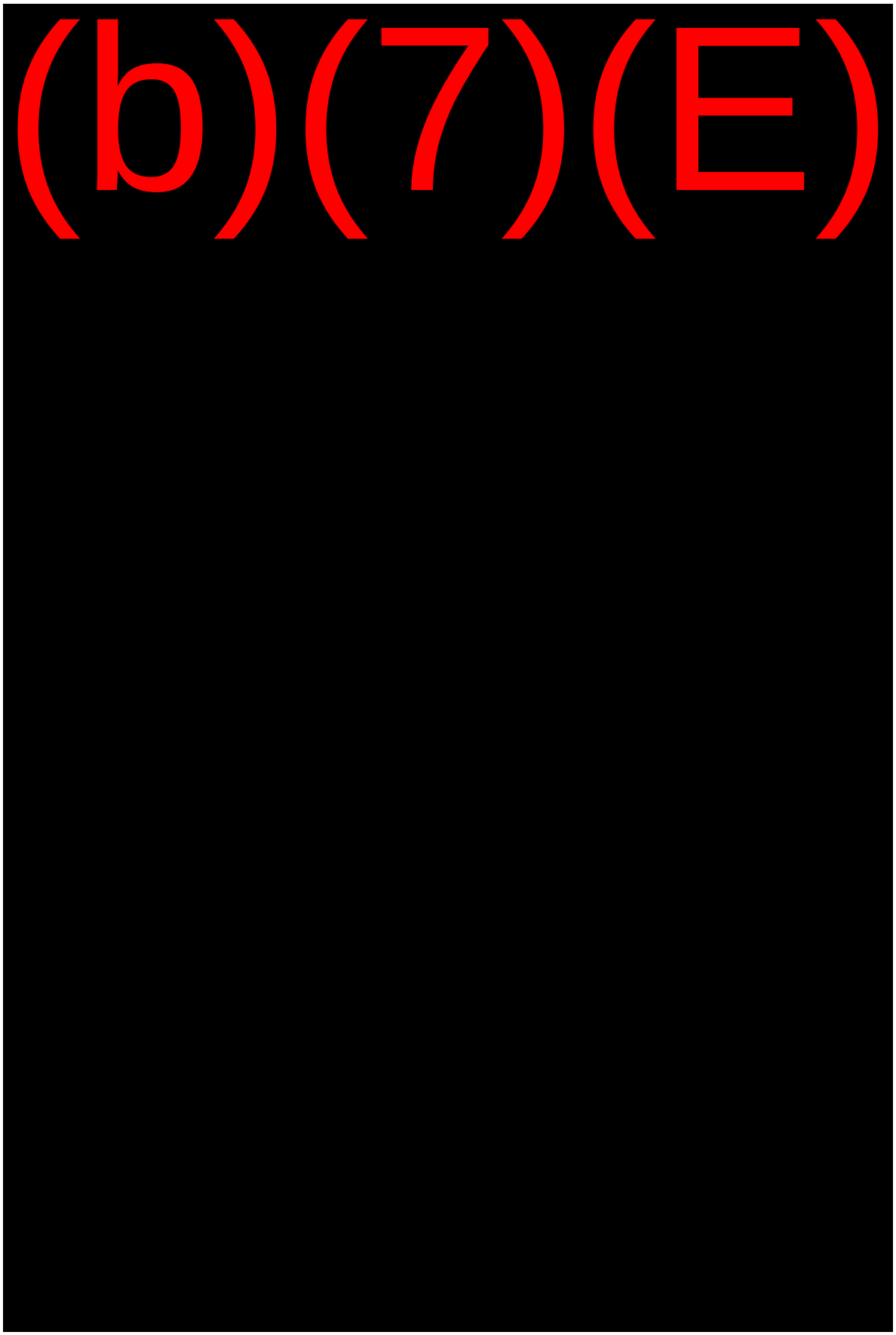
Table 1, Mandatory IT Security Awareness, Training, and Education Requirements

Role/Job Function	Mandatory General Security Awareness and Training Requirements	Mandatory Specialized Security Training and Education Requirements
Senior Management and Budget Officials	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 3 days of entrance on duty)	
System Owners	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 3 days of entrance on duty)	• See CITR-006
SAISOs, ITSOs, ISSOs	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 30 days of entrance on duty)	• Must possess CITR-006 approved professional certification upon appointment and provide annual evidence of credential maintenance.
Network and System Administrators	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 3 days of entrance on duty)	
General IT User	• New employee orientation on IT security. • NOAA-wide web-based general user awareness training. (Required within 3 days of entrance on duty and annually)	

Sources for all of the above training are located on the **NOAA Training, Education. and Awareness page**

Appendix F: Vulnerability Management

1

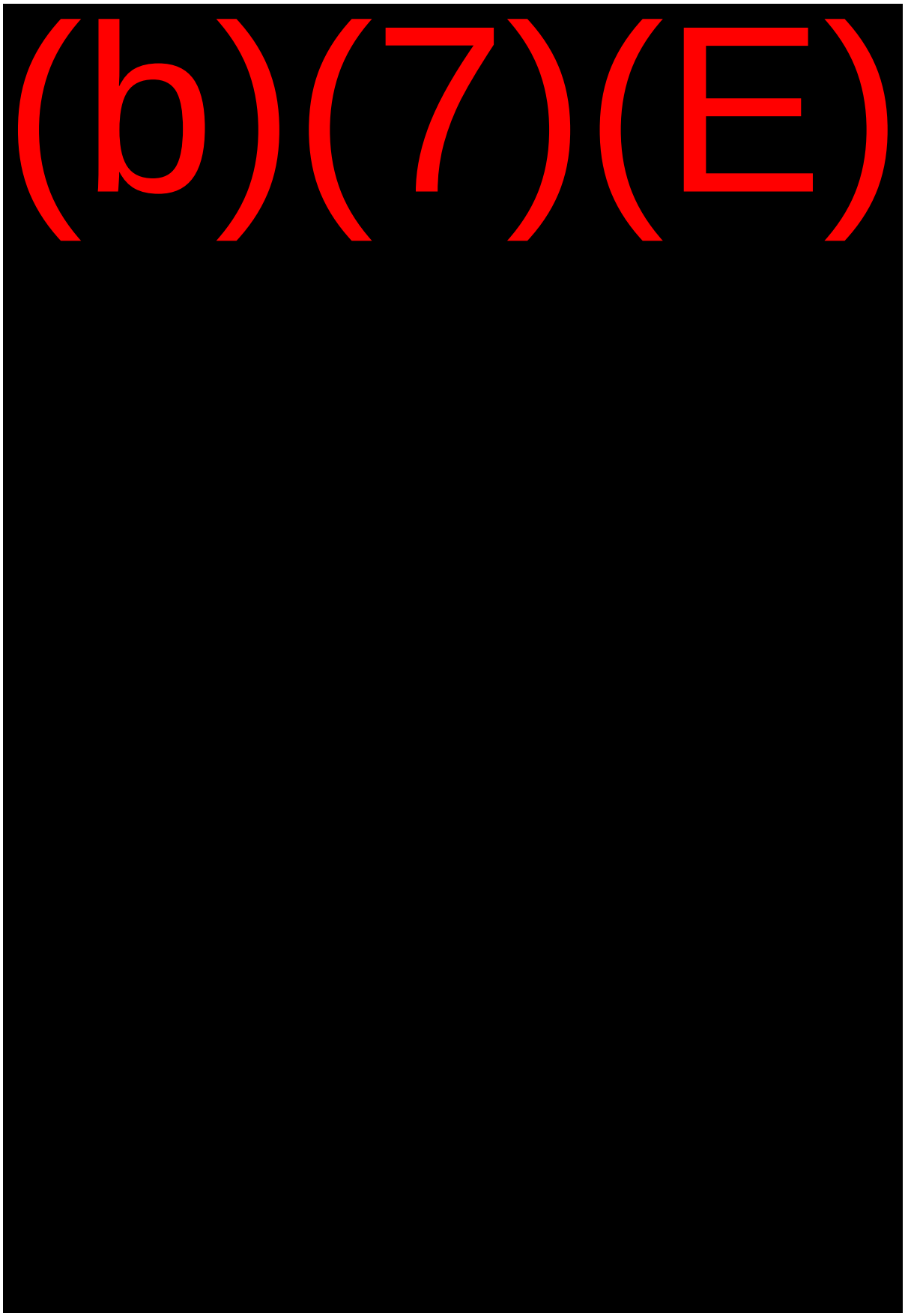

(b)(7)(E)

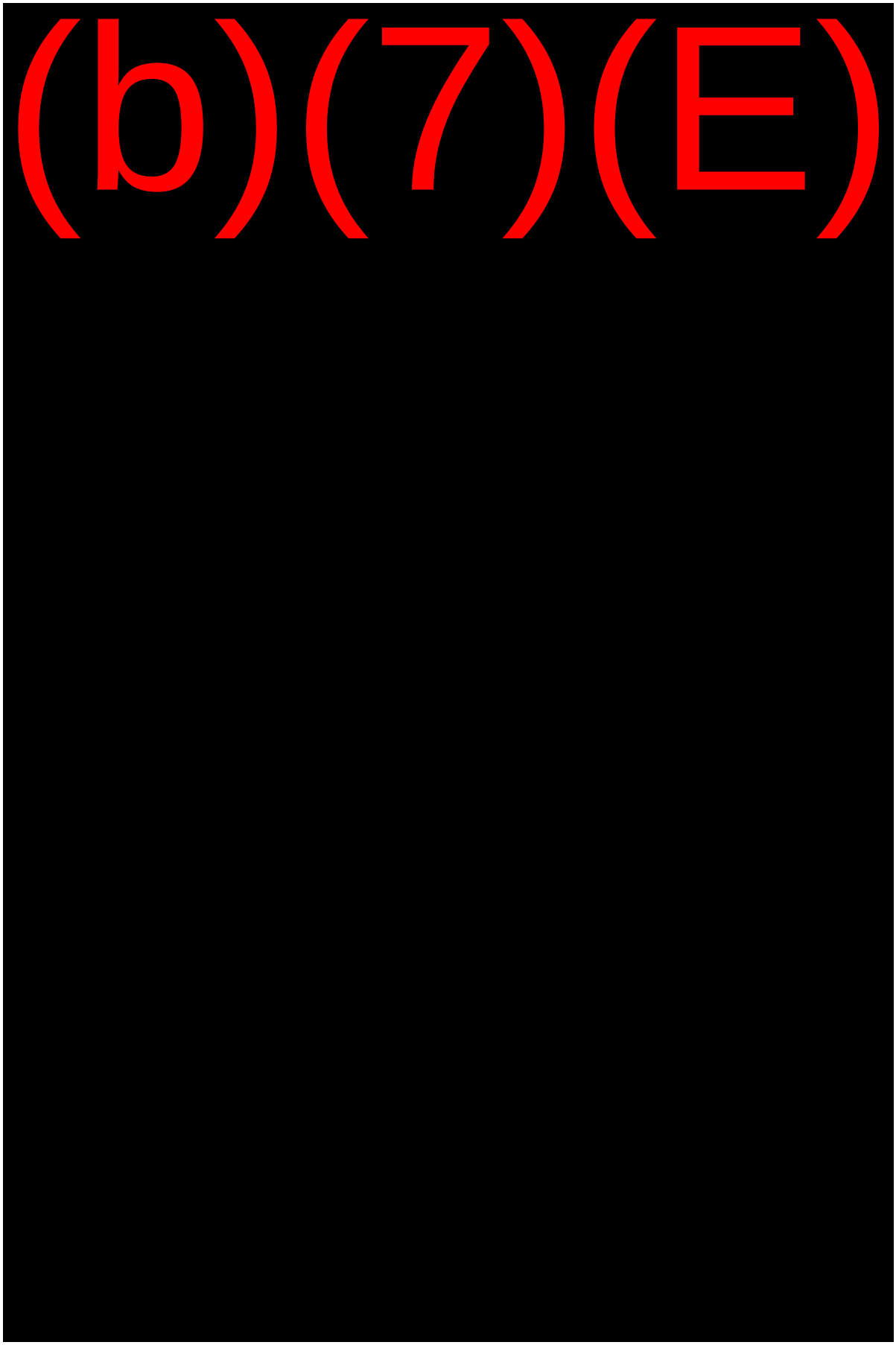
(b)(7)(E)

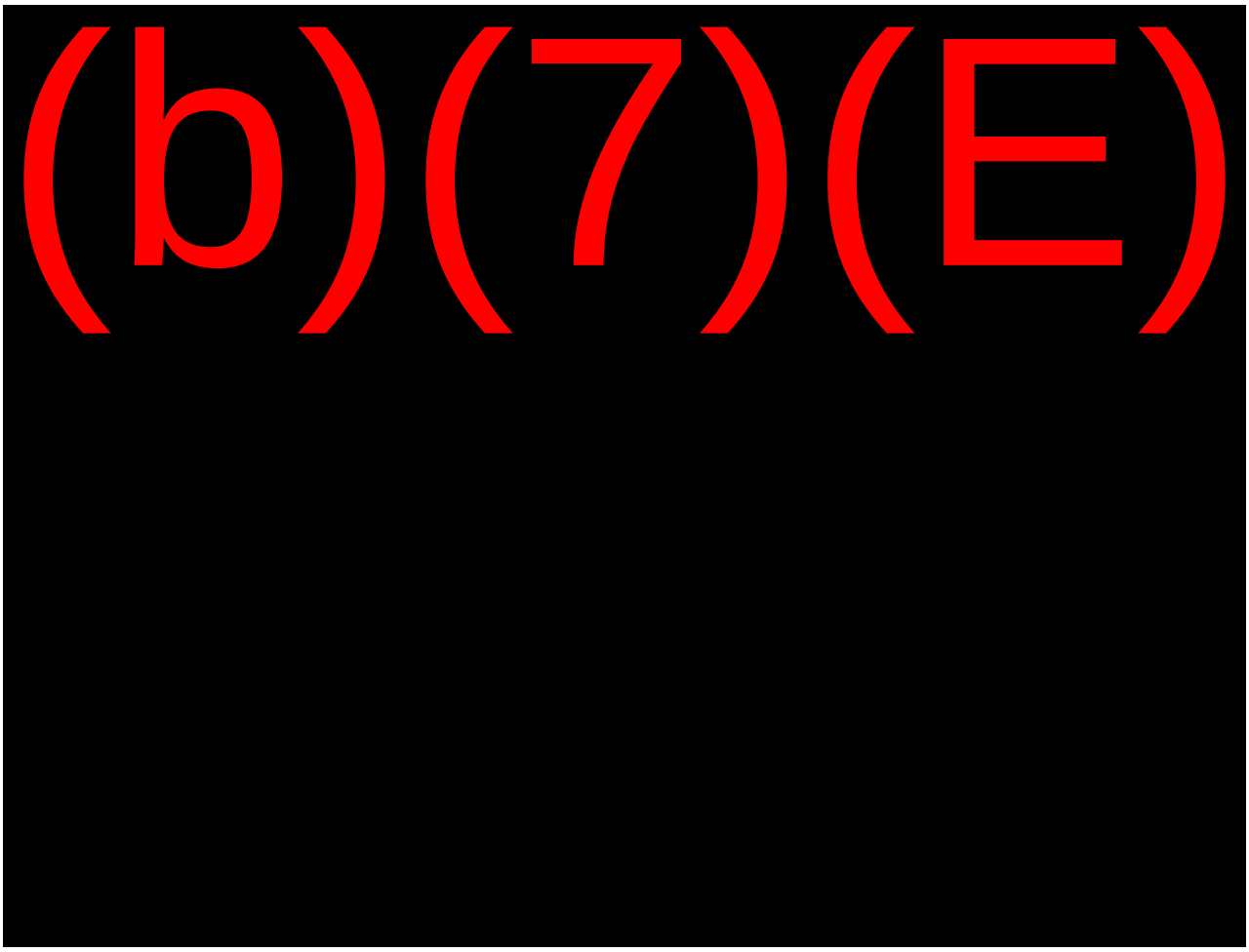
f)

(b)(7)(E)

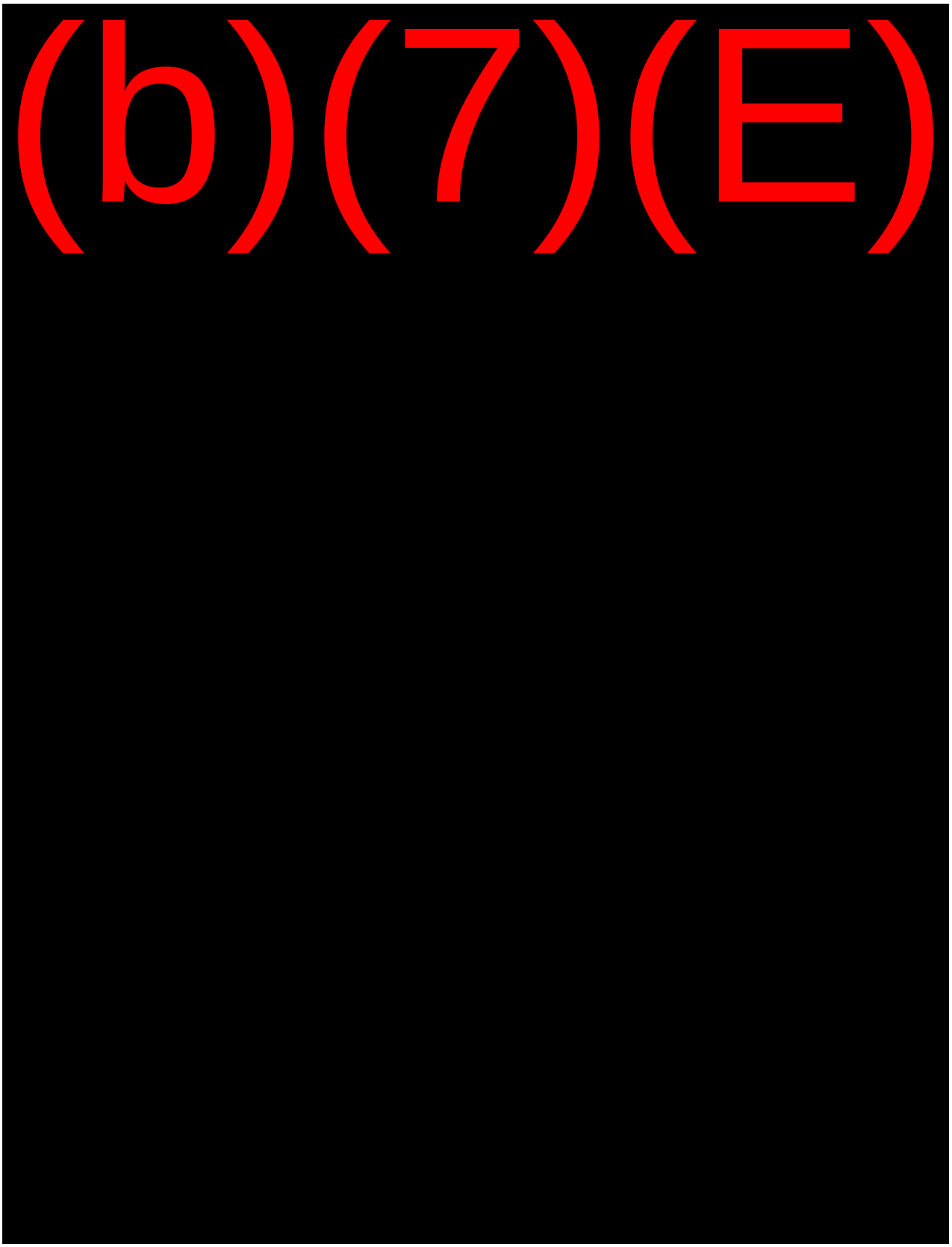
2) (b)(7)(E)


(b)(7)(E)


(b)(7)(E)


(b)(7)(E)

Appendix G: Privacy Controls




(b)(7)(E)

E-mail a link to this directive

OFFICE OF INSPECTOR GENERAL

Number: DOO 23-1

Effective Date: 2013-04-26

SECTION 1. PURPOSE.

.01 This Order prescribes the organization and functions of the Office of Inspector General (OIG) established in the Department of Commerce (the Department) under the Inspector General Act of 1978, 5 U.S.C.A. Appendix 3 as amended (the Act). The scope of authority and functions of the Inspector General are set forth in Department Organization Order 10-13.

.02 This revision updates the Order to incorporate the statutory changes brought about by the Inspector General Reform Act of 2008; reflect the recent reorganizations approved by Congress in May 2008 and September 2011, to reflect the current organization of the OIG and to incorporate title changes of certain subordinate officials who assist the Inspector General. Specifically, this Order eliminates the positions of Assistant Inspector General for Inspections and Program Evaluations and Assistant Inspector General for Systems Evaluation. This revision establishes the positions of Associate Deputy Inspector General, Principal Assistant Inspector General for Audit and Evaluation, and Principal Assistant Inspector General for Investigations.

SECTION 2. ORGANIZATION.

The OIG, directed by the Inspector General, is composed of the immediate office of the Inspector General, the Office of Audit and Evaluation, the Office of Investigations, the Office of Administration, and the Office of Counsel to the Inspector General. The OIG conducts its operations at headquarters offices located in the Herbert C. Hoover Building in Washington, D.C., and at such regional and field offices as may be established by the Inspector General.

SECTION 3. OFFICE OF AUDIT AND EVALUATION..

.01 Organization. The Office of Audit and Evaluation (OAE) will be headed by the Principal Assistant Inspector General for Audit and Evaluation (PAIGAE) who shall be responsible for supervising the performance of audits, evaluations, and inspections relating to the programs and operations of the Department, and will report and be responsible to the Deputy Inspector General and/or the Inspector General. The PAIGAE will supervise the performance of all functions and duties assigned to OAE by the Inspector General and will be advisor to, and serve as representative of, the Inspector General on all audits, evaluations, and inspections.

a. The PAIGAE will be assisted by an Assistant Inspector General for Audit (AIGA), an Assistant Inspector General for Systems Acquisition and IT Security (AIG/SAITS), and an Assistant Inspector General for Economic and Statistical Program Assessment (AIG/ESPA).

1. The AIGA will report to the PAIGAE and will be responsible for the audits, evaluations, and inspections carried out by the headquarters audit and evaluation division, and the regional audit offices; will supervise the planning and performance of these audits, evaluations, and inspections; will advise and represent the OIG on matters regarding these audits, evaluations, and inspections; will advise Department officials regarding these audits, evaluations, and inspections; and will represent the OIG with officials of other Federal agencies or other groups regarding these audits, evaluations, and inspections.

2. The AIG/SAITS will report to the PAIGAE and will be responsible for audits, evaluations, and inspections related to the Department's information technology systems, major systems acquisition projects, and IT security; will supervise the planning and performance of systems acquisition, information technology audits, evaluations, and inspections; will advise and represent the OIG on matters regarding these audits, evaluations, and inspections; will advise Department officials regarding these audits, evaluations, and inspections; and will represent the OIG with officials of other Federal agencies or other groups regarding these audits, evaluations, and inspections.

3. The AIG/ESPA will report to the PAIGAE and will generally be responsible for audits, evaluations, and inspections related to the Department's economic and statistical programs; will supervise the planning and performance of economic and statistical program audits, evaluations, and inspections; will advise and represent the OIG on matters regarding these audits, evaluations, and inspections; will advise the Department officials regarding these audits, evaluations, and inspections; and will represent the OIG with officials of other Federal agencies or other groups regarding these audits, evaluations, and inspections.

b. The functions and duties of OAE will be carried out by the Office of Audit, the Division of Systems Acquisition and IT Security, the Division of Economic and Statistical Program Assessment, and such other divisions or specialized units as may be established to facilitate the performance of OAE's assigned responsibilities.

1. Within the OAE, there may be regional and headquarters offices. These offices may be headed by a Director or Regional Inspector General for Audits (RIGA), who reports to the AIGA.

.02 Functions. OAE will conduct, supervise, and coordinate audits, evaluations, and inspections of all organizational units and activities of the Department and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG's mission.

SECTION 4. OFFICE OF INVESTIGATIONS.

.01 Organization. The Office of Investigations (OI) will be headed by the Principal Assistant Inspector General for Investigations (PAIGI), who shall be responsible for supervising the performance of investigative activities relating to programs and operations of the Department, and will report and be responsible to the Deputy Inspector General and/or the Inspector General. The PAIGI will manage the performance of all functions and duties assigned to OI by the Inspector General; will be advisor to and serve as the representative of the Inspector General on all investigative, Hotline, and whistleblower protection matters; will advise Department officials regarding OIG investigative matters; will be responsible for promoting awareness of whistleblower protections throughout the Department; will evaluate the sufficiency of Departmental whistleblower protection policies and activities; and will represent OIG and the Department with officials of the Department of Justice and other Federal agencies or other public or private groups regarding investigative matters covered by the Act.

a. The PAIGI will be assisted by an Assistant Inspector General for Investigations (AIGI), and such other subordinate employees as the PAIGI may appoint to assist in carrying out assigned duties and functions.

1. The AIGI will report to the PAIGI and will supervise the planning and performance of inquiries/investigations; will advise and represent the OIG on matters regarding inquiries/investigations; and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG's mission.

b. The functions and duties of OI will be carried out by the divisions or specialized units as may be established by the PAIGI to facilitate the performance of OI's assigned responsibilities.

.02 Functions. The OI will conduct, supervise, and coordinate criminal, civil, and administrative inquiries/investigations involving Department programs, operations, and personnel, as authorized by the Act; will perform related activities designed to prevent and detect fraud, waste, and abuse related to the programs and

operations of the Department; and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG's mission.

SECTION 5. OFFICE OF ADMINISTRATION.

.01 Organization. The Office of Administration (OADM) will be headed by an Assistant Inspector General for Administration (AIG/ADM), who will report and be responsible to the Deputy Inspector General and/or the Inspector General.

a. The AIG/ADM will supervise the provision and management of administrative resources and services to the OIG, and will be the principal advisor to the Inspector General on matters relating to OIG resource management, including planning, information and information technology management, personnel administration and security, budget formulation and execution, and support services; will advise and represent the Inspector General on resource management and administrative matters; will advise Department officials regarding these matters; and will represent the OIG with officials of other Federal agencies or other public or private groups regarding resource management and administrative matters.

b. The functions and duties of the OADM will be carried out by Information Technology, Administrative Operations, Human Resources, and other such offices or specialized units as may be established to facilitate the performance of OADM’s assigned responsibilities.

.02 Functions. The OADM will be responsible for the provision and management of administrative resources and services for the OIG, as provided below; and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG’s mission.

a. The OADM will formulate, justify, and defend the OIG’s annual budget requests; will develop its annual budget operating plan and oversee the plan’s implementation; and will provide for sound financial management of the OIG by effectively monitoring and controlling costs and ensuring that budget outlays and obligations do not exceed appropriated funds and reimbursements.

b. The OADM will administer the OIG’s responsibilities relating to employee health and safety and security (personnel, facilities, information, systems, and other resources).

c. The OADM will administer the OIG’s procurement program, including ensuring that the OIG has appropriate policies, systems, and procedures in place to acquire the goods and services it needs in a timely, efficient, and cost-effective manner.

d. The OADM will manage travel and transportation services for OIG employees, including overseeing use of the contractor-issued government travel card.

e. The OADM will administer the OIG's human resources function in accordance with the authorities established in the Act. This function includes recruitment, staffing, personnel security; position classification, employee relations, performance management and recognition, development and training; equal employment opportunity (EEO) and affirmative action; and personnel/payroll processing.

f. The OADM will plan for, acquire, secure, control, and manage OIG office space, facilities, and personal property, and manage conference meeting planning activities for the OIG.

g. The OADM will be responsible for the provision and management of information technology resources and services for the OIG and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG’s mission.

SECTION 6. OFFICE OF COUNSEL TO THE INSPECTOR GENERAL.

.01 Organization. The Office of Counsel to the Inspector General (OC) will be headed by a Counsel to the Inspector General (Counsel), who will report and be responsible to the Inspector General.

a. The Counsel will be the legal advisor to the Inspector General and the OIG staff; will represent the Inspector General on legal matters; and will represent the OIG with officials of the Department of Justice and other Federal agencies or other public and private groups regarding legal matters.

b. The Counsel may be assisted by Senior Assistant Counsels or Deputy Counsel(s), who will be the chief operating aide to the Counsel; will perform other duties and functions as the Counsel may assign; and will perform the duties and functions of the Counsel in his or her absence.

.02 Functions. OC will provide legal services to the Inspector General and OIG staff in connection with the activities and operations of the OIG and will conduct such other activities as may be assigned to facilitate the accomplishment of the OIG's mission.

a. The Inspector General shall obtain legal advice from OC or a counsel reporting directly to another Inspector General except that the General Counsel will provide the Inspector General advice in the areas of conflict of interest statutes, ethics regulations, and related laws.

b. The Inspector General or Counsel to the Inspector General shall consult with the General Counsel on legal matters when they involve significant issues which may have an impact on the operations of the Department or legal matters of applicability to other Departmental bureaus, or concern statutes of government-wide applicability.

.03 In the performance of the responsibilities of his or her office, the General Counsel will respect the independence and integrity of the OIG; in the performance of the responsibilities of his or her office, the Inspector General will give due regard to the authority of the General Counsel as chief legal officer for the Department.

SECTION 7. EFFECT ON OTHER ORDERS

This Order supersedes DOO 23-1, dated August 31, 2006.

Signed by: Inspector General

Approved Deputy Secretary of Commerce

Questions and Comments

Send Questions or Comments on the Commerce Directives Management program to Directives@doc.gov.

Office of Privacy and Open Government
Office of the Chief Financial Officer and Assistant Secretary for Administration
U.S. Department of Commerce

Page last updated:May 24, 2013

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, April 4, 2018 12:25 PM
To:	Mark Graff NOAA Federal
Subject:	Fwd: Re NOAA8104 PTA
Attachments:	NOAA8104 NEXRAD PTA 13Feb18 Digital Signature AB.pdf

Mark, for your signature. Just was time to renew the PTA.

thx Sarah

Forwarded message
From: **Daniel Hernandez - NOAA Affiliate** <daniel.d.hernandez@noaa.gov>
Date: Tue, Apr 3, 2018 at 4:56 PM
Subject: Re: Re NOAA8104 PTA
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Charles Parish <charles.r.parish@noaa.gov>

Sarah,

Attached is the NOAA8104 PTA with the AO, ITSO, and ISSO signatures... Thanks

Dan

On Mon, Apr 2, 2018 at 7:11 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Thanks, Dan.
>
> On Fri, Mar 30, 2018 at 2:12 PM, Daniel Hernandez NOAA Affiliate <daniel.d.hernandez@noaa.gov> wrote:
>
> > Sarah,
> >
> > The NOAA8104 PTA is currently getting signed by the ITSO and AO. As soon as it is returned, we will forward it on to you. Also, Charles (Chuck) Parish is the new NOAA8104, NOAA8212, and NOAA3065 ISSO, and I am his alternate. Patrick has moved on (internally) to greener pastures... Thanks
> >
> > Dan
> >
> > Forwarded message
> > From: **Patrick Quigley - NOAA Federal** <patrick.l.quigley@noaa.gov>
> > Date: Wed, Mar 28, 2018 at 8:50 AM
> > Subject: Fwd: Re NOAA8104 PTA
> > To: Daniel Hernandez <daniel.d.hernandez@noaa.gov>, Charles Parish NOAA Federal <charles.r.parish@noaa.gov>
> >
> > Did you guys get a signature on the PTA for NEXRAD?

Forwarded message
From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Tue, Mar 27, 2018 at 12:35 PM
Subject: Re NOAA8104 PTA
To: Patrick Quigley <patrick.l.quigley@noaa.gov>
Cc: Andrew Browne NOAA Affiliate <andrew.Browne@noaa.gov>

Patrick, I thought I had emailed you recently to check on your PTA that had been in process of being signed, in February. I was just trying to follow up, but can't find such an email! Can you give me the status?

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Patrick Quigley,
Software Engineering
Radar Operations Center

Dan D. Hernandez, CISSP
Serco Inc.
Support Contractor: NEXRAD Radar Operations Center
Norman, OK
Phone: 405-573-3392

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division

Office 301 628 5751
Ce (b)(6)

Dan D. Hernandez, CISSP
Serco Inc.
Support Contractor: NEXRAD Radar Operations Center
Norman, OK
Phone: 405-573-3392

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, April 4, 2018 1:34 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Re NOAA8104 PTA
Attachments:	NOAA8104 NEXRAD PTA 13Feb18 Digital Signature AB mhg.pdf

Looks good signed and attached.

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) (C)

On Wed, Apr 4, 2018 at 12:25 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, for your signature. Just was time to renew the PTA.
>
> thx Sarah
>
> Forwarded message
> From: **Daniel Hernandez - NOAA Affiliate** <daniel.d.hernandez@noaa.gov>
> Date: Tue, Apr 3, 2018 at 4:56 PM
> Subject: Re: Re NOAA8104 PTA
> To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Charles Parish <charles.r.parish@noaa.gov>
>
> Sarah,
>
> Attached is the NOAA8104 PTA with the AO, ITSO, and ISSO signatures... Thanks
>
> Dan
>
> On Mon, Apr 2, 2018 at 7:11 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Thanks, Dan.
> >
> > On Fri, Mar 30, 2018 at 2:12 PM, Daniel Hernandez NOAA Affiliate <daniel.d.hernandez@noaa.gov> wrote:
> >
> > > Sarah,
> > >
> > > The NOAA8104 PTA is currently getting signed by the ITSO and AO. As soon as it is returned, we will

forward it on to you. Also, Charles (Chuck) Parish is the new NOAA8104, NOAA8212, and NOAA3065 ISSO, and I am his alternate. Patrick has moved on (internally) to greener pastures... Thanks

Dan

Forwarded message
From: **Patrick Quigley - NOAA Federal** <patrick.l.quigley@noaa.gov>
Date: Wed, Mar 28, 2018 at 8:50 AM
Subject: Fwd: Re NOAA8104 PTA
To: Daniel Hernandez <daniel.d.hernandez@noaa.gov>, Charles Parish NOAA Federal <charles.r.parish@noaa.gov>

Did you guys get a signature on the PTA for NEXRAD?

Forwarded message
From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Tue, Mar 27, 2018 at 12:35 PM
Subject: Re NOAA8104 PTA
To: Patrick Quigley <patrick.l.quigley@noaa.gov>
Cc: Andrew Browne NOAA Affiliate <andrew.Browne@noaa.gov>

Patrick, I thought I had emailed you recently to check on your PTA that had been in process of being signed, in February. I was just trying to follow up, but can't find such an email! Can you give me the status?

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Patrick Quigley,
Software Engineering
Radar Operations Center

Dan D. Hernandez, CISSP
Serco Inc.
Support Contractor: NEXRAD Radar Operations Center
Norman, OK
Phone: 405-573-3392

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Dan D. Hernandez, CISSP
Serco Inc.
Support Contractor: NEXRAD Radar Operations Center
Norman, OK
Phone: 405-573-3392

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
WSR-88D Next Generation Weather Radar (NEXRAD)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA / NEXRAD

Unique Project Identifier: 8104

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The National Weather Service (NWS) provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including warnings and forecasts is dependent on a complex interaction of many information resources. This NEXRAD system is the NWS prime observation system for acquiring information about tornados and severe thunderstorms (containing damaging wind, hail, turbulence, and lightning). It also provides information on heavy precipitation leading to flash flooding and heavy snow warnings. NEXRAD is a key element in forecasting aviation related weather events.

The NEXRAD Program (also known as WSR-88D interchangeable nomenclature) supports the mission of the Principal Users DOC, DoD, and DOT. The RPG generates products for WSR-88D Principal Users. Principal Users connect to the WSR-88D through dedicated and dial circuits and all system interconnections are fully documented. The WSR-88D meets common weather radar needs to perform and support Principal User activities. These activities include warning of hazardous weather and flash floods, predicting weather conditions, ensuring safety of flight, protecting base resources, and planning military missions. Each agency uses its own network to obtain weather information generated by a specific site. Only Government to Government connections are permitted and inter-agency agreements are established to define the interface and security requirements. Operational procedures are established and agreed to by the three Principal Users.

There are 159 operational WSR-88D systems deployed throughout the United States and at selected overseas locations. An individual WSR-88D system is composed of hardware, software, and LAN components to support the application software. The purpose of the application software is to acquire weather data, process this weather data into weather products and

deliver these weather products to the Principal Users. These systems have been updated with dual-polarization technology to provide the ability to collect data on the horizontal and vertical properties of weather (e.g., rain, hail) and non-weather (e.g., insect, ground clutter) targets. Dual Polarization technology adds new information about the size and shape of an object. Each WSR-88D system functions as a stand-alone system that does not access the Internet, and cannot be accessed by the public.

NEXRAD is type certified and accredited for fielding at multiple locations. The authorized system baseline configuration is delivered to all operational users at their specific site via distribution of the WSR-88D EHB 6-504 manual. One System Security Plan has been prepared for the system software and hardware, applicable to the following configurations and NEXRAD support equipment: NWS Single Thread, NWS Redundant, FAA, and DoD. This System Security Plan has been shipped to each site, along with the system incident response plan, rules of behavior, contingency plan, and administration and maintenance. The contents are intended for WSR-88D Support and Operations personnel, including System Administrators, managers, programmers, maintenance technicians, operators, engineers, trainers, and other technical staff. This System Security Plan defines the scope of security needs of the WSR-88D, prescribes policy, and discusses assets that need protection, and the extent to which personnel should go to provide the necessary protection.

NEXRAD security testing occurs at the Radar Operation Center (ROC) which is in place and established to accurately represent each of the configurations established in the field for NEXRAD fleet support. All software and hardware changes and tests are developed and performed at the ROC. Security tests of common system components at operational NEXRAD sites are prohibited. At the conclusion of the security testing at the ROC, the test results are documented, along with the certifier's recommendation, and the NEXRAD authorization agreement files are updated. A formal modification document (NWS, DoD and/or FAA) along with a security certification statement is then sent with the software and hardware suite to each site. The site does not need to repeat the baseline tests conducted by the ROC type accreditation effort. The site is prohibited from performing tests on operational systems or making any unauthorized hardware and software changes.

Type authorization applies to NEXRAD, and approval of the NEXRAD Program for Authorization to Operate is the official authorization to employ identical copies of a system in specified environments. It is only permitted and possible by virtue of strict configuration management controls. Combined establishment of type accreditation and stringent configuration management allows for an efficient way to support the tri-agency NEXRAD program.

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X__ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

_X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
____ Members of the public

_X__ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.
____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_X___ I certify the criteria implied by the questions above **do not apply** to the NEXRAD NOAA8104 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):

Charles R. Parish, ISSO_____

Signature of ISSO or SO: PARISH.CHARLES.R.1124635523 Digitally signed by PARISH CHARLES R 1124635523 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn PARISH CHARLES R 1124635523 Date 2018 02 13 10 52 16 06'00' _____ Date: _____

Name of Information Technology Security Officer (ITSO):

Andrew Browne, ITSO_____

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE ANDREW PATRICK 1472149349 Date: 2018 04 02 15:39:13 04'00' _____ Date: _____

Name of Authorizing Official (AO):

Joseph A. Pica, AO_ _____

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2018.04.03 16:52:32 -04'00' _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO):

Mark Graff, BCPO_____

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892 Date 2018 04 04 13 33 29 04'00' _____ Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, April 4, 2018 3:37 PM
To:	Mark Graff NOAA Federal
Subject:	Fwd: Updated PIA/PTA and Annual PIA Cert..
Attachments:	NOAA8882 PIA 040318 (1).pdf; NOAA8882 PTA March 2018 (1).pdf

Somehow we got mixed up. Andrew signed the ones from before you signed rather than the ones i sent back . . pls sign again, thx.

Forwarded message
From: **Nicholas Rappold - NOAA Federal** <nicholas.rappold@noaa.gov>
Date: Wed, Apr 4, 2018 at 2:45 PM
Subject: Re: Updated PIA/PTA and Annual PIA Cert..
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>

Here you go.

Nicholas RappoldInformation System Security Officer (ISSO)

NWS Eastern Region Headquarters
630 Johnson Avenue, STE 202
Bohemia, NY 11716
Phone: (631) 244-0191
Fax: (631) 244-0168

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, April 4, 2018 4:40 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Updated PIA/PTA and Annual PIA Cert..
Attachments:	NOAA8882 PTA March 2018 (1) mhg.pdf; NOAA8882 PIA 040318 (1) mhg.pdf

Here they are signed (b)(5) [redacted].

Mark H. Graff
FOIA Officer/Bureau Chief Privacy Officer (BCPO)
National Oceanic and Atmospheric Administration
(301) 628 5658 (O)
(b)(6) [redacted] (C)

On Wed, Apr 4, 2018 at 3:37 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Somehow we got mixed up. Andrew signed the ones from before you signed rather than the ones i sent back . . pls sign again, thx.
>
> Forwarded message
> From: **Nicholas Rappold - NOAA Federal** <nicholas.rappold@noaa.gov>
> Date: Wed, Apr 4, 2018 at 2:45 PM
> Subject: Re: Updated PIA/PTA and Annual PIA Cert..
> To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
>
> Here you go.
>
> ***Nicholas RappoldInformation System Security Officer (ISSO)***
>
> NWS Eastern Region Headquarters
> 630 Johnson Avenue, STE 202
> Bohemia, NY 11716
> Phone: (631) 244-0191
> Fax: (631) 244-0168

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service Eastern Region (ER) Wide Area Network/Local Area Network

NOAA8882

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Weather Service (NWS) Eastern Region (ER) WAN/LAN

Unique Project Identifier: 006-000351104 00-48-02-00-02-00

Introduction: System Description

National Weather Service's Eastern Region is a General Support System, comprised by Eastern Region HQ located in Bohemia, NY and 23 additional offices across the region. The primary database servers are located at the Eastern Region HQ, in Bohemia, NY.

NWS Eastern Region (ER) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees and volunteers who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports and performing other related administrative tasks. In addition, Weather Forecast Office (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers who provide weather reports to them.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, budget and requisition information, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training (see above, no PII involved), research and development, and collaboration.

PII is collected and stored for employees, as well as for weather volunteers (members of the public). The PII/BII in this system is not shared except within the bureau, and in case of a privacy breach, with the Department or other Federal Agencies.

The legal authorities for information collection addressed in this PIA are:

- 5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
- 44 U.S.C. 3101addresses records management by Department agency heads.
- 15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
- 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

This is a FIPS 199 moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__X___ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X

b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
Other work-related data (specify): Division/organization name, regional location, optional text field that is not to contain PII.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Latitude/Longitude for spotter reports.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X*
Telephone	X	Email	X		
Other (specify):					

*If requesting spotter newsletter

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in

reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NWS ER WAN/LAN system maintains information concerning each member of the ER workforce (employees). This information is managed by the NWS Eastern Region Headquarters (ERH) Administration Personnel.

The administrative information maintained on these databases consists of:

- Name /Position /GS Level/Series/Service Computation Date/Date of Grade/ Date of separation
- Residential information (Address, phone numbers)
- Government email addresses
- Division/Organization Name
- Regional Office Location
- Optional text field with current/relevant personnel issues.

The information is maintained as a supplement to other employee records for purposes of developing statistical reports, and performing other related administrative tasks

There are also local databases at the local WFO/RFC that maintain information on volunteers (members of the public) who provide them weather reports. The database holds the following information on these volunteers:

- First and last name
- Mailing address
- County
- Phone (home/cell)
- Email address (also collected on the Cooperative Web site if requesting the newsletter)
- Hours to be contacted for severe weather reports
- Possession of a rain gauge, anemometer, thermometer, snow stick, or weather station
- Brief description of location of spotter's personal residence
- Last time attended spotter class
- Community Weather Involvement Program Identification (optional) not all offices use this. It's a locally assigned number from the field office.
- Latitude / Longitude

All of this information collected on volunteers is provided voluntarily and most people who sign up do so during a community outreach training program, known as "spotter talks." An ER staff is responsible for the maintenance of this database. This database information is accessible for viewing by all staff members in order to make calls for severe weather information.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Law enforcement

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.nws.noaa.gov/om/coop/index.htm	
X	Yes, notice is provided by other means.	Specify how: For the workforce database, employees are

		notified at the time of recruitment that the collection of their information is mandatory as a condition of employment. For the Spotter Volunteers, notice is provided in the cooperative agreement form when information is collected.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the workforce database, individuals may inform HR staff, verbally or in writing, that they do not want their information added to the database; however, provision of the information is a condition of employment. All information is voluntary for Spotter Volunteers, as part of the cooperative agreement to work with NWS on providing observations. There is a Privacy Act Statement on the Web site.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For the workforce database, employees may choose not to consent to all uses (administrative, job vacancy tracking, statistical reports) by informing HR staff verbally or in writing; however, they are required to provide the information as a condition of employment. The only use of the information for volunteers is for contact purposes, which is explained in the cooperative agreement. No other uses are suggested or specified. Provision of the information and signing of the cooperative agreement implies consent to that use.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the workforce data, information is routinely updated as an employee's role or position changes. Employees cannot directly review the information, but may request to review their information and ask that it be updated, through their supervisors. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Management Division (AMD) Chief. The local manager who recruited the volunteers updates their information when notified by them to do so. Updates are not

		solicited but the instructions for submitting updates are in the cooperative agreement.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Any access to the local database is logged and saved.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 3/31/2018 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access to the system maintaining the PII is controlled via National Active Directory. Authentication is verified by the use of CAC IDs and PIV Cards. Only employees with authority to maintain these databases are allowed access to the information.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/DEPT-13, Investigative and Security Records COMMERCE/DEPT-18, Employee Personnel Files Not Covered By Notices of Other Agencies NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1300 – Weather, 1307-05, Chapter 300 – Personnel
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:

X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Name and contact information for volunteers, and names of employees, are in the system.
X	Quantity of PII	Provide explanation: Limited amount of PII stored.
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields other than optional text field with current/relevant personnel issues (where completed). .
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Secured database managed by federal employees with limited user privileges.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer Name: Nicholas Rappold Office: NWS Eastern Region Headquarters Phone: 631-244-0191 Email: Nicholas.Rappold@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: RAPPOLD.NICHOLAS.PAUL.1459652953 Digitally signed by RAPPOLD.NICHOLAS.PAUL.1459652953 Date: 2018.04.03 14:06:07 04'00'	**Information Technology Security Officer** Name: Andrew Browne Office: NWS OCIO Phone: 301-427-9033 Email: Andrew.browne@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.04.04 14:31:11 04'00'
Authorizing Official Name: Jason Tuell Office: NWS Eastern Region Headquarters Phone: 631-244-0101 Email: Jason.Tuell@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: TUELL.JASON.P.1011566410 Digitally signed by TUELL.JASON.P.1011566410 Date: 2018.04.03 16:33:09 -04'00'	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF MARK HYRUM 1514447892 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GRAFF MARK HYRUM 1514447892 Date 2018 04 04 16 38 14 04'00'

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA National Weather Service
Eastern Region Network

March 26, 2018

U.S. Department of Commerce Privacy Threshold Analysis

NOAA8882 ER LAN/WAN

Unique Project Identifier: 006-000351104 00-48-02-00-02-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:
The NWS Eastern Region (ER) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees, contractors, volunteers, and other individuals who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of tracking job vacancies, developing statistical reports, and performing other related administrative tasks. Weather Forecast Office (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers who provide weather reports to them.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

The statutory authority covering the collection of this data is 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce]. This is a moderate level system.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

_X_ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the

submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X_ DOC employees
_X_ Contractors working on behalf of DOC
_X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_X_ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of Information System Security Officer (ISSO): Nicholas Rappold

Signature of ISSO: RAPPOLD.NICHOLAS.PAUL.1459652953
Digitally signed by RAPPOLD.NICHOLAS.PAUL.1459652953
Date: 2018.04.03 14:39:15 04'00'

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349
Digitally signed by BROWNE.ANDREW.PATRICK.1472149349
Date: 2018.04.04 14:31:38 04'00'

Name of Authorizing Official (AO): Jason P. Tuell

Signature of AO: TUELL.JASON.P.1011566410
Digitally signed by TUELL.JASON.P.1011566410
Date: 2018.04.03 16:33:33 -04'00'

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892
Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.04.04 16:37:05 -04'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, April 5, 2018 11:57 AM
To:	Gioffre, Kathy (Federal); CPO
Cc:	Mark Graff NOAA Federal
Subject:	NOAA8881 certification documents
Attachments:	NOAA8881_PIA_2018 mhg.pdf; NOAA8881 PIA Annual_Review_Certification_Form_with_PA_Officer 2018 for MHG signature mhg.pdf; NOAA8881_PTA_2018 AB mhg.pdf

Attached are the certification, the re signed PIA and the current PTA.

ATO date is 7 31 18.

Last CRB was 6 29 17.

thx Sarah

Sarah D. Brabson
IT Infrastructure Investment Program Manager
PRA Clearance Officer

Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA: NOAA8881 – NWS CR WAN\LAN PIA 2018

FISMA Name/ID (if different): NOAA8881 – NWS CR WAN\LAN

Name of IT System/ Program Owner: Bob Brauch

Name of Information System Security Officer: Adam Van Meter

Name of Authorizing Official(s): Christopher Strager and Richard Varn

Date of Last PIA Compliance Review Board (CRB): 6/29/2017

(This date must be within three (3) years.)

Date of PIA Review: 3/19/2018

Name of Reviewer: Adam Van Meter

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: VAN METER.ADAM.L.1365874057 Digitally signed by VAN METER.ADAM.L.1365874057 Date: 2018.03.20 08:19:37 05'00'

Date of Privacy Act (PA) Review: 3/20/2018

Name of Reviewer: Sarah Brabson

REVIEWER CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: BRABSON.SARAH.1365710488 Digitally signed by BRABSON SARAH 1365710488 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BRABSON SARAH 1365710488 Date 2018 03 20 10 55 53 04'00'

Date of BCPO Review: 4/4/18

Name of the Reviewing Bureau Chief Privacy Officer (BCPO): Mark Graff

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the Bureau Chief Privacy Officer:

GRAFF.MARK.HYRUM.1514447892

Digitally signed by GRAFF.MARK.HYRUM.1514447892
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2018.04.04 14:15:27 -04'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service Central Region (CR) Wide Area Network/Local Area Network

NOAA8881

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Weather Service (NWS) Central Region (CR) WAN/LAN

Unique Project Identifier: 006-48-01-12-01-3118-00-108-023

Introduction: System Description

The NWS Central Region (CR) Wide Area Network (WAN)/Local Area Network (LAN) databases, located in Kansas City, Missouri, consist of basic identifying information about employees and volunteers who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports, and performing other related administrative tasks. In addition, Weather Forecast Office (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers who provide weather reports to them. The Warning Decision Training Division and NWS Training Center (originally in NOAA8900, which has been decommissioned) have been integrated into NOAA8881, but neither of them collects nor stores PII or BII.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems and client-server systems. The system supports a variety of users, functions, and applications, including word processing, budget and requisition information, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training (see above, no PII involved), research and development, and collaboration.

PII is collected and stored for employees, as well as for weather volunteers (members of the public). The PII/BII in this system is not shared.

The legal authorities for information collection addressed in this PIA are:

- 5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
- 44 U.S.C. 3101addresses records management by Department agency heads.
- 15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

This is a moderate level system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.

____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

__X___ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
Other work-related data (specify): Division/organization name, regional location, optional text field with current/relevant personnel issues.					

Distinguishing Features/Biometrics (DFB)

a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Latitude/Longitude for spotter reports.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NWS CR WAN/LAN system maintains information concerning each member of the CR workforce (employees). This information is managed by the NWS Central Region Headquarters (CRH) Administration Personnel. Only the Workforce Manager and the CRH Information Technology (IT) Database Administrator have access to these workforce databases.

The administrative information maintained on these databases consists of:

- Name /Position /GS Level/Series/Service Computation Date/Date of Grade/ Date of separation
- Residential information (Address, phone numbers)
- Government email addresses
- Division/Organization Name
- Regional Office Location
- Optional text field with current/relevant personnel issues, for which inclusion of PII is prohibited.

.

The information is maintained as a supplement to other employee records for purposes of tracking job vacancies, developing statistical reports, and performing other related administrative tasks

There are also local databases at the local WFO/RFC that maintain information on volunteers (members of the public) who provide them weather reports. The database holds the following information on these volunteers:

- First and last name
- Mailing address
- County
- Phone (home/cell)
- Email address
- Hours to be contacted for severe weather reports
- Possession of a rain gauge, anemometer, thermometer, snow stick, or weather station
- Brief description of location of spotter's personal residence
- Last time attended spotter class
- Community Weather Involvement Program Identification (optional) not all offices use this. It's a locally assigned number from the field office.
- Latitude / Longitude

All of this information collected on volunteers is provided voluntarily and most people who sign up do so during a community outreach training program, known as "spotter talks." Spotter talks help the public prepare for the severe weather season. A locally-assigned staff is responsible for the maintenance of this database, with occasional help from 1 to 2 other staff members for data entry. This database information is accessible for viewing by all staff members in order to make calls for severe weather information.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors			
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement

	and/or privacy policy can be found at: http://www.nws.noaa.gov/om/coop/index.htm .	
X	Yes, notice is provided by other means.	Specify how: For the workforce database, employees are notified at the time of recruitment that the collection of their information is mandatory as a condition of employment. For the Spotter Volunteers, notice is provided in the cooperative agreement form when information is collected.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the workforce database, individuals may inform HR staff, verbally or in writing, that they do not want their information added to the database; however, provision of the information is a condition of employment. All information is voluntary for Spotter Volunteers, as part of the cooperative agreement to work with NWS on providing observations. There is a Privacy Act Statement on the Web site.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For the workforce database, employees may choose not to consent to all uses (administrative, job vacancy tracking, statistical reports) by informing HR staff verbally or in writing; however, they are required to provide the information as a condition of employment. The only use of the information for volunteers is for contact purposes, which is explained in the cooperative agreement. No other uses are suggested or specified. Provision of the information and signing of the cooperative agreement implies consent to that use.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the workforce data, information is routinely updated as an employee's role or position changes. Employees cannot directly review the information, but may request to review their information and ask that it be updated, through their supervisors. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Support Division (ASD) Chief (all outside of system boundaries).

		The local manager who recruited the volunteers updates their information when notified by them to do so. Updates are not solicited but the instructions for submitting updates are in the cooperative agreement.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Any access to the local database is logged and saved.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 7/31/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

Access to the system maintaining the PII is controlled via National Active Directory. Authentication is verified by the use of CAC IDs and PIV Cards. Only employees with authority to maintain these databases are allowed access to the information.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE-18, Employee Personnel Files Not Covered By Notices of Other Agencies NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1300 – Weather, 1307-05, Chapter 300 – Personnel
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:

X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Name and contact information for volunteers, and names of employees, are in the system.
X	Quantity of PII	Provide explanation: Limited amount of PII stored.
X	Data Field Sensitivity	Provide explanation: There is an optional text field for current/relevant personnel issues for which inclusion of PII is prohibited.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Secured database managed by federal employees with limited user privileges.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer Name: Adam Van Meter Office: NWS Central Region Headquarters Phone: 816-268-3159 Email: adam.l.van meter@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: VAN METER.ADAM.L.1365874057 Digitally signed by VAN METER.ADAM.L.1365874057 Date: 2018.03.19 09:20:42 05'00' Date signed:	**Information Technology Security Officer** Name: Andrew Browne Office: NWS OCIO Phone: 301-427-9033 Email: Andrew.Browne@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.03.19 11:18:01 -04'00' Date signed:
Authorizing Official Name: Christopher Strager Office: NWS Central Region Headquarters Phone: 816-268-3130 Email: christopher.strager@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: STRAGER.CHRISTOPHER.S.1040261962 Digitally signed by STRAGER.CHRISTOPHER.S.1040261962 Date: 2018.03.19 16:53:43 04'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2018.04.04 14:14:54 -04'00' Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.

Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NWS Central Region WAN/LAN (NOAA8881)

U.S. Department of Commerce Privacy Threshold Analysis

NWS Central Region WAN/LAN (NOAA8881)

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

The NWS Central Region (CR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees, contractors, volunteers, and other individuals who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of tracking job vacancies, developing statistical reports, and performing other related administrative tasks. Weather Forecast Office (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers who provide weather reports to them.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

The statutory authority covering the collection of this data is 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce].

This is a moderate level system.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

____ Companies
____ Other business entities

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_X__ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X_ DOC employees
____ Contractors working on behalf of DOC
_X_ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NWS Central Region WAN/LAN and as a consequence of this applicability. I will perform and document a PIA for this IT system. The current PIA was approved by DOC on 6/29/2017.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Adam Van Meter

Signature of ISSO: VAN METER.ADAM.L.1365874057 Digitally signed by VAN METER.ADAM.L.1365874057 Date: 2018.03.15 10:16:05 -05'00'

Name of Information Technology Security Officer (ITSO): Andrew Browne

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2018.03.15 12:50:18 -04'00'

Name of Authorizing Official (AO): Christopher Strager

Signature of AO: STRAGER.CHRISTOPHER.S.1040261962 Digitally signed by STRAGER.CHRISTOPHER.S.1040261962 Date: 2018.03.15 10:23:41 05'00'

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2018.03.15 15:48:47 04'00'