Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, November 16, 2017 8:49 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA8880 PIA and PTA for your signature as soon as possible, thx
Attachments:	NOAA8880 PTA rev2_ITSO (1) mhg.pdf; NOAA8880 PIA 111317_ITSO (2) mhg.pdf

Signed and attached outstanding. I was getting nervous these wouldn't be there in time.

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

On Thu, Nov 16, 2017 at 8:43 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> NOAA8880 PIA and PTA for your signature asap! Please and thank you.
>
> Forwarded message
> From: **Richard Varn - NOAA Federal** <richard.varn@noaa.gov>
> Date: Thu, Nov 16, 2017 at 8:40 AM
> Subject: Re: NOAA8880 PIA and PTA for your signature as soon as possible, thx
> To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Andrew Browne NOAA Affiliate <andrew.browne@noaa.gov>
> Cc: Kyle Quashnick NOAA Federal <kyle.quashnick@noaa.gov>
>
> resigned.
>
> Thanks,
> Richard Varn
> Assistant Chief Information Officer
> National Oceanic and Atmospheric Administration
> National Weather Service
> Office of the ACIO for Weather
> SSMC2 Room 17410
> 1325 East West Highway
> Silver Spring, MD 20910 3281
> (301) 427 9018
> Mail to: richard.varn@noaa.gov

On Wed, Nov 15, 2017 at 6:21 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Hi, Rich, these docs have been on a long and winding road. They have been signed by Andrew Browne, ITSO, and Angel Corona, SO. Could you please sign and return to me, so I can have Mark Graff sign, hopefully sometime tomorrow am?
>
> DOC Privacy Office is having a conference call to review with us at 11:30 tomorrow. They have the unsigned docs but will need the signed ones to approve.
>
> tx so much! Sarah

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (b)(6) [redacted]

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service (NWS) Alaska Region
General Support System (GSS)
(NOAA8880)

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

Version Number: 01-2015

NWS Alaska Region GSS (NOAA8880)

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

Introduction: System Description

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. The servers for the NOAA8880 are in Anchorage, Alaska. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports and performing other related administrative tasks. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared outside the bureau except in law enforcement cases. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

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 (also listed for NOAA-11).
- 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 (also listed for NOAA-11).
- From DEPT-1: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309.
- 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.

- FROM DEPT-18: 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 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 with no changes that 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	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	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:					

*For government purchases

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	X*
c. Alias		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		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): N/A					

*Bank information for payroll.

**Limited to doctor's notes for a medical accommodation, extended illness where employee had to take three days or more of consecutive sick leave, and WH380 forms for FMLA, stored in the employee's personnel file which is secured in the AMD Chief's office. Access is limited to "need to know".

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

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): N/A					

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	X
g. Other system administration/audit data (specify): Standard system infrastructure and configuration data.					

Other Information (specify)
N/A

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):N/A					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): N/A					

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

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	X
Video surveillance		Electronic purchase transactions*	X
Other (specify):			

*CD435, no PII

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	X	For criminal law enforcement activities	X

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): Weather Data Dissemination			

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 Alaska Region Headquarters maintains PII concerning federal employees in the Alaska Region workforce. This information is managed by the NWS Alaska Region Headquarters Administration Personnel.
The information maintained includes:
Name
Age, Gender, date and place of birth, home contact information and email address
Position, GS Level/Series, Division/Organization Name, Regional Office Name/Location, work history
Financial information, medical information, military service information

This information is maintained to aid in maintenance of organization structures, supplementing management of employee records, and providing statistical data. The information is not shared with any third parties or unauthorized personnel.

There are also local databases at the local Weather Forecast Office/River Forecast Center (WFO/RFC), within the boundaries of the system, which 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
Telephone number (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

Non-sensitive PII in these databases is provided on a voluntary basis; volunteers sign up and provide the information during spotter talks* that the NWS conducts in preparation for the severe weather season. These databases are accessible to forecast staff so they can contact volunteers for severe weather information. The information is collected from members of the public.

*** On-site spotter training classes are conducted annually in various locations in the system area. The spotter training class is designed for people new to severe storm spotting, as well as those that need refresher training. The training is comprised of all of the information that spotters need to be effective and stay safe. Information on the trainings is posted on the applicable NWS Web site.**

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):			

*For law enforcement purposes

	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): N/A			

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 volunteer database, users are notified on the volunteer cooperative agreement form (see PAS). For the workforce database, individuals are notified by NOAA Workforce Management via email, that the collection of PII 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: Prospective volunteers may choose not provide the non-sensitive PII, by not completing the volunteer form, and thus will not become volunteers. For the workforce database, individuals may decline having their PII added to this database by providing a written request to the Chief, Administrative Division, when they start work within the office; however, this action will affect their employment status.
	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 database, the information is provided on a purely volunteer basis and users provide the PII to participate in the program which constitutes consent to use of 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. 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." For the workforce database, written consent to only particular uses of PII must be submitted to the Chief, Administrative Division. However, failure to consent to all particular uses may affect employment status.
	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: Specify how: For the volunteer database, users may request to review their data from, and send updates if needed, to their local station manager. For the workforce database, PII is routinely updated as an employee's role or position changes. Employees may request their information from, 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.
	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 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 is tracked on paper records and stored in HR controlled spaces.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 18, 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.
	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 Common Access (CAC)/Personal Identity Verification (PIV) cards. Only employees with authority to maintain this database 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: The following SORNS apply to the information on this system: NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission; DEPT-1 :Attendance, Leave, and Payroll Records of Employees and Certain Other Persons; DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies DEPT-13, Investigative and Security 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: Chapter 1300 National Weather Service Records Disposition Schedule General Records Schedule (GRS) 20, issued by National Archives and Records Administration (NARA)
	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: Individuals may be identified.
X	Quantity of PII	Provide explanation: Limited amount of PII stored.
X	Data Field Sensitivity	Provide explanation: Human resources information is stored, including DOBs.
	Context of Use	Provide explanation: Employee information only.
	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 or System Owner Name: Angel Corona Office: NWS/AR Phone: 907-271-5119 Email: angel.corona@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: Angel Corona Digitally signed by CORONA.ANGEL.M.1187109503 Date: 2017.11.15 12:53:49 -09'00' Date signed:	**Information Technology Security Officer** Name: Andrew Browne Office: NOAA OACIO Phone: 301-427-9034 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: 2017.11.15 11:38:37 -05'00' Date signed:
Authorizing Official Name: Carven Scott Office: NWS/AR Phone: 907-271-5131 Email: carven.scott@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: VARN.RICHARD.ALAN.II.1073462041 Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2017.11.16 08:38:59 -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: 2017.11.16 08:47:10 -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
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the

National Weather Service (NWS) Alaska Region
General Support System (GSS)
(NOAA8880)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Weather Service (NWS) Alaska Region General Support System (GSS) (NOAA8880)

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:

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. 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. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

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..."

__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 **NWS Alaska Region General Support System (GSS) (NOAA8880)** 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: Angel Corona Digitally signed by CORONA.ANGEL.M.1187109503 Date: 2017.11.15 12:57:02 -09'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2017.11.15 11:28:40 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: VARN.RICHARD.ALAN.II.1073462041 Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2017.11.16 08:39:46 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 2017 11 16 08 48 05 05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, November 16, 2017 9:13 AM
To:	Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO
Cc:	Mark Graff NOAA Federal
Subject:	SIGNED NOAA8880 PIA and PTA
Attachments:	NOAA8880 PIA 111317_ITSO (2) mhg.pdf; NOAA8880 PTA rev2_ITSO (1) mhg.pdf

Sorry for the delay, but here they are, for distribution to the team members. NO changes from the Word versions.

thx Sarah

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

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

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service (NWS) Alaska Region
General Support System (GSS)
(NOAA8880)

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

Version Number: 01-2015

NWS Alaska Region GSS (NOAA8880)

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

Introduction: System Description

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. The servers for the NOAA8880 are in Anchorage, Alaska. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports and performing other related administrative tasks. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared outside the bureau except in law enforcement cases. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

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 (also listed for NOAA-11).
- 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 (also listed for NOAA-11).
- From DEPT-1: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309.
- 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.

- FROM DEPT-18: 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 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 with no changes that 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	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	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:					

*For government purchases

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	X*
c. Alias		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		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): N/A					

*Bank information for payroll.

**Limited to doctor's notes for a medical accommodation, extended illness where employee had to take three days or more of consecutive sick leave, and WH380 forms for FMLA, stored in the employee's personnel file which is secured in the AMD Chief's office. Access is limited to "need to know".

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

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): N/A					

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	X
g. Other system administration/audit data (specify): Standard system infrastructure and configuration data.					

Other Information (specify)
N/A

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):N/A					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): N/A					

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

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	X
Video surveillance		Electronic purchase transactions*	X
Other (specify):			

*CD435, no PII

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	X	For criminal law enforcement activities	X

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): Weather Data Dissemination			

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 Alaska Region Headquarters maintains PII concerning federal employees in the Alaska Region workforce. This information is managed by the NWS Alaska Region Headquarters Administration Personnel.
The information maintained includes:
Name
Age, Gender, date and place of birth, home contact information and email address
Position, GS Level/Series, Division/Organization Name, Regional Office Name/Location, work history
Financial information, medical information, military service information

This information is maintained to aid in maintenance of organization structures, supplementing management of employee records, and providing statistical data. The information is not shared with any third parties or unauthorized personnel.

There are also local databases at the local Weather Forecast Office/River Forecast Center (WFO/RFC), within the boundaries of the system, which 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
Telephone number (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

Non-sensitive PII in these databases is provided on a voluntary basis; volunteers sign up and provide the information during spotter talks* that the NWS conducts in preparation for the severe weather season. These databases are accessible to forecast staff so they can contact volunteers for severe weather information. The information is collected from members of the public.

*** On-site spotter training classes are conducted annually in various locations in the system area. The spotter training class is designed for people new to severe storm spotting, as well as those that need refresher training. The training is comprised of all of the information that spotters need to be effective and stay safe. Information on the trainings is posted on the applicable NWS Web site.**

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):			

*For law enforcement purposes

	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): N/A			

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 volunteer database, users are notified on the volunteer cooperative agreement form (see PAS). For the workforce database, individuals are notified by NOAA Workforce Management via email, that the collection of PII 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: Prospective volunteers may choose not provide the non-sensitive PII, by not completing the volunteer form, and thus will not become volunteers. For the workforce database, individuals may decline having their PII added to this database by providing a written request to the Chief, Administrative Division, when they start work within the office; however, this action will affect their employment status.
	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 database, the information is provided on a purely volunteer basis and users provide the PII to participate in the program which constitutes consent to use of 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. 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." For the workforce database, written consent to only particular uses of PII must be submitted to the Chief, Administrative Division. However, failure to consent to all particular uses may affect employment status.
	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: Specify how: For the volunteer database, users may request to review their data from, and send updates if needed, to their local station manager. For the workforce database, PII is routinely updated as an employee's role or position changes. Employees may request their information from, 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.
	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 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 is tracked on paper records and stored in HR controlled spaces.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 18, 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.
	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 Common Access (CAC)/Personal Identity Verification (PIV) cards. Only employees with authority to maintain this database 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: The following SORNS apply to the information on this system: NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission; DEPT-1 :Attendance, Leave, and Payroll Records of Employees and Certain Other Persons; DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies DEPT-13, Investigative and Security 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: Chapter 1300 National Weather Service Records Disposition Schedule General Records Schedule (GRS) 20, issued by National Archives and Records Administration (NARA)
	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: Individuals may be identified.
X	Quantity of PII	Provide explanation: Limited amount of PII stored.
X	Data Field Sensitivity	Provide explanation: Human resources information is stored, including DOBs.
	Context of Use	Provide explanation: Employee information only.
	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 or System Owner Name: Angel Corona Office: NWS/AR Phone: 907-271-5119 Email: angel.corona@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: Angel Corona Digitally signed by CORONA.ANGEL.M.1187109503 Date: 2017.11.15 12:53:49 -09'00' Date signed:	**Information Technology Security Officer** Name: Andrew Browne Office: NOAA OACIO Phone: 301-427-9034 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: 2017.11.15 11:38:37 -05'00' Date signed:
Authorizing Official Name: Carven Scott Office: NWS/AR Phone: 907-271-5131 Email: carven.scott@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: VARN.RICHARD.ALAN.II.1073462041 Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2017.11.16 08:38:59 -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: 2017.11.16 08:47:10 -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
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the

National Weather Service (NWS) Alaska Region
General Support System (GSS)
(NOAA8880)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Weather Service (NWS) Alaska Region General Support System (GSS) (NOAA8880)

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:

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. 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. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

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..."

__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 **NWS Alaska Region General Support System (GSS) (NOAA8880)** 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: Angel Corona Digitally signed by CORONA.ANGEL.M.1187109503 Date: 2017.11.15 12:57:02 -09'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2017.11.15 11:28:40 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: VARN.RICHARD.ALAN.II.1073462041 Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2017.11.16 08:39:46 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 2017 11 16 08 48 05 05'00' Date: _____

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, November 16, 2017 9:18 AM
To:	Ed Kearns NOAA Federal
Cc:	Robert Swisher NOAA Federal; Sarah Brabson NOAA Federal
Subject:	Fwd: GPD Changes
Attachments:	NOAA8880 PIA 111317_ITSO (2) mhg.pdf; NOAA8880 PTA rev2_ITSO (1) mhg.pdf; NOAA8880 ARHQ FY17 Privacy SCA 20170628.xlsx; NOAA4930_PIA_20171106 mhg.pdf; NOAA4930_PTA_20170222 mhg.pdf; NOAA4930 Security Assessment Workbook FY17 Q1_.xlsx; PTA PIA Management Report 11.16.xlsx

Hi Ed,

To bring you up to speed on NOAA's Compliance Review Board (CRB) status referenced by Rob below, NOAA has two CRBs set for today. The CRB is a review by DOC of the adequacy of the PIA, SORN coverage, Privacy Controls, and PII collections generally that are within the accreditation boundaries of each FISMA system collecting PII within NOAA. Although you are welcome to attend, it is not required, and Sarah and I routinely represent the Bureau to DOC on behalf of NOAA for the CRBs.

Today's CRB will cover NOAA 4930 and NOAA 8880. For your reference, I'm attaching the PIA, PTA, and Privacy Control assessment for each system. These are the documents DOC will be reviewing and asking questions about in determining whether or not to provide SAOP concurrence, which authorizes the system, as it relates to Privacy, to receive an ATO. If approved, the PIA is publicly posted on the DOC site as the artifact of SAOP approval for that system.

We regularly send a follow up to Rob after the CRB, which we'll now direct to you after the meeting, copying Rob, letting him know if the PIAs were approved, and what, if any, were the deficiencies or program takeaways and follow up actions.

I'm also attaching a copy of the PTA/PIA Management Report, which distills the progress of PTAs and PIAs across the Bureau. Sarah maintains this spreadsheet, which we use as the primary tracking artifact for the status of PIA approval. We provide a copy of this spreadsheet in the monthly Privacy report to the ITSOs, ISSOs, AOs, and CIO/NOAA management.

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: **Robert Swisher - NOAA Federal** <robert.swisher@noaa.gov>
Date: Thu, Nov 16, 2017 at 8:27 AM
Subject: GPD Changes
To: OCIO/OPPA <ocio.ppa@noaa.gov>

Recently Doug suggested to me that the FOIA and Privacy Programs would be better suited with the Chief Data Officer Office (CDO) under Ed Kearns. It was initially thought that FOIA/Privacy would transfer to CDO immediately at the start of FY18. After some discussions with Doug and Ed, we've decided to do a half-year transition to flesh out the organic connection between FOIA/Privacy and CDO.

This half year transition is starting now. Mark and Sarah are to begin including Ed on FOIA, Privacy, Privacy Act, and Paperwork Reduction Act activities, email, decisions, and meetings. This will kick-off exploring a possible solid working relationship with CDO. We will also be including Ed in future status meetings and Compliance Review Boards with DOC OPOG as well as monthly and quarterly DOC Privacy and FOIA Calls. For now I remain Mark and Sarah's official Supervisor.

The Grand Vision at this point, subject to change, is that ultimately Mark and Sarah would transfer to CDO and all of their FOIA, Privacy, Privacy Act, and PRA functions as well. Lola would stay with GPD for Data Calls and other functions. The IT Infrastructure Program Manager and Exhibit 300 work would stay with GPD.

Rob Swisher
Director, Governance and Portfolio Division
NOAA OCIO
W 301 628 5755
(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)

(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)

(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)

(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)

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA4930 - Southwest Fisheries Science Center (SWFSC) Network

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
National Marine Fisheries Service
NOAA4930 - Southwest Fisheries Science Center (SWFSC) Network

Unique Project Identifier: 006-03-02-00-01-0511-00

Introduction: System Description

NOAA4930 SWFSC is a General Support System supporting approximately 375 users consisting of scientific, administrative, and support staff (federal employees and contractors) distributed among the California cities of La Jolla, Santa Cruz, and Monterey. There are a variety of 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 primary functions provided include:

· Network File Storage, Sharing, and Printing
· Internet Access
· NMFS Wide Area Network Connectivity
· Administrative Support Systems
· Scientific Database Access contains PII and BII.
· Scientific Statistical Data Analysis
· Geographic Information Systems
· Web Based Information Dissemination
· Telecommunications

As a requirement of the Highly Migratory Species (HMS) Fisheries Management Plan (FMP) implemented in 2005, participants (captains of permitted vessels) in HMS fisheries in the Pacific are required to submit logbook information on fishing activities. In addition, to monitor these fisheries and provide accurate catch estimates as required under the FMP and international obligations, landings information is collected and maintained. Biological and life history data are also collected and maintained to supplement stock assessment information used to assess and monitor fish stocks.

The logbook and landings data contain information that identifies fishery participants and contains information related to the business practices of those participants: Names, contact information including work and home e-mail and mailing addresses and phone numbers, vessel and processor identifiers and sales information including dates, buyers, sellers, amounts and prices.

This data is submitted to the Southwest Fisheries Science Center (SWFSC), where the information is entered into a centralized Oracle database, in an encrypted table space, that is located and maintained at the National Marine Fisheries Service (NMFS) Office of Science and Technology in Silver Spring, Maryland. The data is maintained by SWFSC staff and summarized for reporting. Summarization of the data follows established business rules for maintaining confidentiality of the summaries. Any information obtained from fewer than three persons is further aggregated and combined with other data.

Authorized users (NMFS employees and contractors) have access to the confidential logbook and landings information and access is controlled through database roles. All authorized users that access confidential information must sign a non-disclosure agreement that certifies that the user has read and understands NOAA Administrative Order on Confidentiality of Statistics (NAO 216-100). These non-disclosure agreements are maintained at SWFSC.

The categories of data inputted, stored and processed include administrative, scientific, statistical, economic, research and development, and technical.

The Southwest Highly Migratory Species database (SWHMS) contains database links to external systems that contain BII. These external database systems, including Pacific States Marine Fisheries Commission (PacFIN) a private interstate commission that warehouses state data and provides access to authorized users like us and the U.S. Coast Guard, are accessed through user accounts. We do not distribute or share this BII from our system. The information we receive from those databases is summarized to a non-confidential level and shared in non-confidential data products and reports.

Information collected and managed in the system is mandated under Magnuson-Stevens Fishery Conservation and Management Act (MSA) re-authorization (H.R. 5946--109th Congress), Pacific Highly Migratory Species Fisheries Management Plan (50 CFR Parts 223, 224 and 660) and international reporting obligations. As part of these reporting obligations, information in this system is shared case by case within NOAA, with state, local and tribal governments which provide us with logbook and landings data, and with foreign entities such as the Inter-American Tropical Tuna Commission, who in turn provide us with summaries of catch and effort data from member countries that fish for HMS in the Pacific. That is, we receive raw data from the state, local and tribal governments, and summarized data from foreign entities, and then we share the state, local and tribal summaries with the applicable foreign entities and the foreign entities' summaries with the state, local and tribal governments.

The SWFSC Operations and Management division maintains various type of PII and BII in support Center operations and the management of operational resources. The management information for the management of contracts and awards contains BII. The management of facility security that involves visitor access management, parking authorization and access control for Center personnel/staff, and general access to facilities, buildings and spaces include the maintaining of information that contains PII. The management of official government travel, both foreign and domestic, includes the maintenance of information that contains PII. Finally, the management of human resources, which includes emergency contact information, employee and labor relations/worker's compensation includes the maintenance of information that contains PII.

SWFSC also stores procurement and contract information, stored in a restricted area of the shared drive accessible only by authorized personnel.

Additional authorities:

From NOAA-6: Fish and Wildlife Act as amended (16 U.S.C. 742 et seq.) and Fishery Conservation and Management Act of 1976 as amended (16 U.S.C. 1852).

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.

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.

The impact level of 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.
_ __ 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	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify): BII: dealer identification, vessel and processor identifiers					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: SSNs are stored only in hard copy.					

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		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):					

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	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) BII - Catch amounts and sales information including dates, buyers, sellers, amounts and prices

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	X*	Email	X		
Other (specify): All of the information provided comes from the HMS permit.					

*The phone based communications are for data QA/QC only; primary data collection is not conducted via phone. The notice for this data being collected is communicated to the fishermen in the permitting process via the permit application.

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		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): Driver license readers are used by facility security personnel to register visitors.			

	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	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 technologies (single-session)		For web measurement and customization technologies (multi-session)	X
Other (specify): In compliance with federal and international mandates			

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).

(a) The information collected under the authority of the HMS FMP and international treaty requirements is used to monitor compliance with federal mandates and international reporting requirements (civil enforcement). Contact information is used to contact the submitter when insufficient or erroneous data are submitted. Information is collected from members of the public.

(b) Under requirements of the Western and Central Pacific Commission (WCPF), vessel identifiers are required to be submitted with individual fishing set information. Logbook and landings information, collected from NMFS permit holders and from state, local and tribal entities, are required to be submitted under FMPs and international reporting obligations. This information is used to ensure that all vessel owners that catch or sell HMS have a valid permit and are in compliance with the requirements of that permit. Information is collected from members of the public.

(c) PII is collected for both contractor and federal employee personnel designated to work with SWFSC. This information is collected for administration and business functions within SWFSC. Photographs that are taken are used specifically for identification badges for short term or temporary staff.

(d) For contractual purposes, the SWFSC stores procurement and contract information, stored in a restricted area of the shared drive accessible only by authorized personnel.

All information is stored on a restricted area of a shared drive accessible only by authorized personnel.

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	X		
Public			
Private sector			
Foreign governments			
Foreign entities	X		
Other (specify):			

*In case of 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: NMFS Office of Science and Technology (NOAA4020). Network connection to S&T is via an encrypted wide area network, only authorized users who have signed NDA have access to the S&T system, authentication is via username and strong password that meets DOC password requirements. The system is administered by NMFS ST6 database administration staff at NOAA4020.
	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.westcoast.fisheries.noaa.gov/fisheries/migratory_species/highly_migratory_species_logbooks.html http://www.nmfs.noaa.gov/aboutus/privacy.html	
X	Yes, notice is provided by other means.	Specify how: Notice is provided by language in the logbooks, sent to the fishermen, stating that the information must be submitted in order to maintain a Federal permit, per cited regulations. Notice is given to federal employees and contractors, in writing. 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: Individuals may decline to provide the information by not submitting the logbook, but in order to maintain a Federal fishing permit, it must be provided. Federal employees and contractors may decline to provide information in writing, but it may affect their job status and access to the facility. 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: The information collected is only used for the stated purposes of monitoring and reporting at the level required under federal and international requirements. Individuals provide consent by completing and submitting the logbook. Employees and users accessing the system are provided with the link to NOAA's privacy policy which states: "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." There is only one use for proposals in response to RFIs or RFPs.
	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	Specify how: Periodic renewal notices are sent to permit

	review/update PII/BII pertaining to them.	holders, which give them the opportunity to update their information collected. Vessel name changes and other updates can be provided on the permit renewal forms that are collected and maintained. Fishermen can also call the Permits Program Office to provide updates. All federal/contractor user information is maintained within NOAA Enterprise Messaging System (NEMS) database where users can review and update their contact information. Offerors will contact the office which issued the solicitation, with updated 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.
	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): 9/11/2017 ☐ 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.

The data reside within the boundaries of the NOAA4020 system. Only authorized personnel who have signed a NDA have access to the data. Access to the system from NOAA4930 is via an encrypted WAN connection. Local data is stored on a Windows network fileshare. Access to data stored locally is restricted to authorized personnel only via Windows AD group. Authorized users authenticate to access the data via two factor authentication (CAC card). For authorized users who are in the process of obtaining a CAC card, they access the system via username and strong password that meet the DOC password requirements. The principle of least privilege and separation of duties is implemented by SWFSC to ensure that personnel with the need to know only have access to this information. Authorized users who access the data from outside of the NOAA4930 boundary may only do so via NMFS VPN concentrators (East or West). The NMFS VPN connections are encrypted, the users must authenticate onto the VPN via two factor authentication, and the authorized user may only connect to the NMFS VPN with government furnished equipment (GFE) that is subject to all FISMA system requirements. All NMFS personnel and contractors are instructed on the confidential nature of this information. Through acknowledgement of the NOAA rules of behavior, account request agreements etc. all users are instructed to abide by all statutory and regulatory data confidentiality requirements, and will only release the data to authorized users.

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)*: Fishermen's Statistical Data COMMERCE/NOAA-6 Fishermen's Statistical Data; COMMERCE/DEPT-13, Investigative and Security Records COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies, OPM/GOVT-1, General Personnel 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: NOAA records schedule chapter 1505-11 and 1507-11
	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	Provide explanation: The vessel IDs can be used to identify a person or a business but the disclosure of this data would not be severe or catastrophic.
X	Quantity of PII	Provide explanation: PII is collected from employees and contractors.
X	Data Field Sensitivity	Provide explanation: The BII data is limited to vessel identifiers, harvest amounts, dates and locations. The value of this information is considered low. There is no sensitive PII collected from employees or contractors.
X	Context of Use	Provide explanation: The BII data would only disclose previous fisheries harvest amounts for a given geographic location. Information collected is to granted system access and to maintain employee emergency notification lists. The PII data is only used within the operations and management purposes.

X	Obligation to Protect Confidentiality	Provide explanation: The data is subject to the confidentiality protection of the Magnuson – Stevens Act, 16. U.S.C 1801, Section 402.
X	Access to and Location of PII	Provide explanation: Access to the SWHMS data is limited to fewer than 10 authorized personnel. The PII data that is used for operations and management purposes is stored on a central fileserver that is physically secured in the NOAA4930 LAN room and has access to data restricted to authorized staff only via Windows AD domain group permissions.
	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: Rich Cosgrove (ISSO) Office: NOAA NMFS SWFSC Phone: 858-546-7057 Email: Rich.Cosgrove@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: COSGROVE.RICHARD.E.III.1365890672 Dig tally signed by COSGROVE R CHARD E III 1365890672 DN: c US o U S Government ou DoD ou PKI ou OTHER cn COSGROVE RICHARD E III 1365890672 Date: 2017 11 01 16:19:28 07'00 Date signed: 11/01/2017	**Information Technology Security Officer** Name: Rick Miner (Acting) Office: NOAA NMFS OACIO Phone: 301-427-8822 Email: rick.miner@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: MINER.RICHARD.SCOTT.1398604519 Digitally signed by MINER RICHARD SCOTT 1398604519 DN: c US o U S Government ou DoD ou PKI ou OTHER cn MINER RICHARD SCOTT 1398604519 Date: 2017 11 07 10:54 56 05'00' Date signed: 11/07/2017
Authorizing Official Name: Toby Garfield (Acting for Kristen Koch) Office: NOAA NMFS SWFSC Phone: 858-546-7193 Email: toby.garfield@noaa.gov kristen.c.koch@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: GARFIELD.NEWELL.III.1228631570 Digitally signed by GARFIELD.NEWELL.III.1228631570 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GARFIELD.NEWELL.III.1228631570 Date: 2017.11.06 13:34:04 -08'00' Date signed: 11/06/2017	**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: 2017.11.13 09:21:50 -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
Southwest Fisheries Science Center - Local Area Network
NOAA4930

U.S. Department of Commerce Privacy Threshold Analysis

NOAA4930 / SWFSC LAN

Unique Project Identifier: NOAA4930

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 approximately 375 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 primary functions 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

The categories of data inputted, stored and processed include administrative, scientific, statistical, economic, research and development, and technical.

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.

____ 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): Samer Tominna_

Signature of SO: TOMINNA.SAMER.FAWZI.1231763593 Digitally signed by TOMINNA.SAMER.FAWZI.1231763593 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn TOMINNA.SAMER.FAWZI.1231763593 Date: 2017.02.14 10:47:04 -08'00' Date: 02/14/17

Name of Information Technology Security Officer (ITSO): _Bill Stearn_____

Signature of ITSO: Digitally signed by MINER.RICHARD.SCOTT.1398604519 Date: 2017.02.22 15:36:52 05'00' Date: _____

Name of Authorizing Official (AO): _Kristen Koch_____

Signature of AO: KOCH.KRISTEN.CLARE.1365892284 Digitally signed by KOCH.KRISTEN.CLARE.1365892284 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn KOCH.KRISTEN.CLARE.1365892284 Date: 2017.02.22 12:02:01 -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: 2017.02.23 16:46:55 -05'00' Date: _____

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service (NWS) Alaska Region
General Support System (GSS)
(NOAA8880)

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

Version Number: 01-2015

NWS Alaska Region GSS (NOAA8880)

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

Introduction: System Description

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. The servers for the NOAA8880 are in Anchorage, Alaska. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports and performing other related administrative tasks. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared outside the bureau except in law enforcement cases. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

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 (also listed for NOAA-11).
- 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 (also listed for NOAA-11).
- From DEPT-1: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309.
- 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.

- FROM DEPT-18: 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 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 with no changes that 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	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	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:					

*For government purchases

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	X*
c. Alias		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		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): N/A					

*Bank information for payroll.

**Limited to doctor's notes for a medical accommodation, extended illness where employee had to take three days or more of consecutive sick leave, and WH380 forms for FMLA, stored in the employee's personnel file which is secured in the AMD Chief's office. Access is limited to "need to know".

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

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): N/A					

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	X
g. Other system administration/audit data (specify): Standard system infrastructure and configuration data.					

Other Information (specify)
N/A

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):N/A					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify): N/A					

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

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	X
Video surveillance		Electronic purchase transactions*	X
Other (specify):			

*CD435, no PII

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	X	For criminal law enforcement activities	X

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): Weather Data Dissemination			

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 Alaska Region Headquarters maintains PII concerning federal employees in the Alaska Region workforce. This information is managed by the NWS Alaska Region Headquarters Administration Personnel.
The information maintained includes:
Name
Age, Gender, date and place of birth, home contact information and email address
Position, GS Level/Series, Division/Organization Name, Regional Office Name/Location, work history
Financial information, medical information, military service information

This information is maintained to aid in maintenance of organization structures, supplementing management of employee records, and providing statistical data. The information is not shared with any third parties or unauthorized personnel.

There are also local databases at the local Weather Forecast Office/River Forecast Center (WFO/RFC), within the boundaries of the system, which 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
Telephone number (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

Non-sensitive PII in these databases is provided on a voluntary basis; volunteers sign up and provide the information during spotter talks* that the NWS conducts in preparation for the severe weather season. These databases are accessible to forecast staff so they can contact volunteers for severe weather information. The information is collected from members of the public.

*** On-site spotter training classes are conducted annually in various locations in the system area. The spotter training class is designed for people new to severe storm spotting, as well as those that need refresher training. The training is comprised of all of the information that spotters need to be effective and stay safe. Information on the trainings is posted on the applicable NWS Web site.**

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):			

*For law enforcement purposes

	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): N/A			

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 volunteer database, users are notified on the volunteer cooperative agreement form (see PAS). For the workforce database, individuals are notified by NOAA Workforce Management via email, that the collection of PII 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: Prospective volunteers may choose not provide the non-sensitive PII, by not completing the volunteer form, and thus will not become volunteers. For the workforce database, individuals may decline having their PII added to this database by providing a written request to the Chief, Administrative Division, when they start work within the office; however, this action will affect their employment status.
	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 database, the information is provided on a purely volunteer basis and users provide the PII to participate in the program which constitutes consent to use of 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. 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." For the workforce database, written consent to only particular uses of PII must be submitted to the Chief, Administrative Division. However, failure to consent to all particular uses may affect employment status.
	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: Specify how: For the volunteer database, users may request to review their data from, and send updates if needed, to their local station manager. For the workforce database, PII is routinely updated as an employee's role or position changes. Employees may request their information from, 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.
	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 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 is tracked on paper records and stored in HR controlled spaces.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 18, 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.
	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 Common Access (CAC)/Personal Identity Verification (PIV) cards. Only employees with authority to maintain this database 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: The following SORNS apply to the information on this system: NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission; DEPT-1 :Attendance, Leave, and Payroll Records of Employees and Certain Other Persons; DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies DEPT-13, Investigative and Security 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: Chapter 1300 National Weather Service Records Disposition Schedule General Records Schedule (GRS) 20, issued by National Archives and Records Administration (NARA)
	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: Individuals may be identified.
X	Quantity of PII	Provide explanation: Limited amount of PII stored.
X	Data Field Sensitivity	Provide explanation: Human resources information is stored, including DOBs.
	Context of Use	Provide explanation: Employee information only.
	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 or System Owner Name: Angel Corona Office: NWS/AR Phone: 907-271-5119 Email: angel.corona@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: Angel Corona Digitally signed by CORONA.ANGEL.M.1187109503 Date: 2017.11.15 12:53:49 -09'00' Date signed:	**Information Technology Security Officer** Name: Andrew Browne Office: NOAA OACIO Phone: 301-427-9034 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: 2017.11.15 11:38:37 -05'00' Date signed:
Authorizing Official Name: Carven Scott Office: NWS/AR Phone: 907-271-5131 Email: carven.scott@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: VARN.RICHARD.ALAN.II.1073462041 Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2017.11.16 08:38:59 -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: 2017.11.16 08:47:10 -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
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the

National Weather Service (NWS) Alaska Region
General Support System (GSS)
(NOAA8880)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Weather Service (NWS) Alaska Region General Support System (GSS) (NOAA8880)

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:

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. 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. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

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..."

__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 **NWS Alaska Region General Support System (GSS) (NOAA8880)** 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: Angel Corona Digitally signed by CORONA.ANGEL.M.1187109503 Date: 2017.11.15 12:57:02 -09'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2017.11.15 11:28:40 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: VARN.RICHARD.ALAN.II.1073462041 Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2017.11.16 08:39:46 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 2017 11 16 08 48 05 05'00' Date: _____

(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)

(b)(5)

(b)(5)

(b)(5)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, November 16, 2017 1:26 PM
To:	Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO; Toland, Michael
Cc:	Mark Graff NOAA Federal; Kyle Quashnick NOAA Federal; Nikole Gallegos NOAA Federal; Andrew Browne NOAA Affiliate; Jacqueline Reinhart NOAA Federal
Subject:	NOAA8880 PTA revised per CRB
Attachments:	NOAA8880_PTA_11 16 2017_per CRB.pdf; NOAA8880(11 16 17)Final NOAA response.docx

Attached are the revised PTA and the minutes with our responses.

thx Sarah

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

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

Privacy Impact Assessment (PIA) Compliance Review Board (CRB) Meeting Minutes
NOAA National Weather Service (NWS) Alaska Region General Support System (GSS)
(NOAA8880)
November 16, 2017

Attendees:

Privacy Team
Kathy Gioffre
Mike Toland
Dorrie Ferguson

NOAA
Mark Graff
Sarah Brabson
Eric Cline (OCIO)
Kyle Quashnick
Christian Brown
Andrew Brown

Results/Conclusion:

(b)(5)

Version Number: 01-2015

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

Privacy Threshold Analysis
for the
NOAA8880 General Support System

U.S. Department of Commerce Privacy Threshold Analysis

National Weather Service/NOAA8880 General Support 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 and its purpose 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).

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. 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. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

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.

__X__ Yes. There are building entry card readers and electronic purchase transactions.

____ 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:

__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 Alaska Region General Support System (GSS) (NOAA8880)** 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: Angel Corona Digitally signed by CORONA.ANGEL.M.1187109503 Date: 2017.11.15 12:57:02 -09'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2017.11.15 11:28:40 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: VARN.RICHARD.ALAN.II.1073462041 Digitally signed by VARN.RICHARD.ALAN.II.1073462041 Date: 2017.11.16 08:39:46 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 2017 11 16 08 48 05 05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, November 16, 2017 2:57 PM
To:	Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO; Toland, Michael
Cc:	Mark Graff NOAA Federal; Renita Depp NOAA Affiliate; Jovan Lovelace NOAA Affiliate; Chi Kang; Jean Apedo NOAA Federal
Subject:	NOAA0100 response to actions from Nov 9 CRB
Attachments:	NOAA0100(11 9 17)Final_noaa response.docx; NOAA0100 PTA revised 110917.pdf

Here's the revised PTA again, now that we have OCIO concurrence on the privacy concerns. Also, the minutes with our responses.

thx Sarah

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

NOAA OCIO
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

Privacy Threshold Analysis
for the
NOAA Cyber Security Center

U.S. Department of Commerce Privacy Threshold Analysis

NOAA Cyber Security Center

Unique Project Identifier: 006-48-02-00-01-3511-00

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 and its purpose 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).

NOAA0100, the NOAA Cyber Security Center (NCSC) is a functional body of technologies, processes, and practices designed to support the NCSC mission to protect NOAA networks, computers, programs, and data from cyber-attack, damage, and unauthorized access, enabled by the strategic shift of all NOAA Federal Information System Management Act (FISMA) identified systems to practicing continuous monitoring and real-time assessments. NOAA0100 NCSC monitors NOAA security from four locations, Silver Spring, MD; Boulder, CO; Seattle, WA; and Fairmont, WV. All locations receive mirrored traffic of data feeds both incoming and outgoing for all NOAA internal offices. Silver Spring, MD; Boulder, CO; Seattle, WA; and Fairmont, WV receive two mirrored feeds. The sub-components of NOAA0100 NCSC are:

Trusted Internet Connection Access Point (TICAP)
NOAA0100 provides Trusted Internet Connection (TIC) Access Provider (TICAP) services grouped together in a physical TIC stack at each of the NOAA TICAP Locations. The physical TIC stack is comprised of the following:
a) Web Content filtering
b) Netflow
c) Packet Capture
d) Firewall Services
e) Intrusion Detection Sensor
f) Network System Information and Event Manager (SIEM) for logging, monitoring, and event correlation.
g) Network Time Protocol (NTP) Stratum 1 system
h) NCPS (Einstein 2)
i) Malware analysis/detection Tools

General Support Systems (GSS)
The NOAA0100 GSS is an interconnected set of information resources under the same direct management control that shares common functionality. It includes all inventoried hardware, software and communication mediums utilized to support the NOAA0100 mission.
System Administration Support (SAS): The SAS team works to ensure that the technologies supported by NOAA0100 are maintained. SAS ensures that all components, hardware and software, within the NOAA0100 are authorized, configured, and managed appropriately; to include patch management implementation activities via ECMO (BigFix), SCCM and RedHat Satellite.

Enterprise Support Services

Security Operations Center (SOC): The SOC monitors, detects, responds to security events and works with Security Information and Event Management (SIEM) technology and an integrated workflow to identify events of interest hidden in mountains of log data to consistently improve security intelligence capabilities. SOC provides NOAA0100 with a complete picture of security incidents and the ability to make informed security decisions. The SOC leverages existing NOAA0100 monitoring tools and intelligence to collect and accurately analyze logs produced by application, system or network devices coupled with SIEM content to detect possible incidents by employing security intelligence, workflow, repeatable processes and procedures. SOC team members work with NOAA to further understand the threat landscape, the associated risks to the organization, the ability to employ proper security controls and content to generate events of interest which are then triaged and analyzed.

NOAA Computer Incident Response Team (NCIRT): The NCIRT responds to suspected or verified information technology (IT) security incidents. This includes determining if an IT security incident has taken place; how the incident occurred; what the root cause of the incident is; and what is the scope of the incident. Once root cause and scope are determined, NCIRT establishes what countermeasures are to be deployed to defend, contain, eradicate, and recover from the incident. During an IT security incident, the NCIRT role is the authority overseeing and managing every phase of the incident response effort. The NCIRT focuses on maintaining and supporting the mission of the affected system(s) and recognizes when downtime tolerance is minimal or nonexistent. The NCIRT provides incident response (IR) for the affected site and works closely with the cooperation of System Owners and users. Cooperation between NCIRT and customers is paramount to the development of a successful containment plan, effective corrective actions and eradication, and, if warranted, a holistic and effective recovery.

Enterprise Security Solutions (ESS): The ESS team works to engineer and manage a services-oriented security architecture for NOAA and then integrating the architecture in a multi-layered approach. The ESS team members look at the NOAA enterprise environment to determine how to layer web content filtering; deploying, managing and running vulnerability scanner tools; i.e. Tenable Nessus Security Center. The ESS task of integrating enterprise services builds for NOAA a holistic security reporting and monitoring operations capability. TICAP is a functional component of ESS.
Enterprise Security Operations Center (ESOC): The DOC ESOC provides a comprehensive understanding of cybersecurity posture and threat activity across the Department. It provides Commerce executive leadership with a holistic understanding of cyber risk on a near real time basis and provides recommendations on both immediate and long-term actions which should be taken to

reduce risk. It is also responsible for facilitation of cyber intelligence information sharing and coordination of threat monitoring across the Commerce and its OUs.

The ESOC is staffed on a 24x7 basis with personnel skilled in cyber intelligence analysts, network analysis, vulnerability management, and malicious code analysts. ESOC personnel utilize multiple tools such as Security Information and Event Management (SIEM) tools, distributed security analytics capabilities, Enterprise Governance Risk and Compliance (EGRC) tools and other similar technologies which centralize and prioritize security posture and threat information. ESOC has access to multiple levels of classified systems to ensure better collection and sharing of all levels of cyber threat intelligence.

The ESOC facilitates the collection and use of information about cyber threats and vulnerabilities which could impact the cyber risk posture of DOC systems. It prioritizes sharing of actionable cyber intelligence with all appropriate network defenders and ensuring that cyber threat indicators are effectively managed and actioned within the DOC environment.

Although the ESOC is concerned with any cyber-attacks against the DOC or its OUs, it places emphasis on targeted attacks that specifically seek to infiltrate Commerce systems to steal information, disrupt operations, compromise data integrity, or use the Department as a launching pad for other attacks. Threat monitoring efforts focus on detecting Indicators of Compromise (IOC), malicious code, and patterns of malicious activity at the Internet gateway level as this generally provides the best coverage for detection without interfering with ongoing mission critical systems at the OU level. Additionally, efficiency can be gained by launching sources for unique IOCs from a single source that covers internet traffic from multiple OUs. The ESOC does not have any view into encrypted traffic supporting either Commerce activities or employee's limited personal use of the Internet. The ESOC relies on collected information from Trusted Internet Connection Access Provider (TICAP), Managed Trusted Internet Protocol Service (MTIPS), Enterprise Cybersecurity Monitoring and Operations (ECMO), OU SOCs and other sources.

Although NOAA0100 does not solicit, collect, maintain, or disseminate PII/BII, it is possible for individuals to voluntarily make such information available. Typical examples of the types of PII/BII that may become available to NOAA0100 include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc. NOAA0100 does not ask individuals to post information on its SM/W2.0 websites or applications. Information that individuals voluntarily submit as part of the investigative process is entered as evidence for the NOAA Cyber Security Center [NOAA0100].

As part of NOAA's Continuous Monitoring Operations, sensitive PII is subject to capture, maintenance, and dissemination as part of the NCSC functions. This collection includes Deep Packet Inspection (DPI) inspected within TICAP, and is consented to at the time of user login.
PII/BII from any government or non-government source may be in the system as evidence of a breach.

NOAA shares all breach incident information with DOC and United States Computer Emergency Readiness Team (US-CERT), as well as law enforcement if applicable.

The applicable authority is for civil employment, 5 U.S.C. 301.
The applicable authority for collection of PII as part of a breach investigation is the Privacy Act of 1974.

This is a HIGH impact system.

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): New incident reporting platform (NIRRA)					

____ 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.

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

All information transmitted on NOAA networks is subject to network monitoring tools, inspection, continuous monitoring operations, and collection as part of the NCSC mission, and may involve voluminous collections of sensitive PII, including SSNs. As part of a computer incident response inquiry, the NOAA0100 system may have PII data to include Social Security Numbers included in its investigation that may have been part of the original incident. For example, if an individual transmits a list of social security numbers in violation of NOAA PII policies, this original list may be part of the investigation supporting artifacts. Additionally, if a disk image or file contains PII, the retention is pertinent to the collection of incident information from the affected system.

____ 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.)*

___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.

__X__ 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

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA0100 NCSC and as a consequence of this applicability, PIA for this IT system necessary.

____ I certify the criteria implied by the questions above **do not apply** to the NOAA0100 NCSC and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO): Renita L. Depp

Signature of ISSO: DEPP.RENITA.LYNETTE.1501340789 Dig tally signed by DEPP REN TA LYNETTE 1501340789 DN c=US o=U S Government ou=DoD ou=PKI ou=CONTRACTOR cn=DEPP RENITA LYNETTE 1501340789 Date 2017 09 18 15 46 10 04'00' Date: _____

Name of Information System Owner (SO): Chi Y. Kang

Signature of SO: KANG.CHI.YUN.12462 31652 Digitally signed by KANG.CHI.YUN.1246231652 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=KANG.CHI.YUN.1246231652 Date: 2017.09.19 09:51:45 04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Jean Apedo

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: 2017 09 19 10:11:15 04 00 Date: _____

Name of Authorizing Official (AO): Douglas Perry

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=PERRY.DOUGLAS.A.1365847270 Date: 2017.09.20 15:15:42 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: 2017.09.20 16:18:07 04'00' Date: _____

Privacy Impact Assessment (PIA) Compliance Review Board (CRB) Meeting Minutes
NOAA Cyber Security Center (NCSC) (NOAA0100)
November 9, 2017

Attendees:

Privacy Team
Kathy Gioffre
Mike Toland
Dorrie Ferguson

NOAA
Mark Graff
Sarah Brabson
Joe Brust
Eric Cline (OCIO)
Christian Brown (OCIO)
Rebecca Hall-Herndon
Renita Depp
Jovan Lovelace

James Brown - NOAA Federal

From:	James Brown NOAA Federal
Sent:	Friday, November 17, 2017 7:46 AM
To:	Sarah Brabson NOAA Federal
Cc:	Mark Graff NOAA Federal
Subject:	UPDATED OAR FY18 PTA Submission NOAA3070
Attachments:	FY18 PTA OAR NOAA3070 Corrected.pdf

Hi Sarah,

Attached is the updated PTA for NOAA3070. I apologize for the oversight.

Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

On Mon, Nov 6, 2017 at 10:21 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> James, the NOAA3070 PTA is last year's (2016 signatures). Please send us a current one. Mark will start signing the others in the meantime. thx Sarah
>
> On Thu, Nov 2, 2017 at 8:12 AM, James Brown NOAA Federal <james.l.brown@noaa.gov> wrote:
>
> > Sarah,
> >
> > The Google Drive shared folder link below contains FY18 Privacy Threshold Analysis (PTA) forms for your review and the signature of the NOAA Chief Privacy Officer. Please contact me if you have any questions or concerns regarding the PTA forms.
>
> (b)(5) [redacted]
>
> FISMA System IDs
> ---
> NOAA3000/OARHQ
> NOAA3040/ARL
> NOAA3070/GFDL
> NOAA3080/GLERL
> NOAA3090/NSSL
> NOAA3100/PMEL
> NOAA3400/BNOC
> NOAA3500/ESRL
>
> Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

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

NOAA OCIO
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, November 17, 2017 9:04 AM
To:	Mark Graff NOAA Federal
Subject:	Fwd: UPDATED OAR FY18 PTA Submission NOAA3070
Attachments:	FY18 PTA OAR NOAA3070 Corrected.pdf

Mark Please sign the attached NOAA3070 PTA, which was previously sent with 2016 signatures. I asked James to remind Jeremy about 3090 but will also remind Jeremy directly.

thx Sarah

Forwarded message
From: **James Brown - NOAA Federal** <james.l.brown@noaa.gov>
Date: Fri, Nov 17, 2017 at 7:45 AM
Subject: UPDATED OAR FY18 PTA Submission NOAA3070
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
Cc: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Hi Sarah,

Attached is the updated PTA for NOAA3070. I apologize for the oversight.

Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

On Mon, Nov 6, 2017 at 10:21 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> James, the NOAA3070 PTA is last year's (2016 signatures). Please send us a current one. Mark will start signing the others in the meantime. thx Sarah
>
> On Thu, Nov 2, 2017 at 8:12 AM, James Brown NOAA Federal <james.l.brown@noaa.gov> wrote:
>
> > Sarah,
> >
> > The Google Drive shared folder link below contains FY18 Privacy Threshold Analysis (PTA) forms for your review and the signature of the NOAA Chief Privacy Officer. Please contact me if you have any questions or concerns regarding the PTA forms.
>
> (b)(5) [redacted]
>
> FISMA System IDs

NOAA3000/OARHQ
NOAA3040/ARL
NOAA3070/GFDL
NOAA3080/GLERL
NOAA3090/NSSL
NOAA3100/PMEL
NOAA3400/BNOC
NOAA3500/ESRL

Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Martin, Lisa (Federal)

From:	Martin, Lisa (Federal)
Sent:	Friday, November 17, 2017 1:50 PM
To:	Townsend, Janice; Barnes, Donald; Daniel, Tiffany; Griner, Audra; Rose, Carol; Crenshaw, Byron; Bachman, Robin J; Dwivedy, Raghawendra K; Roberson, Jeffrey (Federal); Kong, Stephen (Federal); Moulder, Pamela (Federal); Ramsey, Joe; Arnold, Josephine (Federal); Schiller, Susannah B.; Schmidt, Carolyn M.; Glenn, K. Robert; Fletcher, Catherine; Graff, Mark (Federal); Brabson, Sarah (Federal); Williams, Eric (Contractor); Swisher, Robert (Federal); Williams, Markia; Kang, Shine; Miller, Michael; Klemmer, Richard; Lynch, Heather; Jones, Stephen; Pham, Toan; Berg, Robin; Gioffre, Kathy (Federal); Ferguson, Dorrie (Federal); Pardun, John
Cc:	Toland, Michael (Federal); Murphy, Tahira (Federal)
Subject:	Privacy Council Meeting Minutes
Attachments:	Monthly PC Mtg Mins (10 24 17).docx

Good Afternoon,

Attached are the meeting minutes for the Privacy Council Telecom held on October 24, 2017.

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

Monthly Privacy Council Telecom Meeting Minutes
October 24, 2017

Hosted by: Dr. Catrina D. Purvis, Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)

Attendees:

OPOG Privacy Team

Kathy Gioffre – Chief Privacy Compliance Officer/OS Bureau Chief Privacy Officer (BCPO)
Lisa Martin – Deputy Director for Departmental Privacy Operations
Tahira Murphy – Digital Privacy Operations Analyst
Michael Toland – Departmental Freedom of Information Act (FOIA) & Privacy Act (PA) Officer

Office of the Chief Information Officer
Ja'Nelle DeVore – Director, Office of Cyber Security

Office of General Counsel
Colin Holmes – Senior Advisor to the General Counsel

Bureau Chief Privacy Officers/Points of Contact

Janice Townsend	BEA
Tiffany Daniel	BIS
Audra Griner	BIS
Raghawendra Dwivedy	Census Bureau
Jeffrey Roberson	EDA
Pamela Moulder	ESA
Joe Ramsey	ITA
Josephine Arnold	MBDA
Catherine Fletcher	NIST
Carolyn Schmidt	NIST
Sarah Brabson	NOAA
Mark Graff	NOAA
Markia Williams	NTIA
Heather Lynch	NTIS
Stephen Jones	OIG
John Pardun	USPTO

Agenda Topics Discussed

CPO's Corner

- SSN Fraud Prevention Act (P.L. 115-59)
  - This Act implements restrictions on mailing documents that include a Social Security number (SSN).
  - In order to provide an accurate report to Congress, a data call will be issued to the BCPOs. The data call will include the "inventory of forms" spreadsheet that was recently completed during the FY 2017 Federal Information Security Modernization Act (FISMA) reporting period. There will be questions added regarding the mailing of forms containing SSNs (e.g., Have hard copies of the form containing SSNs been mailed to individuals? Can the SSN be redacted from or truncated on the form prior to mailing? Has a blank form been sent to a recipient in which it must be returned with the SSN on the form?).
  - The SAOP's staff will draft initial criteria to address the Department's issuance of regulations to minimize the usage of full SSNs when mailed out or required to be received via mail. The draft will be provided to the Privacy Council for comments.
- DOC Privacy Program Plan
  - The DOC Privacy Program Plan is posted to our Privacy website under Privacy Laws, Policies and Guidance. It is also located at the Office of Privacy and Open Government's main page under Hot Topics.
  - The DOC Privacy Program Plan includes several topics, such as:
    - Continuous Monitoring Strategy (CMS) – The CMS addresses the Appendix J controls, privacy overlays, and NIST SP 800-122 controls.
    - Workforce Management – The SAOP continuously works with the Human Resources Director and Chief Information Officer (CIO) to recruit, retain, and train privacy and IT professionals, as well as enhance a current workforce planning process. In FY 2018, BCPO participation in this process will be required. More to come.
- Federal Privacy Summit
  - The Federal Privacy Summit will be held on Tuesday, December 12, 2017, at the Department of Transportation. Details will be forthcoming.

Departmental Privacy Updates

- FY 2017 SAOP FISMA Reporting
  - Thank you for your support in providing the information needed to complete the FY 2017 SAOP FISMA Report. It was a collaborative effort in which the Department was able to complete it within the limited timeframe.
  - 142 IT systems were reported as processing personally identifiable information (PII) on members of the public. 125 of these IT systems had an up-to-date PIA (88%). 119 IT systems had a PIA approved by the SAOP prior to the authorization/re-authorization, which is a great improvement compared to 22 IT systems reported in FY 2016.
  - 69 System of Records Notices (SORNs) were reported, in which 100% of the SORNs were up-to-date.
  - There were 155 PII incidents reported in FY 2017, which is a 32% decrease from FY 2016. This total includes only one (1) scanning incident per bureau.
    - In FY 2018, scanning incidents will no longer be reported as one (1) incident. Each scanning incident will be reported in an effort to ensure that the new configurations of printers are preventing the scanning and sharing of sensitive PII.

- Upcoming Training
  - On December 1, 2017, the Federal Trade Commission (FTC) and Department of Education will co-host an Education Technology Workshop to examine how the FTC's rule implementing the Children's Online Privacy Protection Act applies to schools and intersects with the Family Educational Rights and Privacy Act. This workshop is scheduled from 9:00 a.m. to 4:45 p.m. in the Constitution Center located at 400 7th Street, SW. A live webcast will be available on FTC's website.

Privacy Act Updates

- System of Records Notices (SORNs)
  - Currently, there are 106 SORNs; 14 will be abolished and 92 will be amended.
  - There are multiple levels of review, so don't wait until the last minute to amend or develop a SORN. The goal is to have 100% of SORNs published in FY 2018 in order to report 100% compliance in the FY 2018 FISMA report.
  - Bureaus/operating units (B/OUs) are required to send their draft plans for SORN updates or request an extension by November 1, 2017.
- Privacy Act Handbook
  - The Privacy Act Handbook will be updated by the summer of FY 2018.

Privacy Compliance Updates

- PIAs are required to be reviewed on an annual basis.
  - If there are no changes to the system which create new privacy risks, then the recertification form and the last SAOP approved PIA with updated signatures must be submitted to CPO@doc.gov.
  - A recertification package must be submitted at least two (2) weeks prior to a scheduled Compliance Review Board (CRB) meeting. If not received, then the assumption is that there are changes to the system which create new privacy risks and a CRB meeting is required.
  - Until further notice, PIAs must also be submitted to the Department's Office of the Chief Information Officer at DOCITSecurity@doc.gov.
- The 1st Quarter CRB schedule will be posted by October 27.

BCPO Round Robin

- USPTO – John Owens, USPTO's BCPO/CIO, is leaving the Department soon.
- NIST – Does the BCPO have to sign all IT Compliance in Acquisition Checklists or can this responsibility be delegated? SAOP/CPO answer: Yes, the BCPO must sign all of these checklists. The responsibility has already been delegated from the SAOP/CPO to the BCPO.

Next Privacy Council Meeting

- The regularly scheduled Privacy Council meeting on November 28, 2017 will be canceled.
- The next face-to-face Privacy Council meeting will be held on Wednesday, December 13, 2017.

Action Items

Action Item #	*Assigned*	*Due Date Given*	*Description*
1.	Lisa Martin	10/30/17	Issue data call for SSN Fraud Prevention Act.
2.	SAOP/CPO Staff	12/13/17	Draft initial criteria for issuance of regulations to minimize use of SSNs via mail.
3.	B/OUs	11/01/17	Send draft plan for SORN updates or request extension to Mike Toland.
4.	Kathy Gioffre	10/27/17	Post 1st quarter CRB schedule.

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, November 20, 2017 8:21 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: UPDATED OAR FY18 PTA Submission NOAA3070
Attachments:	FY18 PTA OAR NOAA3070 Corrected 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, Nov 17, 2017 at 9:03 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark Please sign the attached NOAA3070 PTA, which was previously sent with 2016 signatures. I asked James to remind Jeremy about 3090 but will also remind Jeremy directly.
>
> thx Sarah
>
> Forwarded message
> From: **James Brown - NOAA Federal** <james.l.brown@noaa.gov>
> Date: Fri, Nov 17, 2017 at 7:45 AM
> Subject: UPDATED OAR FY18 PTA Submission NOAA3070
> To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
> Cc: Mark Graff NOAA Federal <mark.graff@noaa.gov>
>
> Hi Sarah,
>
> Attached is the updated PTA for NOAA3070. I apologize for the oversight.
>
> Regards,
>
> James Brown
> Information Technology Security Officer(ITSO)
> NOAA/OAR
> 1315 East West Highway SSMC III
> Silver Spring, MD 20910
> Office: 301.734.1116

On Mon, Nov 6, 2017 at 10:21 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

James, the NOAA3070 PTA is last year's (2016 signatures). Please send us a current one. Mark will start signing the others in the meantime. thx Sarah

On Thu, Nov 2, 2017 at 8:12 AM, James Brown NOAA Federal <james.l.brown@noaa.gov> wrote:

Sarah,

The Google Drive shared folder link below contains FY18 Privacy Threshold Analysis (PTA) forms for your review and the signature of the NOAA Chief Privacy Officer. Please contact me if you have any questions or concerns regarding the PTA forms.

(b)(5)

FISMA System IDs

NOAA3000/OARHQ
NOAA3040/ARL
NOAA3070/GFDL
NOAA3080/GLERL
NOAA3090/NSSL
NOAA3100/PMEL
NOAA3400/BNOC
NOAA3500/ESRL

Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

Version Number: 01-2015

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

Privacy Threshold Analysis
For OAR GFDL (NOAA3070)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA OAR GFDL (NOAA3070)

Unique Project Identifier: NOAA3070

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 Office of Oceanic and Atmospheric Research's Geophysical Fluid Dynamics Laboratory (GFDL) is general support facility. GFDL is engaged in comprehensive long lead-time research fundamental to NOAA's mission. Scientists at GFDL develop and use mathematical models and computer simulations to improve our understanding and prediction of the behavior of the atmosphere, the oceans, and climate. GFDL scientists focus on model-building relevant for society, such as hurricane research, prediction, and seasonal forecasting, and understanding global and regional climate change.

The primary function of NOAA3070 is to provide: 1) Local Area Network and Wide Area Network services within the NOAA3070 boundary only, which includes the office space areas of the GFDL facility, 2) VoIP, 3) Wireless Internet connectivity, 4) VTC, 5) Print services, 6) Co-location or hosting services. GFDL is located in Princeton, NJ in a leased facility.

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.

____ 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 OAR GFDL (NOAA3070) 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 OAR GFDL (NOAA3070) 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 Sheldon

Signature of ISSO or SO: SHELDON.JOHN.P.1365825935 Digitally signed by SHELDON.JOHN.P.1365825935 Date: 2017.11.07 20:03:56 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): James Brown

Signature of ITSO: BROWN.JAMES.LEE.1201188217 Digitally signed by BROWN.JAMES.LEE.1201188217 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BROWN.JAMES.LEE.1201188217 Date: 2017.11.15 10:36:45 05'00' Date: _____

Name of Authorizing Official (AO): V. Ramaswamy

Signature of AO: RAMASWAMY.VENKATACHALA.DR.1365856776 Digitally signed by RAMASWAMY.VENKATACHALA.DR.1365856776 Date: 2017.11.16 15:36:50 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: 2017.11.20 08:20:09 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, November 20, 2017 12:38 PM
To:	Mark Graff NOAA Federal
Subject:	Re: UPDATED OAR FY18 PTA Submission NOAA3070
Attachments:	FY18 PTA OAR NOAA3090.pdf

Was still in the PTA/OAR folder. See attached. thx Sarah

On Mon, Nov 20, 2017 at 10:52 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> At doctor's, will find when I get back, in about an hour.
>
> Sent from my iPhone
>
> On Nov 20, 2017, at 10:23 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
>
> I don't see it
>
> If you have it handy it'd be great if you could re send. If not, I'll scour the inbox.
>
> Mark H. Graff
> FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> National Oceanic and Atmospheric Administration
> (301) 628 5658 (O)
> (b)(6) (C)
>
>
>
> On Mon, Nov 20, 2017 at 8:25 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Thanks. Do you still have 3090, or should I locate again?
> >
> > On Mon, Nov 20, 2017 at 8:20 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
> >
> > > 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, Nov 17, 2017 at 9:03 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Mark Please sign the attached NOAA3070 PTA, which was previously sent with 2016 signatures. I asked James to remind Jeremy about 3090 but will also remind Jeremy directly.

thx Sarah

Forwarded message
From: **James Brown - NOAA Federal** <james.l.brown@noaa.gov>
Date: Fri, Nov 17, 2017 at 7:45 AM
Subject: UPDATED OAR FY18 PTA Submission NOAA3070
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
Cc: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Hi Sarah,

Attached is the updated PTA for NOAA3070. I apologize for the oversight.

Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

On Mon, Nov 6, 2017 at 10:21 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

James, the NOAA3070 PTA is last year's (2016 signatures). Please send us a current one. Mark will start signing the others in the meantime. thx Sarah

On Thu, Nov 2, 2017 at 8:12 AM, James Brown NOAA Federal <james.l.brown@noaa.gov> wrote:

Sarah,

The Google Drive shared folder link below contains FY18 Privacy Threshold Analysis (PTA) forms for your review and the signature of the NOAA Chief Privacy Officer. Please contact me if you have any questions or concerns regarding the PTA forms.

(b)(5)

FISMA System IDs

NOAA3000/OARHQ
NOAA3040/ARL
NOAA3070/GFDL
NOAA3080/GLERL
NOAA3090/NSSL
NOAA3100/PMEL
NOAA3400/BNOC
NOAA3500/ESRL

Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, November 20, 2017 1:11 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: UPDATED OAR FY18 PTA Submission NOAA3070
Attachments:	FY18 PTA OAR NOAA3090 mhg.pdf

Great! 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, Nov 20, 2017 at 12:38 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Was still in the PTA/OAR folder. See attached. thx Sarah
>
> On Mon, Nov 20, 2017 at 10:52 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > At doctor's, will find when I get back, in about an hour.
> >
> > Sent from my iPhone
> >
> > On Nov 20, 2017, at 10:23 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
> >
> > I don't see it
> >
> > If you have it handy it'd be great if you could re send. If not, I'll scour the inbox.
> >
> > Mark H. Graff
> > FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> > National Oceanic and Atmospheric Administration
> > (301) 628 5658 (O)
> > (b)(6) (C)
> >
> >

On Mon, Nov 20, 2017 at 8:25 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Thanks. Do you still have 3090, or should I locate again?

On Mon, Nov 20, 2017 at 8:20 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

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, Nov 17, 2017 at 9:03 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Mark Please sign the attached NOAA3070 PTA, which was previously sent with 2016 signatures. I asked James to remind Jeremy about 3090 but will also remind Jeremy directly.

thx Sarah

Forwarded message
From: **James Brown - NOAA Federal** <james.l.brown@noaa.gov>
Date: Fri, Nov 17, 2017 at 7:45 AM
Subject: UPDATED OAR FY18 PTA Submission NOAA3070
To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>
Cc: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Hi Sarah,

Attached is the updated PTA for NOAA3070. I apologize for the oversight.

Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

On Mon, Nov 6, 2017 at 10:21 AM, Sarah Brabson NOAA Federal

<sarah.brabson@noaa.gov> wrote:

James, the NOAA3070 PTA is last year's (2016 signatures). Please send us a current one. Mark will start signing the others in the meantime. thx Sarah

On Thu, Nov 2, 2017 at 8:12 AM, James Brown NOAA Federal <james.l.brown@noaa.gov> wrote:

Sarah,

The Google Drive shared folder link below contains FY18 Privacy Threshold Analysis (PTA) forms for your review and the signature of the NOAA Chief Privacy Officer. Please contact me if you have any questions or concerns regarding the PTA forms.

(b)(5)

FISMA System IDs

NOAA3000/OARHQ
NOAA3040/ARL
NOAA3070/GFDL
NOAA3080/GLERL
NOAA3090/NSSL
NOAA3100/PMEL
NOAA3400/BNOC
NOAA3500/ESRL

Regards,

James Brown
Information Technology Security Officer(ITSO)
NOAA/OAR
1315 East West Highway SSMC III
Silver Spring, MD 20910
Office: 301.734.1116

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

Version Number: 01-2015

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

Privacy Threshold Analysis
For OAR NSSL (NOAA3090)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA OAR NSSL (NOAA3090)

Unique Project Identifier: NOAA3090

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 Office of Oceanic and Atmospheric Research's National Severe Storms Laboratory (NSSL) conducts research for the accurate and timely forecast and warnings of hazardous weather events (e.g. blizzards, ice storms, flash floods, tornadoes, lightning, etc). NSSL accomplishes this mission, in partnership with the National Weather Service (NWS), through a balanced program of research to advance the understanding of weather processes, research to improve forecasting and warning techniques, development of operational applications, and transfer of understanding, techniques, and applications to the NWS and other public and private sector agencies. NSSL Information Technology provides a general support system for their employees, contractors, and associates within their facility in Norman, Oklahoma.

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.

____ 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 OAR NSSL (NOAA3090) 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 OAR NSSL (NOAA3090) 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): Lans Rothfusz

Signature of ISSO or SO: ROTHFUSZ.LANS.P.1365872240 Digitally signed by ROTHFUSZ.LANS.P.1365872240 Date: 2017.10.23 12:38:42 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): James Brown

Signature of ITSO: BROWN.JAMES.LEE.1201188217 Digitally signed by BROWN.JAMES.LEE.1201188217 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BROWN.JAMES.LEE.1201188217 Date: 2017.10.24 10:58:48 -04'00' Date: _____

Name of Authorizing Official (AO): Steven Koch

Signature of AO: KOCH.STEVEN.E.DR.1365855532 Digitally signed by KOCH.STEVEN.E.DR.1365855532 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn KOCH.STEVEN.E.DR.1365855532 Date: 2017.10.23 15:33:46 -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: 2017.11.20 13:10:16 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, November 20, 2017 1:25 PM
To:	James Brown NOAA Federal
Cc:	Jeremy Warren; Mark Graff NOAA Federal
Subject:	NOAA3070 and NOAA3090 PIAs signed by Mark Graff
Attachments:	FY18 PTA OAR NOAA3090 mhg.pdf; FY18 PTA OAR NOAA3070 Corrected mhg.pdf

Please see the attached. We're good for another year!

thx Sarah

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

NOAA OCIO
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

Privacy Threshold Analysis
For OAR GFDL (NOAA3070)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA OAR GFDL (NOAA3070)

Unique Project Identifier: NOAA3070

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 Office of Oceanic and Atmospheric Research's Geophysical Fluid Dynamics Laboratory (GFDL) is general support facility. GFDL is engaged in comprehensive long lead-time research fundamental to NOAA's mission. Scientists at GFDL develop and use mathematical models and computer simulations to improve our understanding and prediction of the behavior of the atmosphere, the oceans, and climate. GFDL scientists focus on model-building relevant for society, such as hurricane research, prediction, and seasonal forecasting, and understanding global and regional climate change.

The primary function of NOAA3070 is to provide: 1) Local Area Network and Wide Area Network services within the NOAA3070 boundary only, which includes the office space areas of the GFDL facility, 2) VoIP, 3) Wireless Internet connectivity, 4) VTC, 5) Print services, 6) Co-location or hosting services. GFDL is located in Princeton, NJ in a leased facility.

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.

____ 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 OAR GFDL (NOAA3070) 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 OAR GFDL (NOAA3070) 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 Sheldon

Signature of ISSO or SO: SHELDON.JOHN.P.1365825935 Digitally signed by SHELDON.JOHN.P.1365825935 Date: 2017.11.07 20:03:56 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): James Brown

Signature of ITSO: BROWN.JAMES.LEE.1201188217 Digitally signed by BROWN.JAMES.LEE.1201188217 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BROWN.JAMES.LEE.1201188217 Date: 2017.11.15 10:36:45 05'00' Date: _____

Name of Authorizing Official (AO): V. Ramaswamy

Signature of AO: RAMASWAMY.VENKATACHALA.DR.1365856776 Digitally signed by RAMASWAMY.VENKATACHALA.DR.1365856776 Date: 2017.11.16 15:36:50 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: 2017.11.20 08:20:09 -05'00' Date: _____

Version Number: 01-2015

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

Privacy Threshold Analysis
For OAR NSSL (NOAA3090)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA OAR NSSL (NOAA3090)

Unique Project Identifier: NOAA3090

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 Office of Oceanic and Atmospheric Research's National Severe Storms Laboratory (NSSL) conducts research for the accurate and timely forecast and warnings of hazardous weather events (e.g. blizzards, ice storms, flash floods, tornadoes, lightning, etc). NSSL accomplishes this mission, in partnership with the National Weather Service (NWS), through a balanced program of research to advance the understanding of weather processes, research to improve forecasting and warning techniques, development of operational applications, and transfer of understanding, techniques, and applications to the NWS and other public and private sector agencies. NSSL Information Technology provides a general support system for their employees, contractors, and associates within their facility in Norman, Oklahoma.

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.

____ 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 OAR NSSL (NOAA3090) 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 OAR NSSL (NOAA3090) 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): Lans Rothfusz

Signature of ISSO or SO: ROTHFUSZ.LANS.P.1365872240 Digitally signed by ROTHFUSZ.LANS.P.1365872240 Date: 2017.10.23 12:38:42 -05'00' Date: _____

Name of Information Technology Security Officer (ITSO): James Brown

Signature of ITSO: BROWN.JAMES.LEE.1201188217 Digitally signed by BROWN.JAMES.LEE.1201188217 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BROWN.JAMES.LEE.1201188217 Date: 2017.10.24 10:58:48 -04'00' Date: _____

Name of Authorizing Official (AO): Steven Koch

Signature of AO: KOCH.STEVEN.E.DR.1365855532 Digitally signed by KOCH.STEVEN.E.DR.1365855532 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn KOCH.STEVEN.E.DR.1365855532 Date: 2017.10.23 15:33:46 -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: 2017.11.20 13:10:16 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, November 20, 2017 3:40 PM
To:	Mark Graff NOAA Federal
Subject:	Fwd: Revised NOAA4020 PTA per Mark's comments
Attachments:	NOAA4020 PTA 2017 revised description_nc_rm.pdf

Mark, for your signature. thx

Forwarded message
From: **Tahir Ismail - NOAA Affiliate** <tahir.ismail@noaa.gov>
Date: Mon, Nov 20, 2017 at 3:35 PM
Subject: Fwd: Revised NOAA4020 PTA per Mark's comments
To: Sarah Brabson <sarah.brabson@noaa.gov>
Cc: Glen Taylor NOAA Federal <glen.taylor@noaa.gov>, "NMFS.InfoSec@noaa.gov" <NMFS.InfoSec@noaa.gov>

Sarah,

Attached, please find the signed PTA.

Thanks,

Tahir

Forwarded message
From: **Rick Miner - NOAA Federal** <rick.miner@noaa.gov>
Date: Mon, Nov 20, 2017 at 3:14 PM
Subject: Re: Revised NOAA4020 PTA per Mark's comments
To: Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov>

Signed

Rick Miner, CISSP-ISSAP, CCSP
IT Security Engineer
NOAA Fisheries
U.S. Department of Commerce
Office: 301.427.8822
Mobile (b)(6)
rick.miner@noaa.gov
www.fisheries.noaa.gov

On Thu, Nov 16, 2017 at 9:46 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

> Rick,
>
> Please sign the NOAA4020 PTA.
>
> Thanks,
>
> Tahir
>
> Forwarded message
> From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
> Date: Thu, Nov 16, 2017 at 8:55 AM
> Subject: Fwd: Revised NOAA4020 PTA per Mark's comments
> To: Tahir Ismail <tahir.ismail@noaa.gov>, "NMFS.InfoSec@noaa.gov" <NMFS.InfoSec@noaa.gov>
> Cc: Glen Taylor <Glen.Taylor@noaa.gov>
>
> Tahir, please have Rick sign and then send to me. thx Sarah
>
> Forwarded message
> From: **Glen Taylor - NOAA Federal** <glen.taylor@noaa.gov>
> Date: Wed, Nov 15, 2017 at 4:36 PM
> Subject: Re: Revised NOAA4020 PTA per Mark's comments
> To: Tahir Ismail <tahir.ismail@noaa.gov>, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Mohamed Mughal NOAA Federal <mohamed.mughal@noaa.gov>
> Cc: Scott Sauri <Scott.Sauri@noaa.gov>, "NMFS.InfoSec@noaa.gov" <NMFS.InfoSec@noaa.gov>, Franklin Schwing NOAA Federal <franklin.schwing@noaa.gov>
>
> Tahir and Sarah,
>
> Please find the updated PTA with the new description attached.
>
> Mohamed, please also substitute this system description for the one in CSAM.
>
> Thanks,
> Glen
>
> On Wed, Nov 15, 2017 at 12:37 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Thanks, Glen!
> >
> > On Wed, Nov 15, 2017 at 12:36 PM, Glen Taylor NOAA Federal <glen.taylor@noaa.gov> wrote:
> >
> > > Hi Sarah,
> > >
> > > The PTA looks fine to me. I'll start the signatures again on our side.
> > >
> > > Thanks,
> > > Glen

On Wed, Nov 15, 2017 at 7:55 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Glen, is this okay with you? Can you start signatures? thx

On Tue, Nov 14, 2017 at 2:21 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Mark had said we should use the system description from the PIA, for the PTA also.

So I kept the one paragraph in the PTA system description and copied in the application descriptions from the PIA.

And in the PIA, I added the paragraph from the PTA as an intro to the application descriptions (see attached also). We still can't finalize this PIA till I get the rest of the privacy act statements posted but here is the version with the paragraph added.

If the PTA looks okay to you, please start signatures.And please also substitute this system description for the one in CSAM.

thx Sarah

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

Glen C. Taylor
IT Operations Branch Chief
Science Information Division (F/ST6)
Office of Science and Technology
NOAA National Marine Fisheries Service
1315 East West Highway, Rm 12326
Silver Spring, MD 20910
Phone: 301 427 8183 | Fax: 301 713 4137
Email: Glen.Taylor@noaa.gov

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

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

Glen C. Taylor
IT Operations Branch Chief
Science Information Division (F/ST6)
Office of Science and Technology
NOAA National Marine Fisheries Service
1315 East West Highway, Rm 12326
Silver Spring, MD 20910
Phone: 301 427 8183 | Fax: 301 713 4137
Email: Glen.Taylor@noaa.gov

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)

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

NOAA OCIO
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)

Purvis, Catrina (Federal)

Subject:	NOAA CRB meetings for NOAA5011; and NOA8873
Location:	Open Office 52017 (SMC) Md Conf Rm Dial in number: (b)(6) (b)(6)
Start:	Thursday, November 30, 2017 9:30 AM
End:	Thursday, November 30, 2017 10:30 AM
Recurrence:	(none)
Meeting Status:	Not yet responsed
Organizer:	Purvis, Catrina (Federal)
Attachments:	NOAA5011 PIA 102617_NCEI coAO signed mhg.pdf; NOAA5011_PTA_09 05 2017 ITSO signed mhg.pdf; NOAA8873_PIA_FY18 ITSO_AO_ISSO signed mhg.pdf; NOAA8873_PTA_July2017 AO mhg.pdf

Rescheduled due to PIAs/PTAs being in possession.

Mark/Sarah,

Please provide the signed PIA/PTAs for the system identified above by 10am Tuesday, December 5 to avoid cancellation of this meetings.

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) 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
National Oceanic and Atmospheric Administration (NOAA)

Privacy Impact Assessment
for the
National Geophysical Data Center (NGDC) Data Archive Management and User System
NOAA5011

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 / Data Archive Management and User System

Unique Project Identifier: NOAA IT Infrastructure investment code 006-000351100

Introduction: System Description

NOAA's National Centers for Environmental Information (NCEI) are responsible for hosting and providing access to one of the most significant archives on earth, with comprehensive oceanic, atmospheric, and geophysical data. From the depths of the ocean to the surface of the sun and from million-year-old tree rings to near real-time satellite images, NCEI is the Nation's leading authority for environmental information. By preserving, stewarding, and maximizing the utility of the Federal government's billion-dollar investment in high-quality environmental data, NCEI remains committed to providing products and services to private industry and businesses, local to international governments, academia, as well as the general public.

The demand for high-value environmental data and information has dramatically increased in recent years. NCEI is designed to improve NOAA's ability to meet that demand. The Consolidated and Further Continuing Appropriations Act, 2015, Public Law 113-235, approved the consolidation of NOAA's existing three National Data Centers: the National Climatic Data Center, the National Geophysical Data Center, and the National Oceanographic Data Center into the National Centers for Environmental Information. NCEI has employees in four major locations: Asheville, NC, Boulder, CO, Silver Spring, MD, and Stennis Space Center, MS. NCEI located in Boulder, CO comprises the NOAA5011 system.

NCEI-CO conducts a data and data-information service in all scientific and technical areas involving solid earth geophysics, marine geology and geophysics, glaciology, space environment, solar activity and the other areas of solar-terrestrial physics. The Center prepares systematic and special data products and performs data-related research studies to enhance the utility of the service to the users. It performs all functions related to data acquisition, archiving, retrieval, indexing, quality assessments, evaluation, synthesis, dissemination, and publication. This information is shared with collaborators from numerous internal and external organizations.

In order to better fulfill its mission, NCEI-CO receives data from other NOAA groups, other federal government agencies such as NASA, the U.S. Air Force, the US Geological Survey; federally funded research institutions such as the National Center for Atmospheric Research (NCAR), and the Woods Hole Oceanographic Institution; universities such as the University of Colorado - National Snow and Ice Data Center (NSIDC), and the Ocean Drilling Program at Texas A&M University; state agencies such as the Alaska Department of Natural Resources, California Department of Water Resources; and intergovernmental entities such as the European Space Agency, and the Australian Surveying and Land Information Group (AUSLIG).

PII and BII information contained within the NOAA5011 system boundary provide the System Owner, ISSO, and administrators with the identity and contact information of all authorized

users of the system. This information is used for data sharing, to reset passwords, notify users of outages, and support NCEI-CO COOP operations.

Typical Transactions on the NOAA5011 System

Customer: A typical Web-based transaction on the NOAA5011 system involves a customer browsing NCEI data holdings and then downloading data based on that browse activity or in instances where the data to be downloaded is too large to acquire in a single session the customer fills out an online form the form contains a link to the NOAA5011 Web privacy policy (http://www.ngdc.noaa.gov/ngdcinfo/privacy.html). Also see section 7.1. On the site where all the services are listed, there is also a privacy act statement: https://www.ngdc.noaa.gov/privacy-act-statement-data-requestors.pdf.

Data Provider: Data providers and principal investigators may be U.S. Federal, state and local governments, for-profit businesses, non-profit organizations, and academia, their non-U.S. equivalents, and intergovernmental entities. These organizations have signed Data Submission Agreements, which have Privacy Act Statements, to provide NOAA with raw data and derived products. The data can be provided in analog or digital form, and can be submitted to NGDC via the Internet, or shipped to NGDC (tape, disk, etc.).

NOAA Employee or Contractor: Employee and contractor work-related data is collected in paper format, and includes: name, job title, work address, work and home email address, and work and home telephone numbers.

Purposes for Collection of PII and BII

Customer provided PII: Customer contact information includes: Name, Company or Organization, Company or Organization Address, Company or Organization Email Address, and Company or Organization Phone Number. This information is used to provide the data in compressed format for later retrieval by the user/customer. In some cases, customer provided data is used to manage account information for access to web applications.

Data Providers' PII/BII: Data providers' and principal investigators' name, email, and physical address are recorded as part of the metadata for the submitted data set, and for contact purposes when needed. Information on the data providers and principal investigators is necessary in order to contact an individual in the event of a problem during the archiving process. Such information is also necessary to identify the sources of data submitted to NCEI, especially for properly crediting the providers and principal investigators on the individual holdings in the archive. Data providers and principal investigators may be U.S. Federal, state and local governments, for-profit businesses, non-profit organizations, and academia, their non-U.S. equivalents, and intergovernmental entities.

The IP address of the computer submitting data using online forms is collected for security purposes. In the event that NCEI receives a malicious file it will be necessary to have an audit trail showing what IP address was used to make the submission. The IP address will be recorded

for possible security issue investigation and statistics related to the geographical distribution of data providers.

Work related PII data:

- Names, work addresses and work email addresses collected from employees and contractors are used to manage account information for access control to systems and web applications.
- Names and work email addresses of employees and contractors are used to direct the public to appropriate personnel within the organization.
- Names, work and home contact information are collected for emergency, disaster recovery, and continuity of operations, employee and contractor.
- Employee job titles and salaries are collected for Workforce Management purposes.
- Data providers' and principal investigators' name, email, and physical address will be recorded as part of the metadata for the submitted data set, and for contact purposes when needed.

Contractor roles are based on qualifications and training, with the exception they have do not have supervisory roles.

NOAA5011 Information Sharing.
NOAA5011 does not share any of the customer information provided with agencies outside of the Department of Commerce. NOAA5011 does not distribute the information collected from www.ngdc.noaa.gov except for information or data explicitly submitted for redistribution; for example, scientific data, *including metadata*, submitted to NESDIS Data Centers for archiving are made available to customers and other public entities, with notice of such possible distribution given on the data submitters' agreement form (see Section 7.1).

Legal Authority.
5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. 1512, Powers and duties of Department also applies: FROM NOAA011.

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.

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.

NOAA5011 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*		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		d. Telephone Number	X	g. Salary	X

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 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):					

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		Email	X		
Other (specify): Email and online apply to data subscribers, and submitters. NOAA5011 requires the use of cryptographic mechanisms by those sending data to the system whenever possible, to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. The mechanisms [for web based transmissions, including web-based forms] include SSL/TLS encryption.					

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	X
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		For criminal law enforcement activities	X
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)	X	For web measurement and customization technologies (multi-session)	
Other (specify):Continuity of Operations (COOP)			

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).

Purposes for Collection of PII and BII

Customer provided PII: Customer contact information includes: Name, Company or Organization, Company or Organization Address, Company or Organization Email Address, and Company or Organization Phone Number. This information is used by NOAA5011 data administrator staff to provide the data in compressed format for later retrieval by the user/customer. In some cases, customer provided data is used by NOAA5011 data administrator staff to manage account information for customer access to web applications (members of the public).

Data Providers PII/BII: As part of the signed Data Submission Agreements, data providers' and principal investigators' name, email, and physical address are recorded as part of the metadata for the submitted data set, and for contact purposes when needed. Information on the data providers and principal investigators is necessary in order for a system administrator to contact an individual in the event of a problem during the archiving process. Such information is also necessary to identify the sources of data submitted to NCEI, especially for properly crediting the providers and principal investigators on the individual holdings in the archive. Data providers and principal investigators may be U.S. Federal, state and local governments, for-profit businesses, non-profit organizations, and academia, their non-U.S. equivalents, and intergovernmental entities.

The IP address of the computer submitting data using online forms is collected for security purposes. In the event that NCEI receives a malicious file it will be necessary to have an audit trail showing what IP address was used to make the submission. The IP address will be recorded for possible security issue investigation and statistics related to the geographical distribution of data providers (members of the public). Notification for collection of IP address is made in the NOAA5011 Privacy Policy. This is also addressed in Section 7.1.

Work related PII data:

- Names, addresses, and email addresses collected from employees and contractors are used to manage account information for access control to systems and web applications.
- Names and work email addresses of employees and contractors are used to direct the public to appropriate personnel within the organization.
- For emergency, disaster recovery, and continuity of operations, employee and contractor names, work and home emails and work and home telephone numbers are collected.
- Employee job titles and salaries are collected for Workforce Management purposes.

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	X		
Public	X		
Private sector	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.

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: • NCDC LAN/NOAA5009 and NODC LAN/NOAA5010. ○ Physical and logical access to PII/BII is restricted to authorized personnel only. ○ Encryption is used for PII/BII in transit. ○ Backup tapes containing PII/BII are transported in locked containers. ○ Media is sanitized prior to disposal or reuse. • NESDIS HQ LAN (NOAA5006). ○ Physical and logical access to PII/BII is restricted to authorized personnel only. ○ Encryption is used for PII/BII in transit. Where a higher level of integrity and/or confidentiality is required, NOAA5011 employs cryptographic mechanisms, such as SSH, HTTPS, or FTPS. Secure Sockets Layer or Transport Layer Security (SSL/TLS) is used to protect the confidentiality of data transmission when authentication is required.
	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.ngdc.noaa.gov/wiki/images/f/f4/NOAA_Sub_Agreement.docx (link in Data Submission User Agreement Executive Summary, Page ii, after cover page and approval page); and for subscribers: https://www.ngdc.noaa.gov/privacy-act-statement-data-requestors.pdf. For continuity of operations, there is a PAS on the document enclosed with this PIA. .	
X	Yes, notice is provided by other means.	Specify how: Notice is provided to the customers via the NOAA5011 Web Privacy Policy (www.ngdc.noaa.gov/ngdcinfo/privacy.html) and the NOAA Privacy Policy (http://www.noaa.gov/privacy.html). This includes notice of collection of IP address. Data providers and principal investigators are notified in the **Data Submission User Agreement** that their information will be stored in the metadata associated with their data. This includes notice regarding redistribution of research data (in the Executive Summary**).** Information collected for employee/contractor emergency contact, and disaster recovery/continuity of operations is requested in writing. NOAA5011 distributes a request – via a paper form - for NCEI Emergency Contact information to each NOAA5011 staff member (federal and contractor). NOAA5011 Supervisors receive a paper copy: "NCEI Emergency Listing," for their division, for COOP and other emergency contact. This Supervisor's NCEI Emergency Listing paper form is marked: "Confidential." Information collected for account management is requested in writing or via email by the user's supervisor in the request for an account on the information system.
	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: Only contact information, in the form selected by the customer or data provider is requested. The customer will provide this information only if he/she wants certain products and information. As stated in the NGDC privacy policy (http://www.ngdc.noaa.gov/ngdcinfo/privacy.html), stating that any information to NGDC is voluntary. Employees filling out forms may decline to provide PII /BII for emergency contact and disaster recovery. However, in choosing

		to do so, they will not be contacted in the event of an emergency or COOP situation.
	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 NOAA5011 web-site, Privacy Policy page (http://www.ngdc.noaa.gov/ngdcinfo/privacy.html) details how customer and data-provider information may be used. *By checking products and notifications desired, the customer consents to the use of his/her contact information for the purpose of providing those items.* Data providers and principal investigators consent to the collection and publication of their data when they submit data for archiving – as stated in the NOAA5011 signed Data Submission Agreements. Employee and contractor information is required for emergency notifications. Employees and contractors are informed of the use of their data as stated in the Emergency Contact forms the employee fills out and updates.
	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: Instructions for updating contact information fields are provided in the forms the customer fills out. Data providers receive a copy of the NOAA5011 Data Submission Agreement they have signed, and have the opportunity to submit updates pertaining to the BII, by email to the database administrator, as will be stated in the revised agreement. The employee fills out and updates the Emergency Contact form at least annually.
	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: Access or attempted access to PII/BII on the system 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): 01/18/2017 ☐ 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.
	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 NOAA5011 output devices (monitors, printers and audio devices) are operated within NOAA5011 controlled spaces. Critical consoles for NOAA5011 servers are located in keycard access controlled computer rooms. NOAA5011 positions monitors away from windows whenever possible.

- Encryption is used for PII/BII in electronic transit.
- Backup tapes containing PII/BII are transported in locked containers.
- Media is sanitized prior to disposal or reuse.
- A shredder has been made available to NOAA5011 personnel for destruction of sensitive documents.

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"; Commerce/Department 18 - "Employees Personnel Files Not Covered by Notices of Other Agencies" Commerce/Department 13, Investigative and Security 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: GRS 1: Civilian Personnel Records, GRS 3.1 General Technology Management Records, Item 040: Information technology oversight and compliance records, GRS 3.2 Information Systems Security Record, Items 030, 031: System access records, NOAA Records Schedules 1406-01: In Situ and Remotely Sensed Environmental Data; 1406-02, Order Processing Information Systems, 1406-03, Metadata Management Database
	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: There is little PII and it is not sensitive.
X	Data Field Sensitivity	Provide explanation: There is no sensitive information.
X	Context of Use	Provide explanation: Information is not used in sensitive context.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access to PII is described above in Section 8.2. Physical and logical access restrictions are in place as prescribed in NIST SP 800-53.
	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: Privacy Act Statement for data requestors.
	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: Marcus O. Ertle, ISSO Office: NOAA/NESDIS/National Center for Environmental Information (NCEI) Phone: 303-497-6139 Email: 303-589-2169 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: ERTLE.MARCUS.O.1365880871 Digitally signed by ERTLE.MARCUS.O.1365880871 DN: c=US o=U.S. Government ou=DoD ou=PKI ou=OTHER cn=ERTLE.MARCUS.O.1365880871 Date: 2017.10.24 11:01:40 -06'00' Date signed: 10/24/2017	**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 DN: c=US o=U.S. Government ou=DoD ou=PKI ou=OTHER cn=DEFRANCESCO.NANCY.A.1377370917 Date: 2017.10.24 14:12:37 -04'00' Date signed: 10/24/2017
Authorizing Official Name: Margarita Gregg, co-AO Office: NOAA/NESDIS/NCEI Phone: 828-271-4848 Email: Margarita.Gregg@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: GREGG.MARGARITA.ELENA.1365899017 Digitally signed by GREGG.MARGARITA.ELENA.1365899017 DN: c=US o=U.S. Government ou=DoD ou=PKI ou=OTHER cn=GREGG.MARGARITA.ELENA.1365899017 Date: 2017.10.26 09:12:54 -04'00' Date signed: 10-26-2017	**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: 2017.10.26 13:41:58 -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: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Data Archive Management and User System
NOAA5011

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Data Archive Management and User System

Unique Project Identifier: NOAA5011

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 and its purpose 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).

NOAA's National Centers for Environmental Information (NCEI) are responsible for hosting and providing access to one of the most significant archives on earth, with comprehensive oceanic, atmospheric, and geophysical data. From the depths of the ocean to the surface of the sun and from million-year-old tree rings to near real-time satellite images, NCEI is the Nation's leading authority for environmental information. By preserving, stewarding, and maximizing the utility of the Federal government's billion-dollar investment in high-quality environmental data, NCEI remains committed to providing products and services to private industry and businesses, local to international governments, academia, as well as the general public.

The demand for high-value environmental data and information has dramatically increased in recent years. NCEI is designed to improve NOAA's ability to meet that demand. The Consolidated and Further Continuing Appropriations Act, 2015, Public Law 113-235, approved the consolidation of NOAA's existing three National Data Centers: the National Climatic Data Center, the National Geophysical Data Center, and the National Oceanographic Data Center into the National Centers for Environmental Information. NCEI has employees in four major locations: Asheville, NC, Boulder, CO, Silver Spring, MD, and Stennis Space Center, MS. NCEI located in Boulder, CO comprises the NOAA5011 system.

NCEI-CO conducts a data and data-information service in all scientific and technical areas involving solid earth geophysics, marine geology and geophysics, glaciology, space environment, solar activity and the other areas of solar-terrestrial physics. The Center prepares systematic and special data products and performs data-related research studies to enhance the

utility of the service to the users. It performs all functions related to data acquisition, archiving, retrieval, indexing, quality assessments, evaluation, synthesis, dissemination, and publication.

This information is shared with collaborators from numerous internal and external organizations.

In order to better fulfill its mission, NCEI-CO receives data from other NOAA groups, other federal government agencies such as NASA, the U.S. Air Force, the US Geological Survey; federally funded research institutions such as the National Center for Atmospheric Research (NCAR), and the Woods Hole Oceanographic Institution; universities such as the University of Colorado - National Snow and Ice Data Center (NSIDC), and the Ocean Drilling Program at Texas A&M University; state agencies such as the Alaska Department of Natural Resources, California Department of Water Resources; and intergovernmental entities such as the European Space Agency, and the Australian Surveying and Land Information Group (AUSLIG).

PII and BII information contained within the NOAA5011 system boundary provide the System Owner, ISSO, and administrators with the identity and contact information of all authorized users of the system. This information is used for data sharing, to reset passwords, notify users of outages, and support NCEI-CO COOP operations.

The Security Boundary of the NCEI-CO data center is contained by an IP address scheme that is unique to the NCEI-CO network and separated from the DSRC network backbone by a Juniper SRX-5600 firewall.

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.)."

__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 Data Archive Management and User System (NOAA5011) 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 Data Archive Management and User System (NOAA5011) 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):

Marcus O. Ertle, ISSO

Signature of ISSO or SO: ERTLE.MARCUS.O.1365880871 Digitally signed by ERTLE MARCUS O 1365880871 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn ERTLE MARCUS O 1365880871 Date 2017 09 20 13 12 09 06'00' Date: 09/20/2017

Name of Information Technology Security Officer (ITSO): Nancy A. DeFrancesco

Signature of ITSO: DEFRANCESCO.NANCY.A.1377370917 Digita ly 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 09 20 15 19 12 04'00' Date: 09/20/2017

Name of Authorizing Official (AO): Margarita Gregg

Signature of AO: GREGG.MARGARITA.ELENA.1365899017 Digitally signed by GREGG MARGARITA ELENA 1365899017 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn GREGG MARGARITA ELENA 1365899017 Date 2017 09 21 16 37 40 04 00' Date: 09/21/2017

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 2017 09 28 09 56 13 04'00' Date: 09/28/2017

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA8873
National Data Buoy Center (NDBC)

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/NDBC

Unique Project Identifier: NOAA8873

Introduction: System Description

(a) General Description

The National Data Buoy Center (NDBC), a part of the National Oceanic and Atmospheric Administration (NOAA), National Weather Service (NWS), provides comprehensive, reliable systems and marine observations to support the missions of the NWS and NOAA, promote public safety, and satisfy the future needs of our customers. NDBC operates three major buoy arrays as well as a network of coastal marine observing stations. These systems provide critical data on oceanic and atmospheric conditions that is used by weather and hurricane forecasters, researchers, climatologists, oceanographers, commercial fishers, and recreational boaters, among others.

The NDBC manages the development, operations, and maintenance of the national data buoy network. It serves as the NOAA focal point for data buoy and associated meteorological and environmental monitoring technology. It provides high quality meteorological/environmental data in real time from automated observing systems that include buoys and a Coastal-Marine Automated Network (C-MAN) in the coastal zone surrounding the United States and the open ocean. It provides engineering support, including applications development, and manages data buoy deployment and operations, and installation and operation of automated observing systems installed on fixed platforms. It hosts the Volunteer Observing Ship (VOS) program to acquire additional meteorological and oceanographic observations supporting NWS mission requirements. The VOS is managed by federal employees within the NWS called PMOs (Port Meteorological Officers); their job is to recruit ships to take/report weather observations in the open seas. The NDBC program tracks only metadata on the observations and the ships, no information on the general public. The ships are typically commercial/cruise ships.

NDBC is located at the Stennis Space Center in Bay St. Louis, Mississippi, and has operated a network of off-shore weather buoys and unmanned coastal observing stations (Coastal Marine Automated Network or C-MAN stations) since 1990. In 2001 and 2005 respectively, NDBC began to assume responsibility for operating moored buoys supporting NOAA's Deep-Ocean Assessment and Reporting of Tsunami (DART) program and the Tropical Atmosphere Ocean (TAO) program that were developed and formerly operated by NOAA's Pacific Marine Environmental Laboratory (PMEL).

NDBC currently operates and maintains 195 moored buoys and 46 C-MAN stations. The U.S. Coast Guard provides ship transit services for NDBC so that it can repair and maintain its weather buoys. The Coast Guard also maintains a small staff at NDBC. NOAA vessels provide support for the NDBC mission when their schedules allow. NDBC also leases privately-owned vessels when required to support the mission and maintenance schedules.

Surveys of meteorologists have shown about 40 percent of NWS marine warnings and advisories are based, at least in part, on NDBC's meteorological data. In addition to this critical purpose, the observations are used by meteorologists who need to adjust flight level wind speeds reported by hurricane reconnaissance aircraft to surface winds; by geophysicists who use our sea surface temperature, wind, and wave reports to help calibrate remotely sensed measurements from spacecraft; and by engineers who obtain directional wave measurements to study beach erosion and shore protection. Additionally, surfers, fishermen, and boaters acquire the reports via the Internet to help them determine if they want to venture offshore.

Identifying Numbers:

- Passports of Foreign National visitors are collected via fax and transmitted electronically via Accellion to the NOAA security office and in person to the NASA security office. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of this and other PII/BII.

General Personal Data:

- Name, home address, and telephone numbers are collected from NDBC employees (federal and contractor) in support of Continuity of Operations (COOP) activities.
- When contacting the NDBC webmaster, customers' (i.e., general public, government, private sector, and educational institutions), email addresses are used in order to provide a response to questions and service requests. Further, the customers voluntarily provide contact information to include their name and phone numbers based on the type of response expected.

Work-Related Data:

- Occupation, job title, work address, telephone number, and email addresses are maintained on NDBC employees (federal and contractor) for administrative purposes.
- Electronic personnel-related forms of NDBC employees (federal) are transferred to NOAA HR in bulk or on a case-by-case basis via Accellion or via tracked Federal Express (FedEx) package. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.
- Performance plans of NDBC employees (federal) are maintained for administrative purposes.

- Proprietary information related to federal acquisition actions are maintained for administrative purposes.

Distinguishing Features/Biometrics:

- NDBC management utilizes photographs of NDBC employees (federal and contractor) to populate an organizational chart that is shared strictly within NDBC. Further, photographs are taken during NDBC buoy deployments and maintained on the shared drives. NDBC personnel (federal and contractor) give written permission for use of photos via the DOC Photo Release Form maintained by the HR liaison (we are now using this form with the PAS added).

System Administration/Audit Data:

- User IDs of NDBC employees (federal and contractor) are administered and maintained via a local implementation of Active Directory.
- Login success/failure is monitored on NOAA8873 for IT security purposes (ArcSight).
- Date/Time of access is monitored on NOAA8873 for IT security purposes (ArcSight).
- ID files accessed are monitored on NOAA8873 for IT security purposes (ArcSight).
- Contents of files are monitored on NOAA8873 for IT security purposes (ArcSight).

c) Information Sharing

Personnel and Foreign National (FN) information is shared/transferred to NOAA Human Resource (HR) and Security offices via Accellion. Foreign national information is delivered to NASA Security in person via the HR liaison. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

In case of a security or privacy breach, information will be shared with the Department of Commerce and possibly the Department of Justice.

d) Legal Authority to Collect PII/BII

Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1151(Dissemination of Technological, Scientific, and Engineering Information)
- 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)
- DAO 207-12 Foreign Visitor and Guest Access Program
- Authorities from DEPT-6: 5 U.S.C. 301; 44 U.S.C. 3101.
- 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: 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.
- Authorities from NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.
- Authorities 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.

e) FIPS 199 Security Impact

The NOAA8873 information system is categorized as a Moderate 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	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

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	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance Plans					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		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		f. Contents of Files	X
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	X		
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector (PAE)**	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): ***Pacific Architects and Engineers (PAE) is the technical services contractor at NDBC. They provide contact information for COOP.*					

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*	X	Electronic purchase transactions	
Other (specify):			

* This issue was addressed in the last PIA. This is the video surveillance of the data center. There are no discs. The video is placed on a network drive and files are automatically deleted once they are past 30 days. This is for correlation of physical entry into the data center in the case of an IT security event. The network drive access is limited to the NOAA IT staff. Signs are posted that video surveillance is in progress once you enter into the area where the camera view reaches.

	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		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	X
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 information collected and maintained by NOAA8873 is used for administrative purposes such as performance evaluations, logging into the information system, and contact during Continuity of Operations (COOP) activities. This information is that of federal employees and contractors.

Electronic personnel-related forms of NOAA employees only are transferred to NOAA HR in bulk or on a case-by-case basis via DOC Accellion (for NOAA records only) or via tracked Federal Express (FedEx) package. This information is not shared with anyone beyond those that are required to process it within the respective bureau. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

Customers voluntarily provide contact information when submitting web inquiries via webmaster and in doing so consent to contact from NDBC webmaster to answer their inquiries. Customers may be general public, government or private sector, including educational institutions.

Foreign nationals (FNs) requesting access to NDBC provide passports in support of the NOAA FN clearance process (application). The passports are transmitted via Accellion by the NDBC HR liaison. NASA also requires clearance of FNs since NDBC is a tenant on a NASA installation. FN passport information is delivered in person by the NDBC HR liaison in support of this process. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

Proprietary information related to federal acquisition actions are maintained for administrative purposes.

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):			

*In case of privacy/security breach

**NASA security office, and Department of Justice in case of 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: NOAA WFMO Recruitment Analysis Data System (RADS). NOAA8873 uploads employee PII in specified formats to RADS. The individual user (HR Liaison role) within the Resources Branch (OBS23)

	has been provided an encrypted drive (non-portable) for storage of PII/BII.
	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.ndbc.noaa.gov/contact_us.shtm A form for new employees with a PAS is stored in a folder, and attached with this PIA.	
X	Yes, notice is provided by other means.	Specify how: **Identifying Numbers**: Written notice is included on all personnel forms that employees (federal) complete. Notice is provided verbally to a foreign visitor by the US sponsor or the DOC staff at DOC International Affairs Office, at the time of the Foreign National's (FN's) appearance at the office, that completion of the information on the Foreign National Visitor and Guest Access request form is required for obtaining authorization for a visit. **General Personal Data**: Notice is provided to customers initiating web inquiries via webmaster by a privacy act statement on the web site. For NDBC COOP activities, employees are asked permission in person by their supervisors when collecting the applicable information. **Work-Related Data**: Written notice is included on all personnel forms that employees complete. For DOC performance/award documents, employees are informed by their supervisors in person or via email that the evaluations are in process. Employees have access to view the official documents. **Distinguishing Features/Biometrics**: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by

		the HR liaison. **System Administration/Audit Data**: NIST SP 800-53A Rev 4 requires information systems to collect audit data in support of IT security activities. NDBC employees (federal and contractor) are given notice via the NOAA IT Security Awareness Training.
	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: **Identifying Numbers**: FNs are given the opportunity to decline to provide information during the clearance process with NOAA. If FNs decline to provide the information (by not providing it) then access to NOAA sites (including NDBC) are denied. HSPD-12 requires personnel log into the information system using two factor authentication (2FA). If an employee declines to provide, no network access is provided. **General Personal Data**: For the Continuity of Operations (COOP) activities, NDBC personnel can inform their supervisor in person or in writing that they decline to provide PII/BII. Customers voluntarily provide information when submitting web inquiries via webmaster, so that they may be contacted. **Work-Related Data**: Performance/position information is part of the official personnel record for DOC employees, with notice given on the forms completed as part of the hiring process. Individuals may have chosen not to provide information, by not completing the forms, but this would affect their employment status. . **Distinguishing Features/Biometrics**: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison. If personnel decline participation, no DOC Photo Release Form is filed with the HR liaison.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: **System Administration/Audit Data**: NIST SP 800-53A Rev 4 requires information systems to collect audit data in support of IT security.

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: **Identifying Numbers**: FNs are given the opportunity via the NOAA forms to consent to the use of their information in support of the clearance process during the application process with NOAA.

		Personnel may choose not to log in to the information system, but HSPD-12 requires personnel to log in using two factor authentication (2FA). This is the only use for this information. **Work-Related Data**: Performance/position information is part of the official personnel record for DOC employees. Employees may choose not to consent to a particular use, in writing, to their supervisors, but this may affect their employment status. **General Personal Data**: For the Continuity of Operations (COOP) activities, there is only one use. Customers voluntarily provide information when submitting web inquiries via webmaster and in doing so consent to contact from NDBC webmaster to answer his/her inquiry. This is the only use of the information. **Distinguishing Features/Biometrics**: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: **System Administration/Audit Data**: NIST SP 800-53A Rev 4 requires information systems to collect audit data in support of IT security.

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: **Identifying Numbers**: FNs are given the opportunity to update their information during a subsequent clearance process with NOAA where the FN completes a new application. **General Personal Data**: For the Continuity of Operations (COOP) activities, NDBC personnel are asked via email from either the NDBC HR liaison or the NDBC ISSO to review/update PII/BII annually in person. **Distinguishing Features/Biometrics**: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison. **Work-Related Data**: Performance/position information is part of the official personnel record for DOC employees and will be updated upon official personnel actions. **General Personal Data**: Customers voluntarily provide email address and contact information at their discretion when contacting the NDBC Webmaster, but we collect information only per each email, rather than keeping a record.
	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: *Windows file system auditing monitors, tracks, and records changes to the files containing PII/BII and a report is sent to the NDBC ISSO daily.*
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): *01/28/2017* ☐ 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.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

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

All NDBC 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 electronically signs the Rules of Behavior (ROB) via the NOAA IT Security Awareness training indicating that they have read and understand the ROB. The ROB outlines privacy and the PII definition, storage, sharing, and reporting of PII incidents.

To protect data contained on mobile devices, all NDBC laptops are fully encrypted using the NOAA enterprise supplied encryption software. In addition, all NDBC government issued phones are protected via MaaS 360.

NDBC employees are required to utilize DOC Accellion for the transmission of any sensitive data.

The individual user (HR Liaison role) within the Resources Branch (OBS23) has been

provided an encrypted drive (non-portable) for storage of all PII/BII in the system.

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, Employees Personnel Files Not Covered by Notices of Other Agencies* *DEPT 6, Visitor Logs and Permits for Facilities under Department Control* *NOAA 11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.* *OPM/GOVT 1, General Personnel 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: *NARA, General Records Schedule 20 Electronic Records* *NARA, General Records Schedule 24 Information Technology Operations and Management 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		Deleting	X
Other (specify): Destruction of Hard Drives			

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: *Customers voluntarily provide only as much information as they feel necessary when submitting web inquiries via NDBC webmaster.*
X	Quantity of PII	Provide explanation: *NDBC employees (federal and contractor) total less than 250 and minimal PII is collected/maintained.*
X	Data Field Sensitivity	Provide explanation: *Some sensitive PII is collected, mainly from foreign visitors.*
X	Context of Use	Provide explanation: *Information is for official use only and contained within DOC and NOAA.*
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: *Security and privacy controls for protecting PII/BII are in place and functioning for NOAA8873 IAW NIST SP 800 53 Revision 4.*
	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.
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: Joy Baker Office: DOC/NOAA/NWS/OBS2 (NDBC) Phone: 228-688-2801 Email: Joy.Baker@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: BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER.JOY.ALLISON.1269758577 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BAKER.JOY.ALLISON.1269758577 Date: 2017.10.25 12:37:25 -05'00' Date signed:	**Information Technology Security Officer** Name: Beckie Koonge Office: DOC/NOAA/NWS/ACIO Phone: 301-427-9020 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: 2017.10.30 13:46:56 04'00' Date signed:
Authorizing Official Name: Joseph Pica Office: DOC/NOAA/NWS/OBS Phone: 301-427-9778 Email: Joseph.A.Pica@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: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.10.25 15:11:31 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: 2017.10.30 15:52:52 -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: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA8873-National Data Buoy Center (NDBC)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NDBC

Unique Project Identifier: NOAA8873

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 Data Buoy Center (NDBC), a part of the National Oceanic and Atmospheric Administration (NOAA), National Weather Service (NWS), provides comprehensive, reliable systems and marine observations to support the missions of the NWS and NOAA, promote public safety, and satisfy the future needs of our customers. NDBC operates three major buoy arrays as well as a network of coastal marine observing stations. These systems provide critical data on oceanic and atmospheric conditions that is used by weather and hurricane forecasters, researchers, climatologists, oceanographers, commercial fishers, and recreational boaters, among others.

The NDBC manages the development, operations, and maintenance of the national data buoy network. It serves as the NOAA focal point for data buoy and associated meteorological and environmental monitoring technology. It provides high quality meteorological/environmental data in real time from automated observing systems that include buoys and a Coastal-Marine Automated Network (C-MAN) in the coastal zone surrounding the United States and the open ocean. It provides engineering support, including applications development, and manages data buoy deployment and operations, and installation and operation of automated observing systems installed on fixed platforms. It hosts the Volunteer Observing Ship (VOS) program to acquire additional meteorological and oceanographic observations supporting NWS mission requirements.

NDBC is located at the Stennis Space Center in Bay St. Louis, Mississippi, and has operated a network of off-shore weather buoys and unmanned coastal observing stations (Coastal Marine Automated Network or C-MAN stations) since 1990. In 2001 and 2005 respectively, NDBC began to assume responsibility for operating moored buoys supporting NOAA's Deep-Ocean Assessment and Reporting of Tsunami (DART) program and the Tropical Atmosphere Ocean (TAO) program that were developed and formerly operated by NOAA's Pacific Marine Environmental Laboratory (PMEL).

NDBC currently operates and maintains 195 moored buoys and 46 C-MAN stations. The U.S. Coast Guard provides ship transit services for NDBC so that it can repair and maintain its weather buoys. The Coast Guard also maintains a small staff at NDBC. NOAA vessels provide support for the NDBC mission when their schedules allow. NDBC also leases privately-owned vessels when required to support the mission and maintenance schedules.

Surveys of meteorologists have shown about 40 percent of NWS marine warnings and advisories are based, at least in part, on NDBC's meteorological data. In addition to this critical purpose, the observations are used by meteorologists who need to adjust flight level wind speeds reported by hurricane reconnaissance aircraft to surface winds; by geophysicists who use our sea surface temperature, wind, and wave reports to help calibrate remotely sensed measurements from spacecraft; and by engineers who obtain directional wave measurements to study beach erosion and shore protection. Additionally, surfers, fishermen, and boaters acquire the reports via the Internet to help them determine if they want to venture offshore.

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.*

The NDBC currently has a video surveillance system installed in the data center to monitor physical access to the restricted area. In addition, access to the information technology (IT) areas is physically controlled via room entry readers. Select buoys are outfitted with cameras to collect visual environmental data and images collected are stored on the information system.

____ 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 NOAA8873 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 NOAA8873 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): Joy Baker, ISSO

Signature of ISSO or SO: BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER.JOY.ALLISON.1269758577 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BAKER.JOY.ALLISON.1269758577 Date: 2017.06.02 13:58:10 -04'00' 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 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BROWNE.ANDREW.PATRICK.1472149349 Date: 2017.06.02 15:03:58 -04'00' Date: _____

Name of Authorizing Official (AO): Joseph Pica, AO

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.07.13 17:26:43 -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: 2017.07.25 09:25:50 -04'00' Date: _____

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, November 20, 2017 4:24 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: Revised NOAA4020 PTA per Mark's comments
Attachments:	NOAA4020 PTA 2017 revised description_nc_rm mhg.pdf

Looks good, and this captures the takeaway from the CRB. 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, Nov 20, 2017 at 3:39 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, for your signature. thx
>
> Forwarded message
> From: **Tahir Ismail - NOAA Affiliate** <tahir.ismail@noaa.gov>
> Date: Mon, Nov 20, 2017 at 3:35 PM
> Subject: Fwd: Revised NOAA4020 PTA per Mark's comments
> To: Sarah Brabson <sarah.brabson@noaa.gov>
> Cc: Glen Taylor NOAA Federal <glen.taylor@noaa.gov>, "NMFS.InfoSec@noaa.gov" <NMFS.InfoSec@noaa.gov>
>
> Sarah,
>
> Attached, please find the signed PTA.
>
> Thanks,
>
> Tahir
> Forwarded message
> From: **Rick Miner - NOAA Federal** <rick.miner@noaa.gov>
> Date: Mon, Nov 20, 2017 at 3:14 PM
> Subject: Re: Revised NOAA4020 PTA per Mark's comments
> To: Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov>

Signed

Rick Miner, CISSP-ISSAP, CCSP
IT Security Engineer
NOAA Fisheries
U.S. Department of Commerce
Office: 301.427.8822
Mobile (b)(6) [redacted]
rick.miner@noaa.gov
www.fisheries.noaa.gov

On Thu, Nov 16, 2017 at 9:46 AM, Tahir Ismail NOAA Affiliate <tahir.ismail@noaa.gov> wrote:

> Rick,
>
> Please sign the NOAA4020 PTA.
>
> Thanks,
>
> Tahir
>
> Forwarded message
> From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
> Date: Thu, Nov 16, 2017 at 8:55 AM
> Subject: Fwd: Revised NOAA4020 PTA per Mark's comments
> To: Tahir Ismail <tahir.ismail@noaa.gov>, "NMFS.InfoSec@noaa.gov" <NMFS.InfoSec@noaa.gov>
> Cc: Glen Taylor <Glen.Taylor@noaa.gov>
>
> Tahir, please have Rick sign and then send to me. thx Sarah
>
> Forwarded message
> From: **Glen Taylor - NOAA Federal** <glen.taylor@noaa.gov>
> Date: Wed, Nov 15, 2017 at 4:36 PM
> Subject: Re: Revised NOAA4020 PTA per Mark's comments
> To: Tahir Ismail <tahir.ismail@noaa.gov>, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Mohamed Mughal NOAA Federal <mohamed.mughal@noaa.gov>
> Cc: Scott Sauri <Scott.Sauri@noaa.gov>, "NMFS.InfoSec@noaa.gov" <NMFS.InfoSec@noaa.gov>, Franklin Schwing NOAA Federal <franklin.schwing@noaa.gov>
>
> Tahir and Sarah,
>
> Please find the updated PTA with the new description attached.
>
> Mohamed, please also substitute this system description for the one in CSAM.

Thanks,
Glen

On Wed, Nov 15, 2017 at 12:37 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Thanks, Glen!

On Wed, Nov 15, 2017 at 12:36 PM, Glen Taylor NOAA Federal <glen.taylor@noaa.gov> wrote:

Hi Sarah,

The PTA looks fine to me. I'll start the signatures again on our side.

Thanks,
Glen

On Wed, Nov 15, 2017 at 7:55 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Glen, is this okay with you? Can you start signatures? thx

On Tue, Nov 14, 2017 at 2:21 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Mark had said we should use the system description from the PIA, for the PTA also.

So I kept the one paragraph in the PTA system description and copied in the application descriptions from the PIA.

And in the PIA, I added the paragraph from the PTA as an intro to the application descriptions (see attached also). We still can't finalize this PIA till I get the rest of the privacy act statements posted but here is the version with the paragraph added.

If the PTA looks okay to you, please start signatures.And please also substitute this system description for the one in CSAM.

thx Sarah

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

Glen C. Taylor
IT Operations Branch Chief
Science Information Division (F/ST6)
Office of Science and Technology
NOAA National Marine Fisheries Service
1315 East West Highway, Rm 12326
Silver Spring, MD 20910
Phone: 301 427 8183 | Fax: 301 713 4137
Email: Glen.Taylor@noaa.gov

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

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

Glen C. Taylor
IT Operations Branch Chief
Science Information Division (F/ST6)
Office of Science and Technology
NOAA National Marine Fisheries Service
1315 East West Highway, Rm 12326
Silver Spring, MD 20910

Phone: 301 427 8183 | Fax: 301 713 4137
Email: Glen.Taylor@noaa.gov

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)

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

NOAA OCIO

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 Threshold Analysis
for the
NOAA4020
Office of Science and Technology

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Office of Science and Technology

Unique Project Identifier: 006-48-01-14-02-3305-00

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 and its purpose 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 NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

1) The Financial Services Division collects information from applicants for the following programs and purposes: The Fisheries Finance Program (FFP), credit information, personal identification including social security number, and tax returns. The information is used to verify applicants for fisheries loans. Capital Construction Fund (CCF), personal identification including social security numbers and tax returns. The information is used to verify applicants for CCF accounts and projects. Fishermen's Contingency Fund (FCF), personal identification including social security numbers, and personal transaction information. The information is used to verify business losses and lost fishing gear for claims made by the fishermen. Information collected includes tax returns.

   Information collected: applicant's name and address, the amount of financing applied for, the purpose of loans, an appraisal of the vessel or facility involved, financial information including the last 3 tax returns (these are not stored electronically), a list of creditors and buyers with relevant credit terms, identification of authorized representatives (accountant, attorney, insurance agent), and legal history (status regarding bankruptcy, litigation, delinquency on and Federal debt, etc.). Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the

original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated. Loan applications are entered into the system from paper forms completed by the public, into an online application, which is managed by NMFS NOAA4020. Regional offices access the information in order to administer loans for applicants. The loan data is stored only in NOAA4020.

When a United States (U.S.) commercial fisherman sustains losses and/or damages as a result of oil and gas activities on the U.S. Outer Continental Shelf (OCS), the fisherman may apply for compensation from the U.S. Federal government, using fillable pdf forms on the applicable Web site.

NMFS also has programs to reduce excess fishing capacity by paying fishermen to surrender their vessels/permits. These fishing capacity reduction programs, or buybacks, are conducted pursuant to the Magnuson-Stevens Fishery Conservation and Management Act, and the Magnuson-Stevens Reauthorization Act (Pub. L. 109-479). The buybacks can be funded by a Federal loan to the industry or by direct Federal or other funding. Buyback regulations are at 50 CFR Part 600. The information collected by NMFS involves the submission of buyback requests by industry, submission of bids, referenda of fishery participants and reporting of collection of fees to repay buyback loans. For Fishery Capacity Reduction Program Buyback Requests, certain forms are submitted on paper and entered into a database, and others are submitted online.

Information is not shared except within the program (NMFS Headquarters, West Coast Region and Southeast Region), or in the case of a breach, within the bureau, the Department and other federal agencies (Justice).

2) International Trade Data System (ITDS).

ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports and exports of fisheries products. Types of BII data collected are Name of business, Address and Contact information. The data is collected from the U.S. Customs and Border Control's ITDS database. Reasons for the NMFS database:
(1) The CBP's ITDS only grants access to a small group of people who can meet their security clearance requirements which will take time and it seems they do want to limit the number of users. (2) The CBP's ITDS can't meet the specific requirements of the NMFS programs. So we developed our own ITDS to support the NMFS programs. For example, one program needs to the functions to track the harvesting vessel trips, all programs need the functions to review the data and track issues; the programs need to search data relevant to their programs etc.

3) Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL)

The Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL) system will be a tool to load raw data from various sources, format them and run through various

QA/QC processes. NOAA4020 collects PII and BII data from MRIP ETL only for the NSAR, see below. Types of PII collected are fishing license info, Name, Address, Driver's license, Phone, Email and Date of Birth of the angler. Some states have requested that their data cleansed by this process be sent back to them.

4) National Saltwater Angler Registry - NSAR

The National Saltwater Angler Registry system allows the integration of the state-provided saltwater angler license data with the existing national registration data into a database, which can be used as a consolidated phone book of the nation's recreational salt-water anglers. The captured data is entered into the database and will be used to furnish frames for the MRIP survey. Types of PII collected are Name, Address, Driver's license, Telephone, Email and Date of Birth of the angler.

5) NOAA Fisheries Committee on Scientific Stature.

The NOAA Fisheries Committee on Scientific Stature (NFCSS) is a national-level Performance Management Advisory Committee (PMAC) established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. There is a website and database to manage and record the results of NFCSS member reviews conducted for the purpose of evaluating a scientist's credentials and contributions to allow them to be assigned to a higher pay Band without being a supervisor and to produce a standard report for the committee chair (OST Science Director). In 2014, OST upgraded the NFCSS website and database to enable password protected, role-based secure storage and retrieval of review package documents. Access to the database is restricted to the OST Science Director, the six regional Deputy Science Directors, one Band V research scientist from each regional science center, the NOAA Fisheries HR Business Partner, and the NFCSS database administrator and is provided by the NFCSS database administrator only at the request of the NFCSS Chair. Information collected: name, work contact information, letters of reference and curricula vitae, performance plan, science director memoranda and name of immediate supervisor. The administrator uploads copies of a memorandum from the NFCSS Chair to the Science Center director of staff being reviewed. The data (name, email, documents) for staff being reviewed are entered by their Deputy Science Director. The review comments are entered by the NFCSS members.

6) Protected Resources National Inventory of Marine Mammals (NIMM) System.

National Inventory of Marine Mammals (NIMM) was rolled out to the marine mammal Owners and Facilities, on July 18, 2017, with an initial user base of 151 users. NIMM maintains current

and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. NOAA4020 collects PII and BII data from this system. Types of BII collected are Institution Name, Mailing address, Contact email, Phone and Fax Numbers. No PII is collected.

7) Highly Migratory Species.

Effective July 1, 2005, all dealers importing, exporting, or re-exporting bluefin tuna, swordfish, southern bluefin tuna and frozen bigeye tuna must hold a Highly Migratory Species International Fishery Trade Permit (HMS IFTP) and follow the required reporting procedures established at 50 C.F.R. 300.183 through 300.187. The HMS IFTP is required to assist the United States implement international trade tracking programs addressing illegal, unreported, and unregulated fishing activities, improve conservation and management measures, and enhance the scientific evaluation of these stocks.

Under international agreements and domestic law, the United States implements recommendations of the International Commission for the Conservation of Atlantic Tunas (ICCAT) and Inter-American Tropical Tuna Commission (IATTC). Both IATTC and ICCAT have implemented a statistical document program for frozen bigeye tuna. In addition, ICCAT has implemented bluefin tuna and swordfish statistical document programs.

The NMFS Office of Science and Technology developed a legacy Highly Migratory Species Dealer Permit System more than 10 years ago to meet the requirements outlined in the purpose above. The system has since been migrated over to the NMFS National Permit System, whose information is stored in NOAA4000. For historical validating of permits, the system is currently being retained for its reporting functionality for viewing and validating permit information on dealers. Please note that once all permits have expired on these two reports, there will be no more need to maintain these interfaces and will therefore be deactivated. NOAA4020 collects PII and BII data from Highly Migratory Species. Types of PII and BII data collected and processed are Applicant Name, Social Security Number, Position Type, Birthdate, Mailing Address Street Name, Business Name, Federal ID No/SSN, Date Business Formed, Business Type, Mailing Address Street Name etc. *No new data is being collected through this legacy system.*

8) NOAA Emergency Contact List
NOAA collects the Emergency Contact List that is used to track and locate staff in the office of Science and Technology. This is PII data.

9) NOAA4020 collects system user ID information from employees and contractors accessing

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.*

__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): New application (NIMM) rolled out in 7/17.					

____ 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.

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

NOAA 4020 contains a variety of PII and BII, including permit application data and loan application data.

____ 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 [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: TAYLOR.GLEN.CLIFFORD.1365840934 Digitally signed by TAYLOR GLEN CLIFFORD 1365840934 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=TAYLOR GLEN CLIFFORD 1365840934 Date: 2017 11 15 12:48:07 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: MINER.RICHARD.SCOTT.1398604519 2017.11.20 15:14:15 05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn CYR.EDWARD.C.DR.1365869436 Date: 2017.11.15 15:59:45 -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: 2017.11.20 16:23:08 -05'00' Date: _____

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, November 20, 2017 4:27 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NCCM Delayed POA&M
Attachments:	DLP Plan Final in Word.docx

I guess development of the plan could be the original CIO briefing. I'll attach the original DLP Memo in word that reflects development of the plan before approval at the CIO Council. That can be the artifact for plan development.

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

On Mon, Nov 20, 2017 at 3:41 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Both milestones? Development of plan and approval of plan? thx
>
> On Mon, Nov 20, 2017 at 3:24 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
>
> > Yes, I'd include the Memo from Zach as an artifact for milestone completion as well.
> >
> > Mark H. Graff
> > FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> > National Oceanic and Atmospheric Administration
> > (301) 628 5658 (O)
> > (b)(6) (C)
> >
> >
> >
> > On Mon, Nov 20, 2017 at 2:22 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> >
> > > Can you answer my questions, so I can complete updates to the DLP POA&M? Also, the original one is still in the IT Risk Management system. I need to find out how to cancel that out.
> > >
> > > Forwarded message

From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Mon, Nov 20, 2017 at 12:47 PM
Subject: Re: NCCM Delayed POA&M
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Okay, I changed the finish date of the 'develop plan' milestone to 9 7 17. Does the memo from Zach go here as well as the final plan, or with the 'plan approved' milestone?

On Mon, Nov 20, 2017 at 11:17 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Yes, thanks, as soon as I get back to my desk.
>
> Sent from my iPhone
>
> On Nov 20, 2017, at 11:10 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
>
> Here are the artifacts. Can you upload into CSAM Milestones? Attached are:
>
> Alternative Plan signed by Zach
> CIO Announcement confirming first phase rollout
>
> Mark H. Graff
> FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> National Oceanic and Atmospheric Administration
> (301) 628 5658 (O)
> (b)(6) [redacted] (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.
>
> Forwarded message
> From: **Hadona Diep - NOAA Affiliate** <hadona.diep@noaa.gov>
> Date: Mon, Nov 20, 2017 at 11:02 AM
> Subject: FW: NCCM Delayed POA&M
> To: Mark Graff NOAA Federal <mark.graff@noaa.gov>
> Cc: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Jean Apedo NOAA Federal <jean.apedo@noaa.gov>, Duaa Bukhari NOAA Affiliate <duaa.bukhari@noaa.gov>, Kirsten Carr NOAA Affiliate <kirsten.carr@noaa.gov>, James Jones NOAA Federal <james.jones@noaa.gov>
>
> Mark,

Please see below in regards to 70550. Please upload any related artifacts into the Milestones, request for closure, and we will review.

Thanks,

Best regards,

Hadona Diep
Contractor - The Ambit Group, LLC
NOAA Office of Chief Information Officer
Cell: (b)(6)

From: Mark Graff - NOAA Federal [mailto:mark.graff@noaa.gov]
Sent: Thursday, October 12, 2017 5:11 PM
To: Hadona Diep - NOAA Affiliate
Cc: Jean Apedo - NOAA Federal; James Jones - NOAA Federal
Subject: Re: NCCM Delayed POA&M

Hello Hadona,

Certainly. The DLP rollout was a phased approach, so I failed to close the POA&M where the rollout is still ongoing. My mistake thank you for the reminder.

Mark H. Graff

FOIA Officer/Bureau Chief Privacy Officer (BCPO)

National Oceanic and Atmospheric Administration

(301) 628 5658 (O)

(b)(6) (C)

On Thu, Oct 12, 2017 at 4:27 PM, Hadona Diep NOAA Affiliate <hadona.diep@noaa.gov> wrote:

Mark,

James Jones and I have noticed there are a few POA&Ms within NCCM that are over 120 days late. POA&M #70550 was assigned to you on 4/19/2016 with a scheduled completion date of 12/30/2016 – this POA&M is based on the implementation of a DLP.

Would you be able to upload the necessary artifacts and submit a closure request to these POA&Ms ASAP?

Best regards,

Hadona Diep
Contractor The Ambit Group, LLC
NOAA Office of Chief Information Officer
Cell: (b)(6)

<DLP Alternative Approach signed NOAA Data Loss Prevention.pdf>

<CIO Announcement.pdf>

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

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

NOAA OCIO
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)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, November 20, 2017 4:36 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NCCM Delayed POA&M
Attachments:	DLP Plan Final signed.pdf

This is the signed plan (attached), signed on Aug. 30, 2016.

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

On Mon, Nov 20, 2017 at 3:54 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> And what was the plan approval date? Same? I don't find in either saved, archived or trashed emails. If you can re send your email to Emily HO that I meant to use way back .. that would be great.
>
> On Mon, Nov 20, 2017 at 3:41 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Both milestones? Development of plan and approval of plan? thx
> >
> > On Mon, Nov 20, 2017 at 3:24 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
> >
> > > Yes, I'd include the Memo from Zach as an artifact for milestone completion as well.
> > >
> > > 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 Mon, Nov 20, 2017 at 2:22 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> > >
> > > > Can you answer my questions, so I can complete updates to the DLP POA&M? Also, the original one is still in the IT Risk Management system. I need to find out how to cancel that out.

Forwarded message
From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Mon, Nov 20, 2017 at 12:47 PM
Subject: Re: NCCM Delayed POA&M
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Okay, I changed the finish date of the 'develop plan' milestone to 9 7 17. Does the memo from Zach go here as well as the final plan, or with the 'plan approved' milestone?

On Mon, Nov 20, 2017 at 11:17 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

Yes, thanks, as soon as I get back to my desk.

Sent from my iPhone

On Nov 20, 2017, at 11:10 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

Here are the artifacts. Can you upload into CSAM Milestones? Attached are:

Alternative Plan signed by Zach
CIO Announcement confirming first phase rollout

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

Forwarded message
From: **Hadona Diep - NOAA Affiliate** <hadona.diep@noaa.gov>
Date: Mon, Nov 20, 2017 at 11:02 AM
Subject: FW: NCCM Delayed POA&M
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>
Cc: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Jean Apedo NOAA Federal <jean.apedo@noaa.gov>, Duaa Bukhari NOAA Affiliate <duaa.bukhari@noaa.gov>, Kirsten Carr NOAA Affiliate <kirsten.carr@noaa.gov>, James Jones NOAA Federal <james.jones@noaa.gov>

Mark,

Please see below in regards to 70550. Please upload any related artifacts into the Milestones, request for closure, and we will review.

Thanks,

Best regards,

Hadona Diep
Contractor - The Ambit Group, LLC
NOAA Office of Chief Information Officer
Cell: (b)(6)

From: Mark Graff - NOAA Federal [mailto:mark.graff@noaa.gov]
Sent: Thursday, October 12, 2017 5:11 PM
To: Hadona Diep - NOAA Affiliate
Cc: Jean Apedo - NOAA Federal; James Jones - NOAA Federal
Subject: Re: NCCM Delayed POA&M

Hello Hadona,

Certainly. The DLP rollout was a phased approach, so I failed to close the POA&M where the rollout is still ongoing. My mistake thank you for the reminder.

Mark H. Graff

FOIA Officer/Bureau Chief Privacy Officer (BCPO)

National Oceanic and Atmospheric Administration

(301) 628 5658 (O)

(b)(6) (C)

contents is strictly prohibited. Please notify us immediately that you have received this message in error, and delete the message.

On Thu, Oct 12, 2017 at 4:27 PM, Hadona Diep NOAA Affiliate <hadona.diep@noaa.gov> wrote:

Mark,

James Jones and I have noticed there are a few POA&Ms within NCCM that are over 120 days late. POA&M #70550 was assigned to you on 4/19/2016 with a scheduled completion date of 12/30/2016 – this POA&M is based on the implementation of a DLP.

Would you be able to upload the necessary artifacts and submit a closure request to these POA&Ms ASAP?

Best regards,

Hadona Diep
Contractor The Ambit Group, LLC
NOAA Office of Chief Information Officer
Cell: (b)(6)

<DLP Alternative Approach signed NOAA Data Loss Prevention.pdf>

<CIO Announcement.pdf>

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751

Ce (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)

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

NOAA Data Loss Prevention Plan

Office of the Chief Information Officer
Governance and Portfolio Division
August 2016

Background

[01] The protection of sensitive and personal information is more important than ever with electronic communications becoming increasingly prevalent. Safeguarding Personally Identifiable Information (PII) in the possession of the Federal Government and preventing its breach are essential to retaining the trust of the American public[1]. This responsibility is shared by officials accountable for administering operational, privacy, and security programs. PII is any information that, by itself or in combination with other information, may be used to uniquely identify an individual. Within NOAA systems, this primarily can consist of Social Security Numbers (SSN), names, addresses, dates and places of birth, bank account numbers, e-mail addresses, telephone numbers, and passport numbers. The Office of Management and Budget (OMB) and the Department of Commerce (Commerce) released several memoranda to address the issue of safeguarding PII[2].

[02] This plan is intended as a framework for future action that will address user and system specific restrictions, controls, use cases, parameters, and other actions implemented based on the needs of individual systems and mission goals. This plan is intended to satisfy the implementation plan obligations to meet the minimum Privacy DLP Standards within 1 year as outlined in the April 15, 2016 Memorandum entitled "Departmental Privacy Standards for Commerce Data Loss Prevention (DLP) Security Tools", as well as the corresponding May 3, 2016 data call issued by Commerce.

NOAA Data Overview

[01] NOAA provides the data, science, and information that allow the economy to function effectively and grow sustainably. NOAA helps to ensure a competitive economy by monitoring and predicting changes in the Earth's environment, protecting lives and property, and conserving and managing the nation's coastal and marine resources. NOAA's data portfolio mirrors the diversity and complexity of its mission … and NOAA is very complex! Our mission and data diversity includes:

- 21,335 Staff (federal, contractor, associate)
- 435 Buildings
- 122 Weather Forecast Offices
- 13 River Forecast Centers
- 1,429 Real-Time Weather Stations
- 17 Satellites
- 8 Buoy Networks: 1042 Stations Deployed
- 13 National Marine Sanctuaries and 1 Marine National Monument
- 286 Data Centers

---

[1] The definition of PII can be found in the OMB Memorandum M-06-19, July 12, 2006.

[2] See, e.g., Memorandum from David A. Sampson, RE: Safeguarding Personally Identifiable Information, November 6, 2006.

- 94 Federal Information System Management Act Systems
- 33 Exhibit 300 IT Investments

NOAA DLP Strategy Overview

[01] NOAA uses, and will further deploy, a "Defense in Depth" approach to DLP. NOAA will use existing operational controls and privacy enhancing technologies. These include PII identifying solutions, encryption, firewalls, authorized use system access controls, and system audit logs. To further reduce the risk of compromise of sensitive PII in agency communications, NOAA will implement a Data Loss Prevention (DLP) solution set that monitors network communications and prevents sensitive PII from leaving the network, in addition to other sensitive data, as determined when the scope and capability of the solution is determined. Other sensitive data may include law enforcement sensitive data, business identifiable data, or other data sets for which the DLP solution can feasibly be leveraged. Each of these data sets may have one or more data owners, who will classify the information type, as described in the fourth development step below. In addition to these technical controls, NOAA utilizes administrative policies and procedures, as well as privacy training, to further safeguard information privacy and control access to information systems and information assets.

[02] NOAA conducts Privacy Threshold Analyses, (PTA's), and, where applicable, Privacy Impact Assessments (PIAs) on all information systems to ensure privacy implications are addressed when planning, developing, implementing, and operating information technology (IT) systems that maintain information on individuals. NOAA utilizes a PIA template and guidance on conducting PIAs. The NOAA Bureau Chief Privacy Officer (BCPO) collaborates with system owners and IT security professionals to assess existing, new, or proposed programs, systems or applications for privacy risks, and recommends methods to protect individual privacy.

[03] The NOAA DLP solution(s) will be designed to monitor and prevent data from being leaked. NOAA's DLP strategy, however, is to make sure the DLP solution(s) are as efficient and effective as possible. DLP needs to be rationally deployed in order to ensure that false positives do not overwhelm the system and the capacity of NOAA privacy and cyber security managers and staff. DLP tools such as McAfee Security, as powerful as they may be, require careful and organized deployment, otherwise reported incidents may be of little value.

[04] In response to the OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, and NIST SP 800-122, at 2.1, the NOAA Governance and Portfolio Division is leading the DLP initiative to promote secure practices in electronic communications (e-mails and Internet access) on the NOAA network to protect Controlled Unclassified Information (CUI) data. Taking a phased approach, the DLP initiative may include plans to implement specific solutions, for example, McAfee's Data Loss Prevention (DLP) commercial off-the-shelf software solution that is capable of identifying and tracking a number of NOAA's defined PII datasets. The NOAA DLP solution(s) will be designed to give NOAA an enterprise view into where it's most sensitive data are stored, who has access to the data, and where and by whom the data are sent outside the NOAA network. By using this information, NOAA can spot broken business processes and reduce the overall risk of exposure. The DLP solution(s) will take a data-centric approach to security, in which policies can be developed

around the content that should be protected and then deployed across multiple data states or functionalities, such as identifying, monitoring, and preventing.

DLP Development Steps

[01] A multi-layered approach will be applied to prevent data leakage for all routes and states. Data is classified under one of several schemes like data in motion, data in use, and at rest; or by data in-store, in-use and in-transit.

- Data in motion: Data that needs to be protected when in transit including HTTP/S, S/FTP/S, IM, P2P, SMTP.
- Data in use: Data that resides on end user workstation and needs to be protected from being leaked through removable media devices like USB, DVD, CD's.
- Data at rest: Data that resides on local storage media or server storage.

[02] Each of these layered types of data will be considered during deployment to maximize the prevention of data leakage. A multi-step approach to deployment, shown below, will be used as well. These steps are discussed in detail below.

1. Define policies
2. Identify sensitive data
3. Determine information flows
4. Identify data owners
5. Identify deployment scenarios
6. Plan DLP operations
7. Deploy DLP product(s)

Define Policies

[01] NOAA will build policies to protect the sensitive data. Every policy will consist of some rules, such as to protect credit card numbers, PII, and social security numbers, if such policies are not already in place. If there is a requirement for NOAA to protect sensitive information and a DLP product such as McAfee DLP does not support it out of the box, then NOAA will create rules using regular expressions (regex). It should be noted that DLP policies at this stage will be defined and not applied.

[02] Those policies will reflect the internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our objective: Commerce Directives; and OMB, White House, and National Institute for Standards and Technology (NIST) guidelines. Each of these sources provide a framework for implementing an automatic tool to monitor transfers of PII and for developing, or implementing, a commercial off-the-shelf product. We are evaluating these controls against an enterprise life cycle approach, and by reviewing enterprise life cycle commercial off-the-shelf artifacts and documents supporting the procurement, budget, and expenses for the DLP solution.

[03] Policies will take into consideration existing guidelines and recommendations as well as other factors, such as impact and dependency for other systems, also needed to be considered when implementing a DLP solution. The National Institute for Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information[3][1], recommends that agencies implement automated tools, such as a network data leakage prevention tool, to monitor transfers of PII and to monitor inbound and outbound communications for unauthorized activities. In addition, the Government Accountability Office's Standards for Internal Control in the Federal Government[4][2] provides that application controls should be designed to help ensure completeness, accuracy, authorization, and validity of all transactions during application processing. Controls should be installed as an application interfaces with other systems to ensure that all inputs are received and are valid and that outputs are correct and properly distributed.

Identify Sensitive Data

[01] NOAA will identify all the confidential, restricted, and highly restricted data across the whole organization and across the three categories, i.e. for data in-transit, in-store and in-use. In identifying the sensitive data, NOAA will define the scope within which the DLP Solution will function. Each data set analyzed will be considered as to whether or not leveraging the DLP product would be an efficient use of resources, whether the data is non-sensitive, or whether the DLP would be an effective tool in further securing the data. DLP products work with signatures to identify any restricted data when it is crossing boundaries. To identify the critical data and develop its signatures, there is a term in DLP products known as fingerprinting. Data is stored in various forms at various locations in an organization and it requires identifying and fingerprinting. Various products come with a discovery engine which crawl all searchable data in a given data store, index it and make it accessible through an intuitive interface which allows quick searching on data to find its sensitivity and ownership details.

Determine Information Flows

[01] It is very important for an organization to identify their information flow. NOAA OCIO will prepare a questionnaire to identify and extract all the useful information. A sample questionnaire would address, at a minimum, the following three issues:

- What is a standard data flow, and what should be the source and destination of the identified data?
- What are all the egress points present in the network?
- What processes are in place to govern the informational flow?

---

[3] National Institute of Standards and Technology, NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 2010).

[4] Government Accountability Office (formerly known as the General Accounting Office), GAO/AIMD-00-21.3.1, Internal Control: Standards for Internal Control in the Federal Government (Nov. 1999).

Identify Data Owners

[01] Identification of the NOAA staff and line office owners of data is also an important step in the planning strategy of DLP, so a list will be prepared by OCIO of whom to send the notifications to in case any sensitive data is lost. NOAA OCIO will distribute an assessment to identify the owners of each of the different sensitive data elements across the organization. The data owners also will be responsible for classifying the information types[5]. Many types of data will have multiple owners, governed by separate line and staff office policies for the collection and use of that data, depending on mission needs. The assessment will attempt to identify each offices ownership, collection, storage, and transmission of sensitive data so that when an incident occurs, the incident is properly triaged, escalated where necessary, reported[6], and the DLP processes and application are modified and tuned as necessary.

Identify Deployment Scenarios

[01] The following questions arise in identifying potential Deployment Scenarios. Each of these must be addressed prior to agency-wide deployment of a mature DLP solution.

1. Will the Initial Deployment be applied to all of the traffic of data in use, or in motion, or at rest?
2. Alternatively, should NOAA deploy the DLP appliance by copying the network traffic and analyzing it at a different port before deploying it directly to the data states of the network traffic?
3. Should the deployment occur in high availability mode or should we configure in bypass mode?
4. How will the setup of endpoints with the DLP manager occur?
5. How do we maintaining integrity between communication ports and firewalls?
6. How do we ensure proper configuration of a crawling agent?

[02] As discussed above, sensitive data falls under three categories, i.e. data in motion, data at rest and data in use. After identifying the sensitive data and defining policies, NOAA will prepare for the deployment of DLP product(s). DLP deployment scenario of all three categories include :

- Data in motion: Data that needs to be protected when in transit, i.e. data on the wire. This includes channels like HTTP/S, S/FTP/S, IM, P2P, SMTP etc. NOAA will install the DLP protector appliance or software so it is not directly inline with the traffic. This is prudent to start with a minimally invasive method by not putting the appliances inline, to prevent a huge number of false positives or a network outage if the inline device fails. The NOAA approach will be to deploy DLP appliances or software in a span port first,

---

[5] See, NIST SP 800-60.

[6] Reporting here is referring to both internal reporting to the Office that owns the information, the Bureau Chief Privacy Officer, and N-CIRT as necessary, as well as external notifications (such as Privacy Incident reporting to DOC) and external reporting to OMB. Organizations report annually on specific privacy and security activities in their annual FISMA reports to OMB. The most recent memorandum is OMB M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, available at http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-15.pdf

and then after the DLP strategy is mature, then put into inline mode. In order to mitigate the second risk, NOAA may deploy two options: first, deploy DLP in High Availability mode, and second, configure the inline DLP product in bypass mode, which will enable the traffic to bypass the inline DLP product in case the DLP product is down.

- Data in Use: Data that resides on the end user workstation and needs to be protected from being leaked through removable media devices like USB, DVD, CDs, etc. will fall under this category. In Data in Use, an agent may be installed in every NOAA endpoint device like laptop, desktop, etc. which is loaded with policies and is managed by a centralized DLP management server. Agents would be distributed on the endpoints via pushing strategies like SMS, GPO, etc.
- Data in Store: Data that resides on file servers and DBs and needs to be monitored from being getting leaked will fall under this category. All NOAA data that resides in storage servers or devices would crawled using a DLP crawling agent. After crawling, data is fingerprinted to see if any unstructured data is present or not.

Plan DLP Operations

[01] NOAA will need to split the DLP operations into three phases: a triaging phase, a reporting and escalation phase, and a tuning phase. The security operation's team will monitor the alerts fired or triggered by the policies set up in the DLP product. N-CIRT will fine tune the policies as a result of some mis-configurations earlier or due to eventual policy or guidance changes and apply the changes to the DLP product. NOAA will need to identify the staffing, budget, training, and other resource demands that each phase of the DLP Operations will require, and determine the capabilities in effectively carrying out each phase with the available resources.

Deploy DLP Product(s)

[01] Deployment of security components is of no use if they cannot be monitored, and a DLP product is no exception. Below is an overview of what a DLP operation of an organization can be. First of all, the DLP product needs to be created with the right set of policies on the identified data among data at rest, in motion or in transit categories. The DLP operations can be separated into three phases, namely: the triaging phase, the reporting and escalation phase, and the tuning phase. These will need to be modified depending on the nature of the incident identified in the triaging phase for referral to N-CIRT and for DOC notification, as necessary. The triaging phase, incident reporting and escalation, as well as the any parameter modifications and tuning will be carried out in accordance with existing PII/BII Breach Response and Notification Plan.

Conclusion

[01] NOAA will employ a Defense in Depth approach to DLP. NOAA's DLP solution(s) need to minimize deployment and operating costs. As an off-the-shelf product, the McAfee Total Protection, or a similar product solution would potentially be an additional tool within the DID approach to effectively protect PII and BII data wherever it may be.

[02] NOAA has maintained a high awareness of data security, and is vigilant in protecting the sensitive information located within its systems. These Data Loss Prevention measures will

enhance the security of NOAA information systems and maintain the highest level of compliance with all regulatory and guidance documents that govern Data Loss Prevention at the agency[7].

Definitions

Business Identifiable Information (BII) Information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person and privileged or confidential." Commercial or financial information is considered confidential if disclosure is likely to cause substantial harm to the competitive position of the person from whom the information was obtained.

Personally Identifiable Information (PII) Information that can be used to distinguish or trace an individual's identity, such as name, Social Security number (SSN), 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. [OMB M-07-16].

Sensitive Personally Identifiable Information (Sensitive PII) Sensitive PII is defined as PII which, when disclosed, could result in harm to the individual whose name or identity is linked to the information. Further, in determining what PII is sensitive, the context in which the PII is used must be considered. For example, a list of people subscribing to a government newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII. As well as context, the association of two or more non-sensitive PII elements may result in sensitive PII. For instance, the name of an individual would be sensitive when grouped with place and date of birth and/or mother's maiden name, but each of these elements would not be sensitive independent of one another. For the purpose of determining which PII may be electronically transmitted, the following types of PII are considered sensitive when they are associated with an individual. Secure methods must be employed in transmitting this data when associated with an individual:

- Place of birth
- Date of birth
- Mother's maiden name
- Biometric information
- Medical information, except brief references to absences from work
- Personal financial information
- Credit card or purchase card account numbers
- Passport numbers

[7] NIST SP 800-53A, Recommended Security Controls for Federal Information Systems, establishes common criteria for assessing the effectiveness of security controls in federal information systems. Organizations use the recommended assessment procedures from NIST SP 800-53A to develop their own assessment procedures.

- Potentially sensitive employment information, e.g., personnel ratings, disciplinary actions, and result of background investigations
- Criminal history
- Any information that may stigmatize or adversely affect an individual.

This list is not exhaustive, and other data may be sensitive depending on specific circumstances. Social Security Numbers (SSNs), including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual. If it is determined that such transmission is required, then secure methods must be employed. [DOC Electronic Transmission of PII Policy].

Controlled Unclassified Information (CUI) Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Signed this ____ day of _____, 2016.

GOLDSTEIN.ZACHARY.G.1228698985

Digitally signed by GOLDSTEIN.ZACHARY.G.1228698985
DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GOLDSTEIN.ZACHARY.G.1228698985
Date: 2016.08.30 15:28:33 04'00'

Zachary Goldstein, NOAA CIO

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Tuesday, November 21, 2017 9:08 AM
To:	Mark Graff NOAA Federal
Subject:	NOAA8223 PTA for signature
Attachments:	NOAA8223_PTA_FY18.pdf

Correct system description and answers to questions (NO PII).

thx Sarah

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

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

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Tuesday, November 21, 2017 9:48 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA8223 PTA for signature
Attachments:	NOAA8223_PTA_FY18 mhg.pdf

You bet 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 Tue, Nov 21, 2017 at 9:26 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> I know. Can you sign and I'll correct?
>
> On Tue, Nov 21, 2017 at 9:14 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
>
> > 4(c) should not have an answer marked if there is no PII in the system. There is no context of PII use if there is no PII.
> >
> > Mark H. Graff
> > FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> > National Oceanic and Atmospheric Administration
> > (301) 628 5658 (O)
> > (b)(6) (C)
> >
> >
> >
> > On Tue, Nov 21, 2017 at 9:08 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> >
> > > Correct system description and answers to questions (NO PII).
> > >
> > > thx Sarah
> > >
> > > Sarah D. Brabson

IT Infrastructure Investment Program Manager
PRA Clearance Officer

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Consolidated Logistics System (CLS) NOAA8223

U.S. Department of Commerce Privacy Threshold Analysis

NOAA National Weather Service, Office of Observations Consolidated Logistics System (CLS) NOAA8223

Unique Project Identifier: NOAA8223

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: Consolidated Logistics System (CLS) is a DOC/NOAA owned logistics software package operated by the National Logistics Support Center (NLSC) and serving as a General Support System (GSS) for the National Weather Service and operations for other US Government agencies. The CLS supports warehouse inventory management functions including shipping and receiving stock; tracking stock items through the quality control process; cyclic stock inventory; on-line customer ordering; stock item management; and data transfer with a number of DOC IT systems. The Weather Logistics Information System (WLIS) is a sub-system of CLS that provides the data transfer functionality with the Department of Defense's MILSTRIP requisitioning system. Barcode technology is prevalent throughout warehouse operations for scanning shipping labels, stock identification labels and stock location labels. Authorized users are employees and contractors of NOAA and NWS, Department of Defense, and the Federal Aviation Administration. Access to CLS information is limited to computers connected to government authorized computer networks and access to CLS functions beyond "View Products" and "View Status" requiring a valid CLS account and password. There is no public access to CLS.

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):					

**YES** ☐ 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..."

___ 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.

_**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 Consolidated Logistics 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 Consolidated Logistics 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):

Steven M. Michnick NOAA8223 System Owner

Signature of SO: Steven M Michnick Digitally signed by MICHNICK.STEVEN.M.1383826469 Date: 2017.11.07 20:54:13 -06'00' 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: 2017.11.20 12:12:45 05'00' Date: _____

Name of Authorizing Official (AO): Joseph A. Pica

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.11.20 16:40:02 -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: 2017.11.21 09:47:57 05'00' Date: _____

Vanessa Rini-Lopez - NOAA Federal

From:	Vanessa Rini Lopez NOAA Federal
Sent:	Wednesday, November 22, 2017 7:43 AM
To:	Mark Graff NOAA Federal
Subject:	Fwd: Login.gov Meeting
Attachments:	LOGIN.GOV_NOAA_MOA20170517 V1.docx

H (b)(5)

Stay tuned.

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)

Forwarded message
From: **Terrance Tielking - NOAA Federal** <terry.tielking@noaa.gov>
Date: Wed, Nov 22, 2017 at 7:26 AM
Subject: Fwd: Login.gov Meeting
To: Vanessa Rini Lopez NOAA Federal <vanessa.rini lopez@noaa.gov>
Cc: Douglas Perry NOAA Federal <Douglas.A.Perry@noaa.gov>, Kenneth Casey <kenneth.casey@noaa.gov>

Vanessa,
(b)(5)
.
Best,
Terry

Forwarded message
From: **Douglas Perry - NOAA Federal** <Douglas.A.Perry@noaa.gov>
Date: Tue, Nov 21, 2017 at 2:55 PM
Subject: Fwd: Login.gov Meeting
To: Irene Parker <irene.parker@noaa.gov>, Kenneth Casey NOAA Federal <kenneth.casey@noaa.gov>, Terrance Tielking <terry.tielking@noaa.gov>
Cc: Emily Ho <emily.s.ho@noaa.gov>, Jerry Mcnamara <jerome.mcnamara@noaa.gov>, Rob Swisher <robert.swisher@noaa.gov>

Terry,

(b)(5) [redacted]

Best regards,

Doug

Forwarded message
From: Zoe Black NOAA AFFILIATE <zoe.black@noaa.gov>
Date: Mon, Oct 30, 2017 at 9:59 AM
Subject: Fwd: Login.gov Meeting
To: Douglas Perry NOAA Federal <Douglas.A.Perry@noaa.gov>

Zoe Black
Contractor - The Ambit Group, LLC
NOAA Office of the Chief Information Officer
((b)(6) [redacted]
Zoe.Black@noaa.gov

Forwarded message
From: **Terrance Tielking - NOAA Federal** <terry.tielking@noaa.gov>
Date: Mon, Oct 30, 2017 at 7:44 AM
Subject: Login.gov Meeting
To: Ann Rivers <Ann.Madden@noaa.gov>
Cc: Emily Ho <emily.s.ho@noaa.gov>, Zoe Black NOAA AFFILIATE <zoe.black@noaa.gov>, "irene.parker" <irene.parker@noaa.gov>, Kenneth Casey <kenneth.casey@noaa.gov>

Ann,
Materials for Oct 31 "Login.gov" meeting with Zach. Let me know if you need anything else. We will need a dial in as one NCEI person will be dialing in from Boulder. Thanks.
Cheers,
Terry

Terrance A. Tielking
Deputy Assistant Chief Information Officer - Satellites (DACIO-S)
National Environmental Satellite, Data and Information Service
National Oceanic and Atmospheric Administration
(O) - (301) 713-7314 / (C) (b)(6) [redacted]

Sent from Gmail Mobile

Terrance A. Tielking

Deputy Assistant Chief Information Officer - Satellites (DACIO-S)
National Environmental Satellite, Data and Information Service
National Oceanic and Atmospheric Administration
(O) - (301) 713-7314 / (C) (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:	Monday, November 27, 2017 3:45 PM
To:	Mark Graff NOAA Federal
Subject:	Re NOAA 23 in new template no changes
Attachments:	NOAA 23 SORN in new template_112717.docx

Mar (b)(5) (b)(5) Did you need to review or should I just forward? Up to you, thx

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

NOAA OCIO
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:	Monday, November 27, 2017 5:04 PM
To:	Toland, Michael; PrivacyAct; Gitelman, Steve (Contractor)
Cc:	Mark Graff NOAA Federal
Subject:	NOAA 23 SORN in new template and small correction to NOAA 16
Attachments:	NOAA 16 updated and in new template_112717 corrected.docx; NOAA 23 SORN in new template_112717.docx

(b)(5)

Thanks, Sarah

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

NOAA OCIO
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)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Tuesday, November 28, 2017 12:29 PM
To:	Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO; Toland, Michael; Cline, Eric (Federal); Brown, Christian (Contractor); DeVore, Ja'Nelle (Federal)
Cc:	Mark Graff NOAA Federal; Andrew Browne NOAA Affiliate; Gary Petroski NOAA Federal
Subject:	Documents for NOAA8884 CRB on 12 7 17
Attachments:	NOAA8884 PIA 11162017 Final mhg.pdf; NOAA8884 SRHQ FY18 privacy control assessment 20171128.xlsx; NOAA8884 PTA 032717 for MHG signature mhg.pdf

All attached are the PIA, PTA and privacy controls assessment (this was the last such assessment not combined with the security controls assessment, before the process changed over).

The SAR will be sent separately via Accellion (and it is in CSAM).

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

NOAA OCIO
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
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.

The only personally identifiable information (PII) maintained in the system is in a local database at the local Weather Forecast Office/River Forecast Center that maintains information on volunteers who provide weather reports to them.

No information is shared except in the case of security or privacy breach (see Section 6.1)

The statutory authorities 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].

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.

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.
__X_ This is an existing information system with no new privacy risks.
____ 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):					

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): General description of volunteer's home location.					

Work-Related Data (WRD)					
a. Occupation		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):					

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)

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		Commercial Data Brokers	
Third Party Website or Application				
Other (specify):				

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		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 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.

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

	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.	
	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: Notice to volunteers is provided when information is collected, via the cooperative agreement 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: 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.
	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.

	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.
	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.
	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):_____**4/39/2017**_____ ☐ 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 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.

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.
	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	
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: Only name and contact information for volunteers, and names of employees, are in the system.
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
X	Context of Use	Provide explanation: Voluntary submission of PII for internal use only
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: 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: Gary Petroski
Office: NOAA/NWS/SRH
Phone: (682) 703-3717
Email: Gary.Petroski@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: PETROSKI.GARY.P.1196647984
Digitally signed by PETROSKI GARY P 1196647984
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn PETROSKI GARY P 1196647984
Date 2017 11 16 14 20 23 06'00'

Information Technology Security Officer

Name: Beckie Koonge
Office: NOAA NWS Office of the CIO
Phone: 301-427-9020
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: KOONGE.BECKIE.A.1408306880
Digitally signed by KOONGE BECKIE A 1408306880
Date 2017 11 17 10 53 28 05'00'

Authorizing Official

Name: Steven Cooper
Office: NOAA/NWS/SRH
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: Steven G. Cooper
Digitally signed by COOPER STEVEN G 1365850930
Date: 2017 11 16 17:13:58 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 2017 11 20 09 15 57 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: 01-2016

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.*

____l 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 l 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.)."

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

____l Companies
____l Other business entities

__X l 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.)*

____1 DOC employees
____1 Contractors working on behalf of DOC
__X 1 Members of the public

____1 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 NOAA8884 and as a consequence of this applicability, I would perform and document a PIA for this IT system. However, there are no new changes creating privacy risks since the PIA was approved by DOC in December 2016.

____ I certify the criteria implied by the questions above **do not apply** to NOAAA8884 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_____

Signature of ISSO or SO: PETROSKI.GARY.P.1196647984 Digitally signed by PETROSKI GARY P 1196647984 DN: c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn PETROSKI GARY P 1196647984 Date: 2017 03 24 09:46:50 05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Beckie Koonge_____

Signature of ITSO: KOONGE.BECKIE.A.1408306880 Digitally signed by KOONGE.BECKIE.A.1408306880 Date: 2017.03.28 15:46:53 04'00' Date: _____

Name of Authorizing Official (AO):

Steven Cooper_____

Signature of AO: COOPER.STEVEN.G.1365850930 Digitally signed by COOPER.STEVEN.G.1365850930 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=COOPER.STEVEN.G.1365850930 Date: 2017.03.24 15:19:52 -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: 2017.04.11 10:24:43 -04'00' Date: _____

(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)

Maurice Mcleod - NOAA Federal

From:	Maurice Mcleod NOAA Federal
Sent:	Wednesday, November 29, 2017 11:18 AM
To:	Sarah Brabson NOAA Federal
Cc:	John D. Parker NOAA Federal; Mark Graff NOAA Federal; Andrea Hardy NOAA Federal; Amanda Wallace NOAA Federal; Ezekiel Abiodun NOAA Affiliate
Subject:	Re: Policy Notification: New NOAA Guidance for Annual Privacy Impact Analysis (PIA)
Attachments:	PTA_NOAA6205_ 2017.docx

As requested.

On Wed, Nov 29, 2017 at 10:19 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Just noticed your 2017 PTA is overdue, last one was 9 12 16. Please do a new one with no changes, so it's consistent with the last PIA, and send to me in Word for review before you get signatures. I need to send this to DOC along with the other docs.
>
> thx Sarah
>
> On Wed, Nov 29, 2017 at 10:17 AM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
>
> > Thank you.
> >
> > On Wed, Nov 29, 2017 at 10:16 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> >
> > > Now sending to Mark for signatures. sb
> > >
> > > On Tue, Nov 28, 2017 at 4:13 PM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
> > >
> > > > Excellent, thank you.
> > > >
> > > > On Tue, Nov 28, 2017 at 4:08 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> > > >
> > > > > Thanks, Maurice! This is two in one day! Will do quick review and send to Mark in the am.
> > > > >
> > > > > sb
> > > > >
> > > > > On Tue, Nov 28, 2017 at 4:06 PM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
> > > > >
> > > > > > Attached are the PIA Annual Review Certification Form, previously approved PIA with new signatures, and the link to the latest version of NOAA6205's security controls assessment:

(b)(5)

> > > > > > On Thu, Oct 19, 2017 at 10:02 AM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:

All,

NOAA Guidance on PIA Annual Review Process:

1. Download the **NOAA6NNN PIA Annual Review Certification Form** located at (remove extra spaces):
    - **http:// business.nos.noaa/cio/ITOB/SecCom/Shared Documents/Policies/NOAA Policies/NOAA Privacy Guidance-PIA-PTA Templates**
2. Complete the DOC PIA Annual Review Certification Form
    - PIA Reviewer can be any of the following individuals: ISSO, SO, AO, ITSO
3. PIA Reviewer digitally sign as the "Name of Reviewer"
4. The previously approved PIA must be resigned. No other changes must occur to the previously approved PIA other than new signatures.
    - You will need to create a new PDF of the previously approved PIA without signatures
    - Then circulate the new PDF of the previously approved PIA for signatures.
5. You will need to provide Mark and Sarah the latest version of your security controls assessment results.
    - I recommend you post the file to CSAM and include the link in the email.
    - Do not use Google email to send the security control assessment results, only use Accellion.
6. Send email and attached the **NOAA6NNN PIA Annual Review Certification Form,** previously approved PIA with new signatures and include a link to your latest version of your security controls assessment (in CSAM) to:
    - Sarah Brabson <sarah.brabson@noaa.gov>
    - Mark Graff <mark.graff@noaa.gov>
    - cc: John D Parker <John.D.Parker@noaa.gov>

DOC Privacy Program Plan, September 2017 is available at (remove extra spaces):

http://www. osec.doc.gov/opog/privacy/Memorandums/PRIVACY_PROGRAM_PLAN_2017.pdf

As a reminder, in October 2012, Zach Goldstein issued a policy memorandum requiring annual review of Privacy Threshold Analysis (PTA). The memorandum is available at (*remove extra spaces from link below*):

http:// business.nos.noaa/cio/ITOB/SecCom/Shared%20Documents/Policies/NOAA%20Policies/Policy%20Memoradums/2012-11-01%20Memo-%20Annual%20review%20of%20NOAA%20FISMA%20Systems%20PTA.pdf

PTA annual review includes obtaining the latest template (NOAA Privacy web link below), completing the template, obtaining the required approvals and having the independent assessor review the approved PTA. The PTA requires approval by:

- Information System Security Officer (ISSO) or System Owner (SO)
- Information Technology Security Officer (ITSO)
- Authorizing Official (AO)

- Bureau Chief Privacy Officer (BCPO)

NOAA Privacy web site (*remove extra spaces from link below*):

http://www. cio.noaa.gov/services_programs/privacy.html

NOAA IT Policies, Policy Memo and Guidance covering NOAA CIO and Privacy policies (*remove extra spaces from links below*):

https://www. csp.noaa.gov/policies/manual/212-1301-V5-6-final.pdf

https:// sites.google.com/a/noaa.gov/cio/internal-use-only/it-governance?pli=1

http://www. cio.noaa.gov/services_programs/privacy.html

https://www. csp.noaa.gov/policies/NOAA_Rules_of_Behavior.xhtml

DOC IT Policies, Policy Memos, Frequently Asked Questions and Guidance covering DOC CIO and DOC Privacy policies (*remove extra spaces from links below*):

http:// connection.commerce.gov/policy/20140528/it-security-program-policy-commerce-information-technology-requirements-and-policy

http:// connection.commerce.gov/collection/it-security-policy-and-fisma-reporting-program

http://www. osec.doc.gov/opog/privacy/laws_and_regs.html#DOCPolicies

http://www. osec.doc.gov/opog/privacy/compliance.html#approvedpias

http://www. osec.doc.gov/opog/privacy/Memorandums/PRIVACY_PROGRAM_PLAN_2017.pdf

NOS ITSP has posted DOC and NOAA Policies, Policy Memos, Frequently Asked Questions and Guidance (*remove extra spaces from links below*) at:

http:// business.nos.noaa/cio/ITOB/SecCom/Shared%20Documents/Policies/

If you have any question, please contact the NOS.ITSP@noaa.gov or call John Parker/John Dandy/Marie Murphy for assistance.

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

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (b)(6)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Purvis, Catrina (Federal)

Subject:	CRB NOAA8884
Location:	Open Office 52017 (SMC) Md Conf Rm Dial in number: (b)(6) (b)(6)
Start:	Thursday, December 7, 2017 9:30 AM
End:	Thursday, December 7, 2017 10:00 AM
Recurrence:	(none)
Meeting Status:	Not yet responsed
Organizer:	Purvis, Catrina (Federal)
Attachments:	NOAA8884 PTA 032717 for MHG signature mhg.pdf; NOAA8884 PIA 11162017 Final mhg.pdf

Updated to add PIA/PTA

Mark/Sarah

Please provide the signed PIA/PTAs for the system identified above by 10am Tuesday, December 5 to avoid cancellation of this meetings.

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) 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.

The only personally identifiable information (PII) maintained in the system is in a local database at the local Weather Forecast Office/River Forecast Center that maintains information on volunteers who provide weather reports to them.

No information is shared except in the case of security or privacy breach (see Section 6.1)

The statutory authorities 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].

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.

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.
__X_ This is an existing information system with no new privacy risks.
____ 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):					

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): General description of volunteer's home location.					

Work-Related Data (WRD)					
a. Occupation		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):					

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)

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		Commercial Data Brokers	
Third Party Website or Application				
Other (specify):				

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		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 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.

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

	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.	
	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: Notice to volunteers is provided when information is collected, via the cooperative agreement 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: 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.
	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.

	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.
	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.
	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):_____**4/39/2017**_____ ☐ 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 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.

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.
	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	
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: Only name and contact information for volunteers, and names of employees, are in the system.
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
X	Context of Use	Provide explanation: Voluntary submission of PII for internal use only
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: 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: Gary Petroski
Office: NOAA/NWS/SRH
Phone: (682) 703-3717
Email: Gary.Petroski@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: PETROSKI.GARY.P.1196647984
Digitally signed by PETROSKI GARY P 1196647984
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn PETROSKI GARY P 1196647984
Date 2017 11 16 14 20 23 06'00'

Information Technology Security Officer

Name: Beckie Koonge
Office: NOAA NWS Office of the CIO
Phone: 301-427-9020
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: KOONGE.BECKIE.A.1408306880
Digitally signed by KOONGE BECKIE A 1408306880
Date 2017 11 17 10 53 28 05'00'

Authorizing Official

Name: Steven Cooper
Office: NOAA/NWS/SRH
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: Steven G. Cooper
Digitally signed by COOPER STEVEN G 1365850930
Date: 2017 11 16 17:13:58 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 2017 11 20 09 15 57 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: 01-2016

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.*

____l 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 l 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.)."

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

____l Companies
____l Other business entities

__X l 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.)*

____1 DOC employees
____1 Contractors working on behalf of DOC
__X 1 Members of the public

____1 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 NOAA8884 and as a consequence of this applicability, I would perform and document a PIA for this IT system. However, there are no new changes creating privacy risks since the PIA was approved by DOC in December 2016.

____ I certify the criteria implied by the questions above **do not apply** to NOAAA8884 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_____

Signature of ISSO or SO: PETROSKI.GARY.P.1196647984 Digitally signed by PETROSKI GARY P 1196647984 DN: c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn PETROSKI GARY P 1196647984 Date: 2017 03 24 09:46:50 05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Beckie Koonge_____

Signature of ITSO: KOONGE.BECKIE.A.1408306880 Digitally signed by KOONGE.BECKIE.A.1408306880 Date: 2017.03.28 15:46:53 04'00' Date: _____

Name of Authorizing Official (AO):

Steven Cooper_____

Signature of AO: COOPER.STEVEN.G.1365850930 Digitally signed by COOPER.STEVEN.G.1365850930 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=COOPER.STEVEN.G.1365850930 Date: 2017.03.24 15:19:52 -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: 2017.04.11 10:24:43 -04'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, November 30, 2017 1:33 PM
To:	Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO
Cc:	Mark Graff NOAA Federal; John D. Parker; MaryLouise Kurchock NOAA Federal
Subject:	NOAA6501 certification
Attachments:	NOAA6501_PTA_FY2018 (template 01 2015) (signed) mhg.pdf; NOAA6501_PIA_11 22 2016 (FY2018 annual review) for signatures sms mhg.pdf; NOAA6501_PIA_Annual Review Certification FY2018 (isso signed) mhg.pdf

I have attached the signed certification, the PIA with new signatures, and the current PTA.

The ATO date is 3 31 18.

thx Sarah

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

NOAA OCIO
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
NOAA6501, Nautical Charting System

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/Nautical Charting System

Unique Project Identifier: UPI Code: 006-48-01-15-01-3401-00

Introduction: System Description

NOAA6501 is an enterprise information system for all actions requiring IT resources for the Office of Coast Survey's (OCS's) mission and organizational administrative functionality. NOAA6501 acquires, processes, and stores internal service delivery information and the following mission information: Geographic Information System (GIS) Application Development, Marine Modeling Applications, Hydrographic Processing Applications, Modeling Data, Geographic Information System Application and Geographic Information System Data.

The OCS collects National and International navigationally relevant and significant source data as required by NOAA's nautical charting and International Hydrographic Office policy and procedures, in order to produce nautical chart, services, and products. All relevant and significant source data received is registered into the internal Marine Chart Division's Data Registry (DREG) system. The OCS coordinates with multiple external federal and state organizations as well as multiple private entities to receive navigational relevant and significant data which is used to update the charting databases. The OCS mission nautical data does not contain PII, but PII is collected from members of the public who submit nautical chart information. This submitted PII is contact information.

Mission data and applications are related to hydrographic processing, hydrographic and cartographic research and development, marine modeling, customer outreach, and nautical products and services. NOAA6501 gathers and stores PII related to hired employees and contractors of the Office of Coast Survey which is collected, stored and maintained for Human Resource-related issues as well as workforce planning, operating budget, COOP Operations, and documentation. OCS collects BII during the pre and post activities associated with the acquisition and management of contracts.

Information Sharing

OCS collects and stores limited PII, specifically, name, telephone numbers and email addresses (voluntarily submitted by data providers and customers) to facilitate external coordination with data providers and to provide responses to customer service related requests from the diverse community of customers.

NOAA6501 as a General Support System for Office of Coast Survey, collects PII as part of the application and hiring of employees (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, information for security badging process, and performance appraisal ranking).

Sensitive PII, such as SSN or financial information, is entered by the employee either on printed form for NOAA Badging or directly into NFC, Travel, or Workforce management application outside of the boundary of NOAA6501.

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

OCS 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 employee PII or BII information. OCS does not have a separate HR division since OCS utilizes the NOAA Workforce Management Office.

Final OCS mission digital data products and services (i.e. Booklet Charts; ENCs; Online Chart Viewer) are delivered to our partners and customers through the downloading of the products and services from OCS's public Web site, http://www.nauticalcharts.noaa.gov. These entities consist, for example, of other NOAA offices, United States Coast Guard, Federal Aviation Administration, the maritime community and the general public.

(a) a citation of the legal authority to collect PII and/or BII:
5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

For PIAs covered, or also covered, by the SORN COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission, 15 U.S.C. § 1512 applies. It is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is: *Overall: Moderate* [Confidentiality Low/ Integrity-Moderate/ Availability-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: N/A					

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): OCS utilizes NOAA for workforce management and NOAA Office of security for badging. General employee information is retained for teleworking agreements and COOP.					

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	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): OCS does not capture photographs for badging since that is performed (and stored) by the NOAA Office of Security. OCS does utilize pictures of specific individuals (with written permission) as part of either internal or external website as part of OCS program, possible profile narrative, and/or presentation of OCS mission nautical activities.					

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) 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.

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		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify) :					

Non-government Sources					
Public Organizations	x	Private Sector	x	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): OCS does not acquire PII from other non-government sources. These non-government sources would be only for BII associated with Pre/Post Acquisition Sensitive Information obtained through delivered bids on OCS 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	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): Collected BII would be associated with determine qualification/eligibility for open acquisitions. PII would be collected for OCS administrative actions, for HR and Workforce management.			

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).

Office of Coast Survey collects PII as part of the application and hiring of employees (electronic copies of resumes and hiring ranking are stored temporary during the hiring phase), including standard HR information (such as Travel authorization and vouchers, passports and international travel forms, information for security badging process, and performance appraisal ranking). OCS' employee and contractor data is collected, stored and maintained for internal OCS COOP, Human Resource, and workforce planning purposes (federal employee/contractor). The storage is in the form of PDF forms or MS Word documents in a secure folder on OCS network. No SSN is collected or stored within NOAA6501. Sensitive PII, such as SSN or financial information, is entered by the employee either on printed form for NOAA Badging or directly into NFC, Travel, or Workforce management application outside of the boundary of NOAA6501.

OCS's contact information (members of the public, other federal, state and private organizations) is collected to provide a means for the Office of Coast Survey to communicate and respond to needs and requests. OCS mission data is shared with multiple external federal and state organizations as well as multiple private entities to receive navigational relevant and significant data which is used to update

the charting databases. In addition, the OCS system communicates with the diverse community of national and international chart product and services users.

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):			

Internal OCS employees' PII is collected for appropriate Human Resource records, COOP Operations /documentation and workforce planning internal to OCS. Since OCS is a NOAA program office under the NOS Line Office, some HR related information will be shared with NOS and NOAA workforce management offices as required to handle HR activities and workforce management.

	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. NOAA6501 is connected to the NOS Line Office information system NOAA6001 and other NOAA information systems for VPN, Security and Network Operations. ***NOAA6501 does NOT share or received PII or BII through these technical infrastructure (backbone) connections.*** OCS 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: http://www.nauticalcharts.noaa.gov/staff/privacy_policy.htm. *A Privacy Act Statement is being processed through OCS and NOS website governance and the OCS Configuration Management process in order to incorporate it into applicable OCS Web pages.*	
x	Yes, notice is provided by other means	Specify how: The contact information is collected through NOAA6501 Web-based applications: CCWEB and Nautical Discrepancy Report System. The Web-based applications request user email address via a Web-based form to facilitate communication and OCS response. b. Notice was provided to partners and customers for the following: • CCWeb data collection; Federal Register Vol. 69, No. 189 Sept. 30, 2004 • ChartFacilities data collection from Marina Owners or Marina Operators; • Register Vol. 69, No. 85 May 3, 2004 (Planned Data Collection).

		These information collections are voluntary. By providing the data through the CCWeb site, the individual consents to its use. United States Power Squadron (USPS) users can access OCS information only by entering in their USPS certificate numbers and a DOC-compliant password which is validated as part of the authentication control. As of 5/1/2016, the CCWEB site was removed, but information is being included in the PIA in case the organization re-establishes the website. Nautical Discrepancy Report System is still available to the public at http://ocsdata.ncd.noaa.gov/idrs/discrepancy.aspx Employees are given notice on the applicable HR 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: Navigational information collections are voluntary. By providing the data through the email or online forms, the individual consents to its use for the purpose of follow-up contact on information provided. OCS administrative PII is collected through the employee's application for employment and workforce management. The employee is fully informed of how the information will be utilized when collected, during the onboarding process. The employment application contains the Privacy Act notice. Applicants have the opportunity to decline to provide PII, in writing, to the HR representative or to their supervisors, but it might affect the overall processing of their employment. BII can be declined to be provided as part of the acquisition package but could impact evaluation of bid.
	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: Navigation information collections are voluntary. By providing the data through the email or online forms, the individual consents to its use for the purpose of follow-up contact on information provided. OCS administrative PII is collected through the employee's application for employment and workforce management. The employee is fully informed of how the information will be utilized when collected. 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 to their supervisors, but it might affect the overall processing of their employment. BII are submitted for a specific purpose which consent is implied with the submittal of the package.
	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: Those accessing information can contact OCS directly by email or phone as listed in the Privacy policy on the NauticalCharts.Noaa.Gov page OCS 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.
	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 agreements.

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: Access to storage folders are restricted by ACL but since PII is not centralized in a database it cannot be easily monitored for access.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 4/22/2016 (next is 12/1/2016) ☐ 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 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 NOAA6501 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 OCS Information System Security Officer for authorization and mission 'need-to-know' requirement prior to implementation. Least privilege was 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 DOC Accellion for encryption in transit.

OCS implements those security controls listed in NIST Special Publication 800-53 R4 required for a Moderate System. NOAA6501 is under a current Authorization To continue to Operate (ATO) signed 03/29/2017. In compliance with NIST Special Publication 800-53, the Office of Coast Survey has a full security program, with performance measures and goals, in order to complete continuous monitoring activities (annual security control reviews, quarterly vulnerability scanning, monthly review of security access control list, weekly review of audit logs, daily handling of Access Change Requests and involved in OCS Change Board activities). The risk assessment included the possible threats and vulnerability to the confidentiality, integrity, and availability of mission and sensitive PII data along with the countermeasures.

Every year the IT system undergoes a thorough Continuous Monitoring for the Assessment and Authorization (A&A) process that is performed independent contractor. The A&A process ensures

that the security plan and operational, management, and technical controls meet Department of Commerce (DOC) 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)*: NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons 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. 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 OCS 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

	OCS's contact information (contractor, partner, and customer) are 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. OCS mission data is associated with Water Transportation and Navigation and does not contain PII data. Only the "historical" chart information is retained indefinitely due to the nature of the information. All other mission data would be retained as long as the information is required to produce the OCS deliverable and each project would establish the records retention scheduled based on the project, model, or deliverable. All mission data is releasable as "public-accessible" information and does not contain PII. NOS Records Disposition schedule for the information system for mission data: N1-370-00-3 Nautical Mapping and Charting 1604-01 to 1604-13 (PII not contained in this record set)
	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.

	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: Administrative PII is not stored in a centralized database, application or location. Most MS Word documents would be stored across the OCS network and would require time to search all network resources to locate PII.
x	Quantity of PII	Provide explanation: OCS has a limited quantity of PII necessary for HR actions and management.
x	Data Field Sensitivity	Provide explanation: OCS has a limited quantity of sensitive PII information necessary for HR actions and management OCS does not store SSN.
x	Context of Use	Provide explanation: This is only limited PII with a specific HR purpose utilized by HR personnel or supervisors.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: Documents are stored to restricted shared networks, restricted based on single individual or OCS division based on need to know basis.
x	Other:	Provide explanation: The loss of a single individual's PII would have an impact on that individual through possible identify theft and OCS as a government identity BUT it would not have an impact on the OCS mission dealing with nautical data, products, and services.

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: A Privacy Act statement added to the OCS Web site. *No change to current OCS business processes, but OCS will be issuing formal policy to reinforce that the storage or retention of SSN is not authorized on any component within NOAA6501.*
	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: Mary Louise A. Kurchock Office: NOS, Office of Coast Survey Phone: 301-713-4545 x205 Email: MaryLouise.Kurchock@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: KURCHOCK.MARY LOUISE.A.1388550917 Digitally signed by KURCHOCK.MARY LOUISE.A.1388550917 Date: 2017.11.21 12:53:54 05'00' Date signed:	**Information Technology Security Officer** Name: John D. Parker Office: National Ocean Services 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: 2017.11.27 09:44:06 05'00' Date signed:
Authorizing Official Name: Shepard M. Smith Office: National Ocean Services Phone:317-713-2770 x134 Email:Shep.Smith@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: SMITH.SHEPARD.M.1006778930 Digitally signed by SMITH.SHEPARD.M.1006778930 Date: 2017.11.28 08:16:24 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: 2017.11.28 14:13:43 -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 PI-

U.S. DEPARTMENT OF COMMERCE

Department of Commerce

Privacy Impact Assessment (PIA)
Annual Review Certification Form

September 2017

Prepared by:
Office of Privacy and Open Government (OPOG)
DOC Privacy Program Plan Appendix L

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

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

Name of PIA: Nautical Charting System

FISMA Name/ID (if different): NOAA6501

Name of IT System/ Program Owner: Office of Coast Survey

Name of Information System Security Officer: Mary Louise A. Kurchock

Name of Authorizing Official(s): RDML Shepard M. Smith/ Hugh R. Johnson

Date of Last PIA Compliance Review Board (CRB): 11/22/2016

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

Date of PIA Review: 10/20/2017

Name of Reviewer: Mary Louise A. Kurchock

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: KURCHOCK.MARY LOUISE.A.1388550917 Digitally signed by KURCHOCK.MARY LOUISE.A.1388550917 Date: 2017.10.20 07:56:14 -04'00'

Date of BCPO Review: 11.28.17

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 2017 11 28 14 12 56 05'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA6501, Nautical Charting System
Office of Coast Survey, NOS, NOAA

U.S. Department of Commerce Privacy Threshold Analysis

[NOAA6501, Nautical Charting System
Office of Coast Survey, NOS, NOAA

Unique Project Identifier: NOAA6501
UPI Code: 006-48-01-15-01-3401-00

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: NOAA6501 is an enterprise information system for all actions requiring IT resources for the Office of Coast Survey's mission and organizational administrative functionality. NOAA6501 acquires, processes, and stores internal service delivery information and the following mission information: GIS Application Development, Marine Modeling Applications, Hydrographic Processing Applications, Modeling Data, Geographic Information System Application and Geographic Information System Data.

The OCS collects National and International navigationally relevant and significant source data as required by NOAA's nautical charting and International Hydrographic Office policy and procedures. All relevant and significant source data received is registered into NCS Data Registry (DREG) system. The OCS interfaces with multiple external federal and state organizations as well as multiple private entities to receive navigational relevant and significant data which is used to update the charting databases.

Final digital data products and services (i.e. Booklet Charts; ENCs; Online Chart Viewer) are delivered to our partners and customers through the downloading of the products and services from OCS's public Web site, http://www.nauticalcharts.noaa.gov. This Web site is supported by the NOAA Web Operations Center, WOC (NOAA0100). These entities consist, for example, other NOAA offices, United States Coast Guard, Federal Aviation Administration, the maritime community and the general public.

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.)."

__X__ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)* **(NOTE only collect and maintain BII for internal OCS purpose.)**

__X__ Companies **(NOTE: only collected through the Pre-Acquisition process through submitted technical/financial proposals for OCS contracts**.)

____ 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 **(NOAA employee's HR PII)**

_X__ Contractors working on behalf of DOC **(Only general business contact information.)**

_X__ Members of the public **(Only general business contact information)**

____ 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. **(Note: Collects and maintains PII but NOT user ID such as social security number).**

____ 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 NOAA, NOS, Office of Coast Survey, NOAA6501 *Nautical Charting 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 [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): Mary Louise A. Kurchock

Signature of ISSO: KURCHOCK.MARY LOUISE.A.1388550917 Digitally signed by KURCHOCK.MARY LOUISE.A.1388550917 Date: 2017.10.04 08:03:57 -04'00' 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: 2017.10.20 08:12:17 -04'00' Date: _____

Name of Authorizing Official (AO): RDML Shepard Smith

Signature of AO: SMITH.SHEPARD.M.1006778930 Digitally signed by SMITH.SHEPARD.M.1006778930 Date: 2017.10.26 08:37:50 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: 2017.10.26 13:38:29 -04'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, December 4, 2017 12:29 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA8873 PTA for signature
Attachments:	NOAA8873_PTA_Nov2017 SIGNED.pdf

They still need to add the new PAS to the rules of behavior. I updated the PIA and added current signatures.

And here's the PTA.

thx Sarah

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

NOAA OCIO
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, December 4, 2017 12:25 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA4020 revised PTA for signature
Attachments:	NOAA4020 PTA 2017 revised description_for BCPO signature.pdf

Mark, we should receive the PIA shortly but could you sign this in the meantime? thx, Sarah

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

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

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, December 4, 2017 12:47 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA4020 revised PTA for signature
Attachments:	NOAA4020 PTA 2017 revised description_for BCPO signature mhg.pdf

(b)(5)

Here it is signed, but just add that narrative and this is good to 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, Dec 4, 2017 at 12:24 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, we should receive the PIA shortly but could you sign this in the meantime? thx, Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> NOAA OCIO
> 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 Threshold Analysis
for the
NOAA4020
Office of Science and Technology

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Office of Science and Technology

Unique Project Identifier: 006-48-01-14-02-3305-00

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 and its purpose 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 NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

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): New application (NIMM) rolled out in 7/17.					

____ 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.

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

NOAA 4020 contains a variety of PII and BII, including permit application data and loan application data.

____ 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 [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: TAYLOR.GLEN.CLIFFORD.1365840934 Digitally signed by TAYLOR GLEN CLIFFORD 1365840934 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=TAYLOR GLEN CLIFFORD 1365840934 Date: 2017 11 15 12:48:07 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2017.12.04 12:03:34 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn CYR.EDWARD.C.DR.1365869436 Date: 2017.11.15 15:59:45 -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: 2017.12.04 12:47:03 -05'00' Date: _____

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, December 4, 2017 12:55 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA8873 PTA for signature
Attachments:	NOAA8873_PTA_Nov2017 SIGNED mhg.pdf

Here is 8873 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, Dec 4, 2017 at 12:29 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> They still need to add the new PAS to the rules of behavior. I updated the PIA and added current signatures.
>
> And here's the PTA.
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> NOAA OCIO
> 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
NOAA8873-National Data Buoy Center (NDBC)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NDBC

Unique Project Identifier: NOAA8873

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 Data Buoy Center (NDBC), a part of the National Oceanic and Atmospheric Administration (NOAA), National Weather Service (NWS), provides comprehensive, reliable systems and marine observations to support the missions of the NWS and NOAA, promote public safety, and satisfy the future needs of our customers. NDBC operates three major buoy arrays as well as a network of coastal marine observing stations. These systems provide critical data on oceanic and atmospheric conditions that is used by weather and hurricane forecasters, researchers, climatologists, oceanographers, commercial fishers, and recreational boaters, among others.

The NDBC manages the development, operations, and maintenance of the national data buoy network. It serves as the NOAA focal point for data buoy and associated meteorological and environmental monitoring technology. It provides high quality meteorological/environmental data in real time from automated observing systems that include buoys and a Coastal-Marine Automated Network (C-MAN) in the coastal zone surrounding the United States and the open ocean. It provides engineering support, including applications development, and manages data buoy deployment and operations, and installation and operation of automated observing systems installed on fixed platforms. It hosts the Volunteer Observing Ship (VOS) program to acquire additional meteorological and oceanographic observations supporting NWS mission requirements.

NDBC is located at the Stennis Space Center in Bay St. Louis, Mississippi, and has operated a network of off-shore weather buoys and unmanned coastal observing stations (Coastal Marine Automated Network or C-MAN stations) since 1990. In 2001 and 2005 respectively, NDBC began to assume responsibility for operating moored buoys supporting NOAA's Deep-Ocean Assessment and Reporting of Tsunami (DART) program and the Tropical Atmosphere Ocean (TAO) program that were developed and formerly operated by NOAA's Pacific Marine Environmental Laboratory (PMEL).

NDBC currently operates and maintains 195 moored buoys and 46 C-MAN stations. The U.S. Coast Guard provides ship transit services for NDBC so that it can repair and maintain its weather buoys. The Coast Guard also maintains a small staff at NDBC. NOAA vessels provide support for the NDBC mission when their schedules allow. NDBC also leases privately-owned vessels when required to support the mission and maintenance schedules.

Surveys of meteorologists have shown about 40 percent of NWS marine warnings and advisories are based, at least in part, on NDBC's meteorological data. In addition to this critical purpose, the observations are used by meteorologists who need to adjust flight level wind speeds reported by hurricane reconnaissance aircraft to surface winds; by geophysicists who use our sea surface temperature, wind, and wave reports to help calibrate remotely sensed measurements from spacecraft; and by engineers who obtain directional wave measurements to study beach erosion and shore protection. Additionally, surfers, fishermen, and boaters acquire the reports via the Internet to help them determine if they want to venture offshore.

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): *Images collected from buoys outfitted with cameras*					

____ 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 NDBC currently has a video surveillance system installed in the data center to monitor physical access to the restricted area. In addition, access to the information technology (IT) areas is physically controlled via room entry readers. Select buoys are outfitted with cameras to collect visual environmental data and images collected are stored on the information system.

____ 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 NOAA8873 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 NOAA8873 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): Joy Baker, ISSO

Signature of ISSO or SO: BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER.JOY.ALLISON.1269758577 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BAKER.JOY.ALLISON.1269758577 Date: 2017.11.30 09:25:26 -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: 2017.11.30 10:28:55 05'00' Date: _____

Name of Authorizing Official (AO): Joseph Pica, AO

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.12.04 09:28:22 -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: 2017.12.04 12:49:57 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, December 4, 2017 3:35 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA4300 PTA for signatrue
Attachments:	NOAA4300 PTA 20171129 initial.pdf

All good. No new privacy risks sets the stage for a certification later.

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

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

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Monday, December 4, 2017 3:40 PM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA4300 PTA for signatrue
Attachments:	NOAA4300 PTA 20171129 initial mhg.pdf

No problems 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, Dec 4, 2017 at 3:35 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> All good. No new privacy risks sets the stage for a certification later.
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> NOAA OCIO
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Version Number: 01-2015

U.S. Department of Commerce
National Marine Fisheries Service

Privacy Threshold Analysis
for the
NOAA4300 Southeast Regional Office LAN

November 29, 2017

U.S. Department of Commerce Privacy Threshold Analysis

NMFS SERO / NOAA4300

Unique Project Identifier: NOAA4300

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 and its purpose 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 Southeast Regional Office NOAA4300 system functions as the overall office automation support system for the NOAA/NMFS offices in St. Petersburg, Florida. It provides access to automated systems typically found in administrative offices within the federal government. It supports all offices within the SER which include the Regional Administrator's Office; Operations, Management & Information Services Office; Economics Office; State/Federal Liaison Office; Sustainable Fisheries Division; Protected Resources Division; and Habitat Conservation Division. The system also supports non-SERO offices located in St. Petersburg including NOAA SE Office of General Counsel (GCSE) and NMFS SE Financial Services office.

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. Permit related information, as well as PII regarding SERO employees and contractors, is processed by staff whose job duties require access to that information.

____ 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 - Permit related BII is collected and maintained.
____ 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 NOAA4300 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):
Eric Barton - ISSO / Kevin McIntosh - Acting System Owner

Signature of ISSO or SO: BARTON.ERIC.H.1365837321 Digitally signed by BARTON.ERIC.H.1365837321 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BARTON.ERIC.H.1365837321 Date: 2017.11.29 14:49:19 -05'00' Date: 11/29/2017

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2017.12.04 15:04:14 05'00' Date: _____

Name of Authorizing Official (AO): Rod E. Crabtree

Signature of AO: [signature] Date: 11/29/17

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: 2017.12.04 15:39:02 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, December 4, 2017 4:37 PM
To:	Gioffre, Kathy (Federal); CPO; Ferguson, Dorrie; Toland, Michael
Cc:	Mark Graff NOAA Federal; Joy Baker NOAA Federal
Subject:	Revised NOAA8873 docs per CRB
Attachments:	NOAA8873_PTA_Nov2017 SIGNED mhg.pdf; NOAA8873 COOP form with PA Statement.docx; NOAA8873_PIA_113017 per CRB.pdf; NOAA8873(11 30 17)Final_NOAA response.docx

Attached are the revised PIA, PTA and form with revised PAS. Note, this is now a COOP form only, with no need to specify to which part of the form the revised Disclosure paragraph applies. The ROB is no longer being used.

Also attached are the annotated CRB minutes.

thx Sarah

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

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

Continuity of Operations Plan (COOP) Personal Data Provision

The National Data Buoy Center (NDBC) collects personal data (i.e., name, home address, home phone, etc.) for COOP purposes.

Privacy Act Statement (PAS)

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA collects this information for the purpose of facilitating external coordination with Nautical Charting System data providers and to provide responses to customer service related requests from the diverse community of customers.

NOAA Routine Uses: NOAA will use this information to enable communication with data providers and customers of the NDBC system. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)** to be shared among NOAA 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-18, Employees Personnel Files Not Covered by Notices of Other Agencies.

Disclosure: Furnishing this information is mandatory. The failure to provide accurate information may delay or prevent you from receiving notifications in the event of an emergency. The failure to provide this information also may have an effect on your Federal service under certain circumstances. For example, failure to supply this information may delay or make it impossible to notify you in the event of an emergency about a change to your duty location and/or the Department's needs for your service in an emergency, which may result in you being placed in an absent without leave status.

By signing this document, I, , understand and agree.

_____ _____

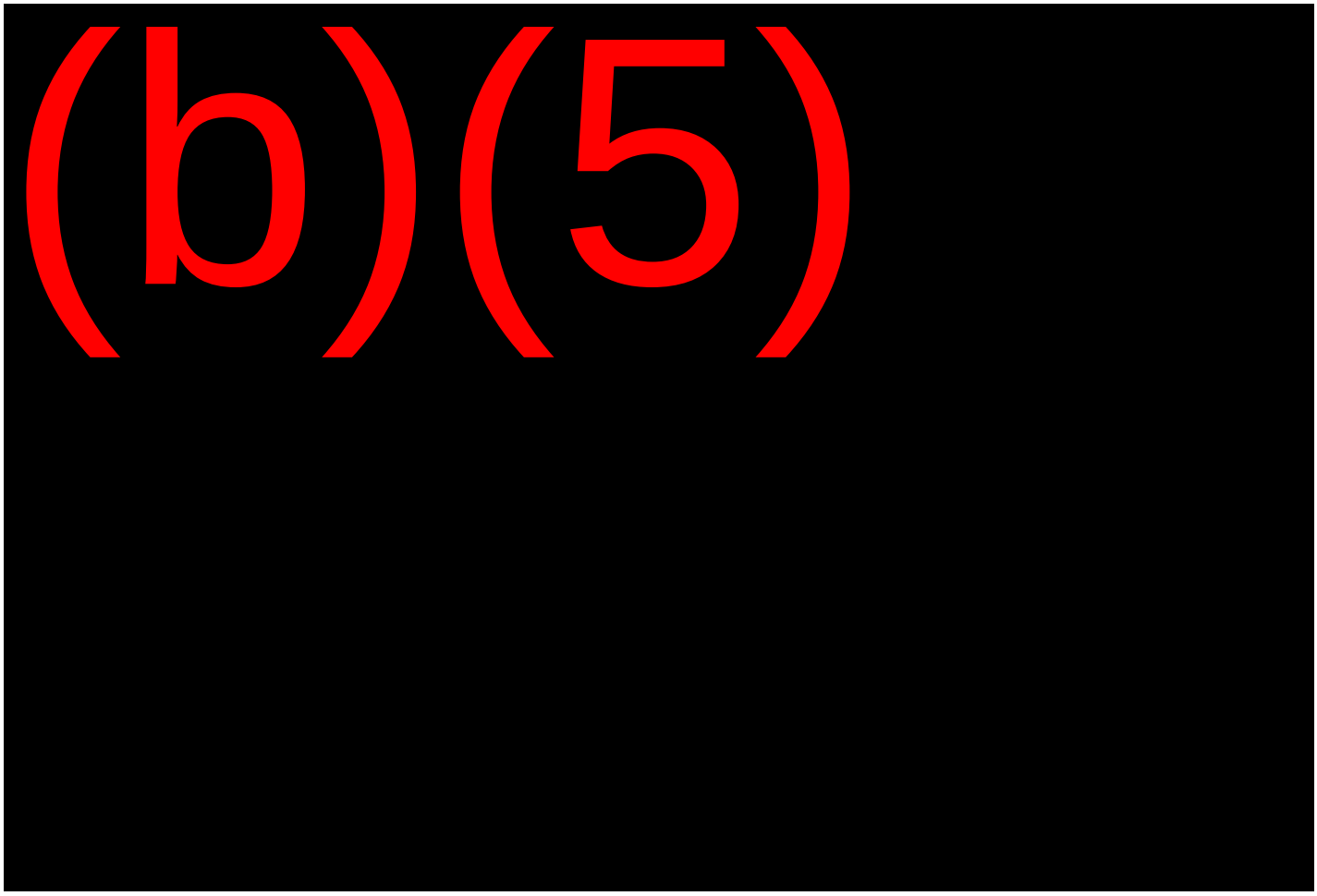
Employee Signature Date

Privacy Impact Assessment (PIA) Compliance Review Board (CRB) Meeting Minutes
NOAA National Data Buoy Center (NDBC) (NOAA8873)
November 30, 2017

Attendees:

Privacy Team
Kathy Gioffre
Mike Toland
Dorrie Ferguson
Christian Brown (OCIO)

NOAA
Mark Graff
Sarah Brabson
Joy Baker
Shannon MacArthur



Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA8873
National Data Buoy Center (NDBC)

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/NDBC

Unique Project Identifier: NOAA8873

Introduction: System Description

(a) General Description

The National Data Buoy Center (NDBC), a part of the National Oceanic and Atmospheric Administration (NOAA), National Weather Service (NWS), provides comprehensive, reliable systems and marine observations to support the missions of the NWS and NOAA, promote public safety, and satisfy the future needs of our customers. NDBC operates three major buoy arrays as well as a network of coastal marine observing stations. These systems provide critical data on oceanic and atmospheric conditions that is used by weather and hurricane forecasters, researchers, climatologists, oceanographers, commercial fishers, and recreational boaters, among others.

The NDBC manages the development, operations, and maintenance of the national data buoy network. It serves as the NOAA focal point for data buoy and associated meteorological and environmental monitoring technology. It provides high quality meteorological/environmental data in real time from automated observing systems that include buoys and a Coastal-Marine Automated Network (C-MAN) in the coastal zone surrounding the United States and the open ocean. It provides engineering support, including applications development, and manages data buoy deployment and operations, and installation and operation of automated observing systems installed on fixed platforms. It hosts the Volunteer Observing Ship (VOS) program to acquire additional meteorological and oceanographic observations supporting NWS mission requirements. The VOS is managed by federal employees within the NWS called PMOs (Port Meteorological Officers); their job is to recruit ships to take/report weather observations in the open seas. The NDBC program tracks only metadata on the observations and the ships, no information on the general public. The ships are typically commercial/cruise ships.

NDBC is located at the Stennis Space Center in Bay St. Louis, Mississippi, and has operated a network of off-shore weather buoys and unmanned coastal observing stations (Coastal Marine Automated Network or C-MAN stations) since 1990. In 2001 and 2005 respectively, NDBC began to assume responsibility for operating moored buoys supporting NOAA's Deep-Ocean Assessment and Reporting of Tsunami (DART) program and the Tropical Atmosphere Ocean (TAO) program that were developed and formerly operated by NOAA's Pacific Marine Environmental Laboratory (PMEL).

NDBC currently operates and maintains 195 moored buoys and 46 C-MAN stations. The U.S. Coast Guard provides ship transit services for NDBC so that it can repair and maintain its weather buoys. The Coast Guard also maintains a small staff at NDBC. NOAA vessels provide support for the NDBC mission when their schedules allow. NDBC also leases privately-owned vessels when required to support the mission and maintenance schedules.

Surveys of meteorologists have shown about 40 percent of NWS marine warnings and advisories are based, at least in part, on NDBC's meteorological data. In addition to this critical purpose, the observations are used by meteorologists who need to adjust flight level wind speeds reported by hurricane reconnaissance aircraft to surface winds; by geophysicists who use our sea surface temperature, wind, and wave reports to help calibrate remotely sensed measurements from spacecraft; and by engineers who obtain directional wave measurements to study beach erosion and shore protection. Additionally, surfers, fishermen, and boaters acquire the reports via the Internet to help them determine if they want to venture offshore.

Identifying Numbers:

- Passports of Foreign National visitors are collected via fax and transmitted electronically via Accellion to the NOAA security office and in person to the NASA security office. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of this and other PII/BII.

General Personal Data:

- Name, home address, and telephone numbers are collected from NDBC employees (federal and contractor) in support of Continuity of Operations (COOP) activities.
- When contacting the NDBC webmaster, customers' (i.e., general public, government, private sector, and educational institutions), email addresses are used in order to provide a response to questions and service requests. Further, the customers voluntarily provide contact information to include their name and phone numbers based on the type of response expected.

Work-Related Data:

- Occupation, job title, work address, telephone number, and email addresses are maintained on NDBC employees (federal and contractor) for administrative purposes.
- Electronic personnel-related forms of NDBC employees (federal) are transferred to NOAA HR in bulk or on a case-by-case basis via Accellion or via tracked Federal Express (FedEx) package. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.
- Performance plans of NDBC employees (federal) are maintained for administrative purposes.

- Proprietary information related to federal acquisition actions are maintained for administrative purposes.

Distinguishing Features/Biometrics:

- NDBC management utilizes photographs of NDBC employees (federal and contractor) to populate an organizational chart that is shared strictly within NDBC. Further, photographs are taken during NDBC buoy deployments and maintained on the shared drives. NDBC personnel (federal and contractor) give written permission for use of photos via the DOC Photo Release Form maintained by the HR liaison (we are now using this form with the PAS added).

System Administration/Audit Data:

- User IDs of NDBC employees (federal and contractor) are administered and maintained via a local implementation of Active Directory.
- Login success/failure is monitored on NOAA8873 for IT security purposes (ArcSight).
- Date/Time of access is monitored on NOAA8873 for IT security purposes (ArcSight).
- ID files accessed are monitored on NOAA8873 for IT security purposes (ArcSight).
- Contents of files are monitored on NOAA8873 for IT security purposes (ArcSight).

c) Information Sharing

Personnel and Foreign National (FN) information is shared/transferred to NOAA Human Resource (HR) and Security offices via Accellion. Foreign national information is delivered to NASA Security in person via the HR liaison. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

In case of a security or privacy breach, information will be shared with the Department of Commerce and possibly the Department of Justice.

d) Legal Authority to Collect PII/BII

Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1151(Dissemination of Technological, Scientific, and Engineering Information)
- 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)
- DAO 207-12 Foreign Visitor and Guest Access Program
- Authorities from DEPT-6: 5 U.S.C. 301; 44 U.S.C. 3101.
- 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: 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.
- 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.
- Authorities from NOAA-11: 5 U.S.C. 301, Departmental Regulations and 15 U.S.C. 1512, Powers and duties of Department.
- Authorities 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.

e) FIPS 199 Security Impact

The NOAA8873 information system is categorized as a Moderate 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	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					

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	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance Plans					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		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		f. Contents of Files	X
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	X		
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector (PAE)**	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): ***Pacific Architects and Engineers (PAE) is the technical services contractor at NDBC. They provide contact information for COOP.*					

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*	X	Electronic purchase transactions	
Other (specify):			

* This issue was addressed in the last PIA. This is the video surveillance of the data center. There are no discs. The video is placed on a network drive and files are automatically deleted once they are past 30 days. This is for correlation of physical entry into the data center in the case of an IT security event. The network drive access is limited to the NOAA IT staff. Signs are posted that video surveillance is in progress once you enter into the area where the camera view reaches.

	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		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	X
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 information collected and maintained by NOAA8873 is used for administrative purposes such as performance evaluations, logging into the information system, and contact during Continuity of Operations (COOP) activities. This information is that of federal employees and contractors.

Electronic personnel-related forms of NOAA employees only are transferred to NOAA HR in bulk or on a case-by-case basis via DOC Accellion (for NOAA records only) or via tracked Federal Express (FedEx) package. This information is not shared with anyone beyond those that are required to process it within the respective bureau. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

Customers voluntarily provide contact information when submitting web inquiries via webmaster and in doing so consent to contact from NDBC webmaster to answer their inquiries. Customers may be general public, government or private sector, including educational institutions.

Foreign nationals (FNs) requesting access to NDBC provide passports in support of the NOAA FN clearance process (application). The passports are transmitted via Accellion by the NDBC HR liaison. NASA also requires clearance of FNs since NDBC is a tenant on a NASA installation. FN passport information is delivered in person by the NDBC HR liaison in support of this process. The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

Proprietary information related to federal acquisition actions are maintained for administrative

purposes.

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):			

*In case of privacy/security breach

**NASA security office, and Department of Justice in case of 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: NOAA WFMO Recruitment Analysis Data System (RADS). NOAA8873 uploads employee PII in specified formats to RADS. The individual user (HR Liaison role) within the Resources Branch (OBS23)

	has been provided an encrypted drive (non-portable) for storage of PII/BII.
	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.ndbc.noaa.gov/contact_us.shtm A form for new employees with a PAS is stored in a folder, and attached with this PIA.	
X	Yes, notice is provided by other means.	Specify how: **Identifying Numbers**: Written notice is included on all personnel forms that employees (federal) complete. Notice is provided verbally to a foreign visitor by the US sponsor or the DOC staff at DOC International Affairs Office, at the time of the Foreign National's (FN's) appearance at the office, that completion of the information on the Foreign National Visitor and Guest Access request form is required for obtaining authorization for a visit. **General Personal Data**: Notice is provided to customers initiating web inquiries via webmaster by a privacy act statement on the web site. For NDBC COOP activities, employees are asked permission in person by their supervisors when collecting the applicable information. **Work-Related Data**: Written notice is included on all personnel forms that employees complete. For DOC performance/award documents, employees are informed by their supervisors in person or via email that the evaluations are in process. Employees have access to view the official documents. **Distinguishing Features/Biometrics**: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by

		the HR liaison. **System Administration/Audit Data**: NIST SP 800-53A Rev 4 requires information systems to collect audit data in support of IT security activities. NDBC employees (federal and contractor) are given notice via the NOAA IT Security Awareness Training.
	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: **Identifying Numbers**: FNs are given the opportunity to decline to provide information during the clearance process with NOAA. If FNs decline to provide the information (by not providing it) then access to NOAA sites (including NDBC) are denied. HSPD-12 requires personnel log into the information system using two factor authentication (2FA). If an employee declines to provide, no network access is provided. **General Personal Data**: For the Continuity of Operations (COOP) activities, NDBC personnel can inform their supervisor in person or in writing that they decline to provide PII/BII. Customers voluntarily provide information when submitting web inquiries via webmaster, so that they may be contacted. **Work-Related Data**: Performance/position information is part of the official personnel record for DOC employees, with notice given on the forms completed as part of the hiring process. Individuals may have chosen not to provide information, by not completing the forms, but this would affect their employment status. . **Distinguishing Features/Biometrics**: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison. If personnel decline participation, no DOC Photo Release Form is filed with the HR liaison.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: **System Administration/Audit Data**: NIST SP 800-53A Rev 4 requires information systems to collect audit data in support of IT security.

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: **Identifying Numbers**: FNs are given the opportunity via the NOAA forms to consent to the use of their information in support of the clearance process during the application process with NOAA.

		Personnel may choose not to log in to the information system, but HSPD-12 requires personnel to log in using two factor authentication (2FA). This is the only use for this information. **Work-Related Data**: Performance/position information is part of the official personnel record for DOC employees. Employees may choose not to consent to a particular use, in writing, to their supervisors, but this may affect their employment status. **General Personal Data**: For the Continuity of Operations (COOP) activities, there is only one use. Customers voluntarily provide information when submitting web inquiries via webmaster and in doing so consent to contact from NDBC webmaster to answer his/her inquiry. This is the only use of the information. **Distinguishing Features/Biometrics**: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: **System Administration/Audit Data**: NIST SP 800-53A Rev 4 requires information systems to collect audit data in support of IT security.

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: **Identifying Numbers**: FNs are given the opportunity to update their information during a subsequent clearance process with NOAA where the FN completes a new application. **General Personal Data**: For the Continuity of Operations (COOP) activities, NDBC personnel are asked via email from either the NDBC HR liaison or the NDBC ISSO to review/update PII/BII annually in person. **Distinguishing Features/Biometrics**: NDBC employees (federal and contractor) give written consent for use of photographs via the DOC Photo Release Form maintained by the HR liaison. **Work-Related Data**: Performance/position information is part of the official personnel record for DOC employees and will be updated upon official personnel actions. **General Personal Data**: Customers voluntarily provide email address and contact information at their discretion when contacting the NDBC Webmaster, but we collect information only per each email, rather than keeping a record.
	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: *Windows file system auditing monitors, tracks, and records changes to the files containing PII/BII and a report is sent to the NDBC ISSO daily.*
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): *01/28/2017* ☐ 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.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): The individual user (HR Liaison role) within the Resources Branch (OBS23) has been provided an encrypted drive (non-portable) for storage of PII/BII.

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

All NDBC 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 electronically signs the Rules of Behavior (ROB) via the NOAA IT Security Awareness training indicating that they have read and understand the ROB. The ROB outlines privacy and the PII definition, storage, sharing, and reporting of PII incidents.

To protect data contained on mobile devices, all NDBC laptops are fully encrypted using the NOAA enterprise supplied encryption software. In addition, all NDBC government issued phones are protected via MaaS 360.

NDBC employees are required to utilize DOC Accellion for the transmission of any sensitive data.

The individual user (HR Liaison role) within the Resources Branch (OBS23) has been

provided an encrypted drive (non-portable) for storage of all PII/BII in the system.

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, Employees Personnel Files Not Covered by Notices of Other Agencies* *DEPT 6, Visitor Logs and Permits for Facilities under Department Control* *DEPT 25, Access Control and Identity Management System* *NOAA 11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.* *OPM/GOVT 1, General Personnel 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: *NARA, General Records Schedule 20 Electronic Records* *NARA, General Records Schedule 24 Information Technology Operations and Management 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		Deleting	X
Other (specify): Destruction of Hard Drives			

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: *Customers voluntarily provide only as much information as they feel necessary when submitting web inquiries via NDBC webmaster.*
X	Quantity of PII	Provide explanation: *NDBC employees (federal and contractor) total less than 250 and minimal PII is collected/maintained.*
X	Data Field Sensitivity	Provide explanation: *Some sensitive PII is collected, mainly from foreign visitors.*
X	Context of Use	Provide explanation: *Information is for official use only and contained within DOC and NOAA.*
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: *Security and privacy controls for protecting PII/BII are in place and functioning for NOAA8873 IAW NIST SP 800 53 Revision 4.*
	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 statement.
	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.
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: Joy Baker Office: DOC/NOAA/NWS/OBS2 (NDBC) Phone: 228-688-2801 Email: Joy.Baker@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: BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER.JOY.ALLISON.1269758577 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BAKER.JOY.ALLISON.1269758577 Date: 2017.10.25 12:37:25 -05'00' Date signed:	**Information Technology Security Officer** Name: Beckie Koonge Office: DOC/NOAA/NWS/ACIO Phone: 301-427-9020 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: 2017.10.30 13:46:56 04'00' Date signed:
Authorizing Official Name: Joseph Pica Office: DOC/NOAA/NWS/OBS Phone: 301-427-9778 Email: Joseph.A.Pica@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: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.10.25 15:11:31 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: 2017.10.30 15:52:52 -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: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOAA8873-National Data Buoy Center (NDBC)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NDBC

Unique Project Identifier: NOAA8873

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 Data Buoy Center (NDBC), a part of the National Oceanic and Atmospheric Administration (NOAA), National Weather Service (NWS), provides comprehensive, reliable systems and marine observations to support the missions of the NWS and NOAA, promote public safety, and satisfy the future needs of our customers. NDBC operates three major buoy arrays as well as a network of coastal marine observing stations. These systems provide critical data on oceanic and atmospheric conditions that is used by weather and hurricane forecasters, researchers, climatologists, oceanographers, commercial fishers, and recreational boaters, among others.

The NDBC manages the development, operations, and maintenance of the national data buoy network. It serves as the NOAA focal point for data buoy and associated meteorological and environmental monitoring technology. It provides high quality meteorological/environmental data in real time from automated observing systems that include buoys and a Coastal-Marine Automated Network (C-MAN) in the coastal zone surrounding the United States and the open ocean. It provides engineering support, including applications development, and manages data buoy deployment and operations, and installation and operation of automated observing systems installed on fixed platforms. It hosts the Volunteer Observing Ship (VOS) program to acquire additional meteorological and oceanographic observations supporting NWS mission requirements.

NDBC is located at the Stennis Space Center in Bay St. Louis, Mississippi, and has operated a network of off-shore weather buoys and unmanned coastal observing stations (Coastal Marine Automated Network or C-MAN stations) since 1990. In 2001 and 2005 respectively, NDBC began to assume responsibility for operating moored buoys supporting NOAA's Deep-Ocean Assessment and Reporting of Tsunami (DART) program and the Tropical Atmosphere Ocean (TAO) program that were developed and formerly operated by NOAA's Pacific Marine Environmental Laboratory (PMEL).

NDBC currently operates and maintains 195 moored buoys and 46 C-MAN stations. The U.S. Coast Guard provides ship transit services for NDBC so that it can repair and maintain its weather buoys. The Coast Guard also maintains a small staff at NDBC. NOAA vessels provide support for the NDBC mission when their schedules allow. NDBC also leases privately-owned vessels when required to support the mission and maintenance schedules.

Surveys of meteorologists have shown about 40 percent of NWS marine warnings and advisories are based, at least in part, on NDBC's meteorological data. In addition to this critical purpose, the observations are used by meteorologists who need to adjust flight level wind speeds reported by hurricane reconnaissance aircraft to surface winds; by geophysicists who use our sea surface temperature, wind, and wave reports to help calibrate remotely sensed measurements from spacecraft; and by engineers who obtain directional wave measurements to study beach erosion and shore protection. Additionally, surfers, fishermen, and boaters acquire the reports via the Internet to help them determine if they want to venture offshore.

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): *Images collected from buoys outfitted with cameras*					

____ 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 NDBC currently has a video surveillance system installed in the data center to monitor physical access to the restricted area. In addition, access to the information technology (IT) areas is physically controlled via room entry readers. Select buoys are outfitted with cameras to collect visual environmental data and images collected are stored on the information system.

____ 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 NOAA8873 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 NOAA8873 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): Joy Baker, ISSO

Signature of ISSO or SO: BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER.JOY.ALLISON.1269758577 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn BAKER.JOY.ALLISON.1269758577 Date: 2017.11.30 09:25:26 -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: 2017.11.30 10:28:55 05'00' Date: _____

Name of Authorizing Official (AO): Joseph Pica, AO

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.12.04 09:28:22 -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: 2017.12.04 12:49:57 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, December 4, 2017 6:15 PM
To:	Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO; Toland, Michael
Cc:	Mark Graff NOAA Federal; Glen Taylor; Scott Sauri; Tahir Ismail; NMFS.InfoSec@noaa.gov; Amores, Catherine (Federal)
Subject:	NOAA 4020 PIA and PTA for Dec 7 CRB, 10 am
Attachments:	NOAA4020 PIA_20171128 for MHG signature mhg.pdf; NOAA4020 PTA 2017 revised description_for BCPO signature mhg.pdf

Please see the attached for Dec 7 CRN. I sent the SAR and SAR workbook earlier.

thx Sarah

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

NOAA OCIO
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
NOAA4020
Science and Technology

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/NOAA4020
Science and Technology

Unique Project Identifier: 006-48-01-14-02-3305-00

Introduction: System Description

The NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

1) The Financial Services Division collects information from applicants for the following programs and purposes: The Fisheries Finance Program (FFP), credit information, personal identification including social security number, and tax returns. The information is used to verify applicants for fisheries loans. Capital Construction Fund (CCF), personal identification including social security numbers and tax returns. The information is used to verify applicants for CCF accounts and projects. Fishermen's Contingency Fund (FCF), personal identification including social security numbers, and personal transaction information. The information is used to verify business losses and lost fishing gear for claims made by the fishermen. Information collected includes tax returns.

   Information collected: applicant's name and address, the amount of financing applied for, the purpose of loans, an appraisal of the vessel or facility involved, financial information including the last 3 tax returns (these are not stored electronically), a list of creditors and buyers with relevant credit terms, identification of authorized representatives (accountant, attorney, insurance agent), and legal history (status regarding bankruptcy, litigation, delinquency on and Federal debt, etc.). Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated. Loan applications are entered into the system from paper forms completed by the public, into an online application, which is managed by NMFS NOAA4020. Regional offices access the information in order to administer loans for applicants. The loan data is stored only in NOAA4020.

   When a United States (U.S.) commercial fisherman sustains losses and/or damages as a result of oil and gas activities on the U.S. Outer Continental Shelf (OCS), the fisherman may apply for compensation from the U.S. Federal government, using fillable pdf forms on the applicable Web site.

NMFS also has programs to reduce excess fishing capacity by paying fishermen to surrender their vessels/permits. These fishing capacity reduction programs, or buybacks, are conducted pursuant to the Magnuson-Stevens Fishery Conservation and Management Act, and the Magnuson-Stevens Reauthorization Act (Pub. L. 109-479). The buybacks can be funded by a Federal loan to the industry or by direct Federal or other funding. Buyback regulations are at 50 CFR Part 600. The information collected by NMFS involves the submission of buyback requests by industry, submission of bids, referenda of fishery participants and reporting of collection of fees to repay buyback loans. For Fishery Capacity Reduction Program Buyback Requests, certain forms are submitted on paper and entered into a database, and others are submitted online.

Information is not shared except within the program (NMFS Headquarters, West Coast Region and Southeast Region), or in the case of a breach, within the bureau, the Department and other federal agencies (Justice).

2) International Trade Data System (ITDS).

ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports and exports of fisheries products. Types of BII data collected are Name of business, Address and Contact information. The data is collected from the U.S. Customs and Border Control's ITDS database. Reasons for the NMFS database:
(1) The CBP's ITDS only grants access to a small group of people who can meet their security clearance requirements which will take time and it seems they do want to limit the number of users. (2) The CBP's ITDS can't meet the specific requirements of the NMFS programs. So we developed our own ITDS to support the NMFS programs. For example, one program needs to the functions to track the harvesting vessel trips, all programs need the functions to review the data and track issues; the programs need to search data relevant to their programs etc.

3) Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL)

The Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL) system will be a tool to load raw data from various sources, format them and run through various QA/QC processes. NOAA4020 collects PII and BII data from MRIP ETL only for the NSAR, see below. Types of PII collected are fishing license info, Name, Address, Driver's license, Phone, Email and Date of Birth of the angler. Some states have requested that their data cleansed by this process be sent back to them.

4) National Saltwater Angler Registry - NSAR

The National Saltwater Angler Registry system allows the integration of the state-provided saltwater angler license data with the existing national registration data into a database, which

can be used as a consolidated phone book of the nation's recreational salt-water anglers. The captured data is entered into the database and will be used to furnish frames for the MRIP survey. Types of PII collected are Name, Address, and Driver's license, Telephone, Email and Date of Birth of the angler.

5) NOAA Fisheries Committee on Scientific Stature.

The NOAA Fisheries Committee on Scientific Stature (NFCSS) is a national-level Performance Management Advisory Committee (PMAC) established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. There is a website and database to manage and record the results of NFCSS member reviews conducted for the purpose of evaluating a scientist's credentials and contributions to allow them to be assigned to a higher pay Band without being a supervisor and to produce a standard report for the committee chair (OST Science Director). In 2014, OST upgraded the NFCSS website and database to enable password protected, role-based secure storage and retrieval of review package documents. Access to the database is restricted to the OST Science Director, the six regional Deputy Science Directors, one Band V research scientist from each regional science center, the NOAA Fisheries HR Business Partner, and the NFCSS database administrator and is provided by the NFCSS database administrator only at the request of the NFCSS Chair. Information collected: name, work contact information, letters of reference and curricula vitae, performance plan, science director memoranda and name of immediate supervisor. The administrator uploads copies of a memorandum from the NFCSS Chair to the Science Center director of staff being reviewed. The data (name, email, documents) for staff being reviewed are entered by their Deputy Science Director. The review comments are entered by the NFCSS members.

6) Protected Resources National Inventory of Marine Mammals (NIMM) System.

National Inventory of Marine Mammals (NIMM) was rolled out to the marine mammal Owners and Facilities, on July 18, 2017, with an initial user base of 151 users. NIMM maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. NOAA4020 collects PII and BII data from this system. Types of BII collected are Institution Name, Mailing address, Contact email, Phone and Fax Numbers. No PII is collected.

7) Highly Migratory Species.

Effective July 1, 2005, all dealers importing, exporting, or re-exporting bluefin tuna, swordfish, southern bluefin tuna and frozen bigeye tuna must hold a Highly Migratory Species International Fishery Trade Permit (HMS IFTP) and follow the required reporting procedures established at 50 C.F.R. 300.183 through 300.187. The HMS IFTP is required to assist the United States implement international trade tracking programs addressing illegal, unreported, and unregulated fishing activities, improve conservation and management measures, and enhance the scientific evaluation of these stocks.

Under international agreements and domestic law, the United States implements recommendations of the International Commission for the Conservation of Atlantic Tunas (ICCAT) and Inter-American Tropical Tuna Commission (IATTC). Both IATTC and ICCAT have implemented a statistical document program for frozen bigeye tuna. In addition, ICCAT has implemented bluefin tuna and swordfish statistical document programs.

The NMFS Office of Science and Technology developed a legacy Highly Migratory Species Dealer Permit System more than 10 years ago to meet the requirements outlined in the purpose above. The system has since been migrated over to the NMFS National Permit System, whose information is stored in NOAA4000. For historical validating of permits, the system is currently being retained for its reporting functionality for viewing and validating permit information on dealers. Please note that once all permits have expired on these two reports, there will be no more need to maintain these interfaces and will therefore be deactivated. NOAA4020 collects PII and BII data from Highly Migratory Species. Types of PII and BII data collected and processed are Applicant Name, Social Security Number, Position Type, Birthdate, Mailing Address Street Name, Business Name, Federal ID No/SSN, Date Business Formed, Business Type, Mailing Address Street Name etc. *No new data is being collected through this legacy system.*

8) NOAA Emergency Contact List
NOAA collects the Emergency Contact List that is used to track and locate staff in the office of Science and Technology. This is PII data.

9) NOAA4020 collects system user ID information from employees and contractors accessing the system.

Authorities

From NOAA-19: 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 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 Western and Central Pacific Fisheries Convention Implementation Act, 16 U.S.C. 6901 et seq. (WCPFCIA); the Marine Mammal Protection Act, 16 U.S.C. 1361; and Taxpayer Identifying Number, 31 U.S.C. 7701.

From NOAA-21: Title XI of the Merchant Marine Act of 1936 as amended and codified, 46 U.S.C. 1177 and 46 U.S.C. 53701 et seq., the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq., and provisions of the Debt Collection Improvement Act as codified at 31 U.S.C. 7701.

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.

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. Types of PII data collected is Contact Name, Phone Number and Address.

The legal authority for the Emergency Contact List 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.

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.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*
__ This is an existing information system with no changes that create new privacy risks.

Changes That Create New Privacy Risks (CTCNPR) - NA					
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): New application (NIMM) rolled out in 7/17.					

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	X*	f. Driver's License		j. Financial Account	X
c. Employer ID		g. Passport		k. Financial Transaction	X
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Required for identification of the individual for payment purposes, and for verification of financial information.
* Sec. 53074(c)(4): for the loan programs, the analysis of an applicant's financial condition requires a credit examination, for which the SSN would be needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	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):					

Work-Related Data (WRD)					
a. Occupation	X	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): For **Fisheries Committee on Scientific Stature**
j. Performance Plan
k. Supervisor Justification
l. Science Director Memoranda
m. Letters of Reference
n. Curriculum Vitae
o. Position Description

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	X
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	X	Online	X*
Telephone		Email			
Other (specify):					

* For the ECL

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	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): To determine loan, compensation and buyback qualifications from fishing vessel owners; to maintain databases for tracking international seafood trading tracking, angler registration, for use in reviewing scientists' research products, and a Protected Resources marine mammal inventory.			

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, members of the public, Capital Construction Fund Agreement, the Fishermen's Contingency Fund, foreign national, visitor or other (specify).

The Fisheries Finance Program (FFP) provides direct loans for certain fisheries costs. Vessel financing is available for the purchase of used vessels or the reconstruction of vessels (limited to reconstructions that do not add to fishing capacity). Refinancing is available for existing debt obligations. FFP loans are not issued for purposes which could contribute to over capitalization of the fishing industry. Finance or refinance fisheries shore side facilities or Aqua cultural facilities. The program provides Individual Fishing Quota (IFQ) financing (at the request of a Fishery Management Council). IFQ financing is available to first time purchasers and small vessel operators in the Halibut Sablefish fisheries. FFP also provides long term fishery buy back financing (at the request of a Fishery Management Council or

Governor) to purchase and retire fishing permits and/or fishing vessels in overcapitalized fisheries. Also, a United States (U.S.) commercial fisherman who sustains losses and/or damages as a result of oil and gas activities on the U.S. Outer Continental Shelf (OCS), the fisherman may apply for compensation from the U.S. Federal government.

FFP financing offers the fishing industry slightly better interest rates and longer term loans than are available elsewhere. The longer-term loans allow the industry to amortize their capital investment over the actual economic life of the fisheries asset. Lower debt service reduces economic pressure, thus allowing the borrower to more easily accommodate more restrictive fishery management initiatives. FFP regulations ensure that FFP traditional lending will not increase harvesting capacity in the fisheries but will simply permit the financing of the acquisition of existing vessels/facilities or the refinancing of existing debt for vessels/facilities already in the fishery.

Applications are required in order to determine qualification for a loan, and to provide contact information with borrowers. Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated.

This information is collected from members of the public.

The Emergency Contact List (ECL) is used to track and locate staff in the office of Science and Technology: name, occupation, work address and email. This information is collected from employees and contractors.

International Trade Data System (ITDS).
ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports and exports of fisheries products. Types of BII data collected are Name of business, Address and Contact information. The data is collected from the U.S. Customs and Border Control's ITDS database, who originally collected it from members of the public.

MRIP ETL
The MRIP ETL is a tool to load raw data from various sources, format them and run through various QA/QC processes. NOAA4020 collects PII and BII data from MRIP ETL. Types of PII collected are fishing license info, Name, Address, Driver's license, Phone, Email and Date of Birth of the angler. The MRIP ETL collects data from the NSAR, below.

National Saltwater Angler Registry - NSAR
The National Saltwater Angler Registry system allows the integration of the state-provided saltwater angler license data with the existing national registration data into a database, which can be used as a consolidated phone book of the nation's recreational salt-water anglers. The captured data is entered into the database and will be used to furnish frames for the MRIP survey. Some states have requested that their data cleansed by this process be sent back to them. Types of PII collected are Name, Address, Driver's license, Telephone, Email and Date

of Birth of the angler.

The **NOAA Fisheries Committee on Scientific Stature (NFCSS)** is a national-level PMAC established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. Information is only shared among the members of the NFCSS. The information is collected from members of the public.

1) **Protected Resources National Inventory of Marine Mammals (NIMM) System**.
National Inventory of Marine Mammals (NIMM) was rolled out to the marine mammal Owners and Facilities, on July 18, 2017, with an initial user base of 151 users. NIMM maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. NOAA4020 collects PII and BII data from this system. Types of BII collected are Institution Name, Mailing address, Contact email, Phone and Fax Numbers. NO PII is collected.

2) **Highly Migratory Species**.
Effective July 1, 2005, all dealers importing, exporting, or re-exporting bluefin tuna, swordfish, southern bluefin tuna and frozen bigeye tuna must hold a Highly Migratory Species International Trade Permit (HMS ITP) and follow the required reporting procedures established at 50 C.F.R. 300.183 through 300.187. The HMS ITP is required to assist the United States implement international trade tracking programs addressing illegal, unreported, and unregulated fishing activities, improve conservation and management measures, and enhance the scientific evaluation of these stocks.
The legacy system has since been migrated over to the NMFS National Permit System, whose information is stored in NOAA4000. For historical validating of permits, the system is currently being retained for its reporting functionality for viewing and validating permit information on dealers. Please note that once all permits have expired on these two reports, there will be no more need to maintain these interfaces and will therefore be deactivated. *No new data is being collected through this legacy system.*

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	X**		
Public	X**		
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach

**NIMM

	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: NOAA4020 connects with NOAA4000. Technical boundary controls are in place to prevent BII leakage. NOAA4020 consists of servers that support the development and deployment of application offerings that facilitate the provision of mission related services to the general public, authorized organizational and non-organizational users. NOAA4000 provides general support system (GSS, i.e. LAN/WAN network connectivity) services to NOAA4020.
	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. NOAA Buyback Program Site with PAS (also on forms): http://www.nmfs.noaa.gov/mb/financial services/buyback.htm Capital Construction Fund: all forms collecting PII are linked on this page: http://www.nmfs.noaa.gov/mb/financial services/ccf docs and forms.htm Fishermen's Contingency Fund: PAS is on this page: http://www.nmfs.noaa.gov/mb/financial services/fcf.htm and will be added to the forms. NSAR Site and PAS: https://www.countmyfish.noaa.gov/register/ The ECL PAS: *Site not available to non NOAA staff. A screen shot with the PAS is included in the cover email for this PIA.*	
X	Yes, notice is provided by other means.	Specify how: The FFP forms specify which information is required. The ECL has a Privacy Act Statement: This information collection is voluntary. The purpose is to maintain an emergency contact list. The personally identifiable information will not be shared outside the S&T. ITDS: The data is collected from the U.S. Customs and Border Control's ITDS database, who provides notice at the time of collection. NSAR: Notice is provided on the registration Web site: Anglers are also notified on the Web site, that their PII/BII may be used as part of a phone survey regarding fishing activities, before purchasing a license. MRIP ETL: No data collected directly by the system. NIMM: Upon being added to an organization as a Responsible Official or a Primary Contact, an automatic email is sent from NIMM. NFCSS: A screen shot signed by the director and operations director is included in the cover email. HMS Legacy System – no new information is being 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 FFP, applicants may decline to provide PII/BII, but if required information is not provided, the applicant

		cannot receive the benefit. For the ECL application, employees and contractors may decline to their supervisors in writing, but they may then not be notified in case of emergencies. ITDS: the NMFS ITDS is not the original point of collection. NIMM: An individual can chose not to be the responsible official or the primary contact. NSAR: The individual will not register if he wishes to decline. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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 FFP, consent for the specified use is implied by completing and signing the loan application. Notice is also provided in NOAA-21. Above the signature is this text: The Applicant certifies that: (1) it is a citizen of the United States (if a corporation, at least 75% of the stock must be held by U.S. citizens), and (2) all information in this application is true and correct to the best of the applicant's knowledge and belief and is submitted to obtain a loan from the Fisheries Finance Program. For the ECL, emergency contact is the only use for the information. ITDS: the NMFS ITDS is not the original point of collection. NIMM: There is only one use for the information. NSAR: Participation in the phone survey is required. Anglers may choose not to purchase a license. There is no option to purchase a license and opt out of the survey if chosen. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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 FFP, applicants/borrowers may provide updates at any time to the program office, by mail, fax, telephone or email, including when annual financial statements are submitted. For ECL, users may log on to the application and update the information at any time. ITDS: the NMFS ITDS is not the original point of collection. NIMM: Those with NIMM user accounts have access rights to review and update their data. NSAR: Information may be updated at the time of registration renewal. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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: Audit log
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 1/9/2017 ☐ 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.

The general controls used to protect the loan PII in these applications, involve controlled physical and logical access: role based access control, proper data segmentation and protection via encryption at rest and proper audit logging of events. Adequate media marking, transport and storage and incident monitoring and response are also used. The levels of implementation for these technologies meet the criteria required by NIST 800-53, Rev 4 under the following controls: Access Enforcement (AC-3), Separation of Duties (AC-5), Least Privilege (AC-6), Remote Access (AC-17), User-Based Collaboration and Information Sharing (AC-21). , Auditable Events (AU-2), Audit Review, Analysis, and Reporting (AU-6), Identification and Authentication (Organizational Users) (IA-2), Media Access (MP-2) , Media Marking (MP-3), Media Storage (MP-4), Media Transport (MP-5), Media Sanitization (MP-6), Transmission Confidentiality (SC-9), Protection of Information at Rest (SC-28), Information System Monitoring (SI-4). In addition to following database CIS benchmarks and best practices, all Oracle tables that contain PII/BII data are stored in an encrypted tablespace.

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-19**, Permits and Registrations for United States Federally Regulated Fisheries **COMMERCE/NOAA-21**, Financial Services Division **DEPT-18**, Employees Personnel Files Not Covered By Notices of Other Agencies **DEPT-13**, Investigative and Security Records.
	Yes, a SORN has been submitted to the Department for approval.
	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: 1510-01 **Pending Application files.** Applications for loans or other forms of assistance. Subdivided by type of aid. **Disposition** 1. Approved applications: Transfer to appropriate code for case file. 2. Rejected applications: Destroy after 5 years. 1510-02 **Fishery Loan files.** Case files on loans made to finance or refinance costs relating to fishing vessels, including their purchase. Includes applications, case histories, insurance policies, mortgages, and related correspondence and forms. **Disposition** 1. Collateral documents: Return to borrower when loan is repaid. 2. Other documents: Cut off when loan is repaid. Destroy 3 years later. 1512-13: International Trade Data System: **TEMPORARY**. Cut off closed files at end of calendar year, and transfer to FRC. Destroy when 20 years old. 1502-03: MRIP ETL: **PERMANENT.** Transfer to FRC after 5 years. Offer to NARA when 25 year 1515-03: NSAR: **TEMPORARY.** Cut off at end of study. Destroy 6 years after the completion of study. NFCSS: Chapter 300 Personnel Management Files 301-09 Supervisors' Personnel Files. Records on positions, authorizations, pending actions, position descriptions, training records, individual development plans, telework agreements, award recommendations, and records on individual employees not duplicated in or not appropriate for the OPF. These records are sometimes called supervisors' working files, unofficial personnel files (UPFs), and employee work folders or "drop" files. DAA-GRS-2017-0007-0012 (GRS 2.2, item 080) Supersedes NOAA Schedule Items: 303-22a (GRS 1, item 18a) 303-22b (GRS 1, item 18b) **TEMPORARY**. Review annually and destroy superseded documents. Destroy remaining documents 1 year after employee separation or transfer. 1514-03: NIMM: **PERMANENT.** Cut off files annually and transfer to FRC when 3 years old. Transfer to the National Archives when 25 years old. HMS: 1513-11 Fishery Law Enforcement and Surveillance Files

	1504 Fishery Management and Coordination Files 1504-18 Permit Fee Files 1504-21 Dealer, Buyer, Processor or Receiver Permits. Although there are some specific time limits on these items listed above, the data for these permits are stored indefinitely in our database. However, after this year when the last set of permitsare due to expire in December, this application will no longer be available. It will be decommissioned. All other data will be handled by the National Permit System (NPS). ECL: DAA-GRS- 2013-0006-003. Disposition instruction: Temporary. Destroy when business need ceases.
	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: Loan data includes Tax ID Numbers, which. uniquely and directly identify individuals or businesses.
X	Quantity of PII	Provide explanation: Collective harm to individuals, but also harm to the organization's reputation and the cost to the organization in addressing a possible breach was considered.

X	Data Field Sensitivity	Provide explanation: There are sensitive data fields, including SSN/EIN.
X	Context of Use	Provide explanation The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated was considered. Whether disclosure of the mere fact that PII is being collected or used could cause harm to the organization or individual was considered.
X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801, Section 402b.
X	Access to and Location of PII	Provide explanation: The nature of authorized access to PII - The number and frequency of access was also considered. The degree to which PII is being stored on or accessed from teleworkers' devices or other systems, such as web applications, outside the direct control of the organization and whether PII is stored or regularly transported off-site by employees was considered.
	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 System Owner Name: Frank Schwing Office: Office of Science and Technology Phone: 301-427-8220 Email: franklin.schwing@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: SCHWING.FRANKLIN.B.DR.1365840748 Digitally signed by SCHW NG FRANKLIN B DR 1365840748 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=SCHWING FRANKLIN B DR 1365840748 Date: 2017 11 28 16:39:20 05'00' Date signed:	**Information Technology Security Officer** Name: Catherine Amores Office: Office of the Chief Information Officer 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: 2017.12.04 14:37:59 -05'00' Date signed:
Authorizing Official Name: Ned Cyr Office: Office of Science and Technology Phone: 301-427-8123 Email:ned.cyr@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: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 Date: 2017.12.04 12:55:24 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5358 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: 2017 12 04 16:23:35 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
National Oceanic and Atmospheric Administration
(NOAA)

Privacy Threshold Analysis
for the
NOAA4020
Office of Science and Technology

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Office of Science and Technology

Unique Project Identifier: 006-48-01-14-02-3305-00

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 and its purpose 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 NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

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): New application (NIMM) rolled out in 7/17.					

____ 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.

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

NOAA 4020 contains a variety of PII and BII, including permit application data and loan application data.

____ 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 [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: TAYLOR.GLEN.CLIFFORD.1365840934 Digitally signed by TAYLOR GLEN CLIFFORD 1365840934 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=TAYLOR GLEN CLIFFORD 1365840934 Date: 2017 11 15 12:48:07 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2017.12.04 12:03:34 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn CYR.EDWARD.C.DR.1365869436 Date: 2017.11.15 15:59:45 -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: 2017.12.04 12:47:03 -05'00' Date: _____

John D. Parker - NOAA Federal

From:	John D. Parker NOAA Federal
Sent:	Wednesday, December 6, 2017 2:16 AM
To:	Sarah Brabson NOAA Federal; Mark Graff NOAA Federal
Cc:	Maurice Mcleod NOAA Federal; _NOS ACIO ITSP
Subject:	Re: Fwd: Policy Notification: New NOAA Guidance for Annual Privacy Impact Analysis (PIA)
Attachments:	PTA_NOAA6205_ 2017.pdf

Hi Mark, Sarah,

I have signed the attached NOAA6205 PTA.

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 12/5/2017 10:56 AM, Maurice Mcleod NOAA Federal wrote:

> Good morning John,
>
> Can you sign the attached? Thanks.
>
> Forwarded message
> From: **Maurice Mcleod - NOAA Federal** <maurice.mcleod@noaa.gov>
> Date: Thu, Nov 30, 2017 at 1:24 PM
> Subject: Fwd: Policy Notification: New NOAA Guidance for Annual Privacy Impact Analysis (PIA)
> To: "John D. Parker NOAA Federal" <John.D.Parker@noaa.gov>
> Cc: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>, Andrea Hardy NOAA Federal <andrea.hardy@noaa.gov>, Amanda Wallace NOAA Federal <amanda.wallace@noaa.gov>, Ezekiel Abiodun NOAA Affiliate <ezekiel.abiodun@noaa.gov>
>
> Attached is our updated PTA for your signature.
>
> Forwarded message
> From: **Maurice Mcleod - NOAA Federal** <maurice.mcleod@noaa.gov>
> Date: Thu, Nov 30, 2017 at 12:54 PM
> Subject: Re: Policy Notification: New NOAA Guidance for Annual Privacy Impact Analysis (PIA)
> To: Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov>

Attached is the signed PTA, it still requires John and Mark's signatures.

On Wed, Nov 29, 2017 at 1:51 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Thanks!
>
> On Wed, Nov 29, 2017 at 1:42 PM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
>
> > Ok, I've converted it to a .pdf file. I will begin obtaining the signatures.
> >
> > On Wed, Nov 29, 2017 at 1:24 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> >
> > > Maurice, I also unchecked the "internal flow". Please use this one attached! thx Sarah
> > >
> > > On Wed, Nov 29, 2017 at 12:31 PM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
> > >
> > > > As requested.
> > > >
> > > > On Wed, Nov 29, 2017 at 12:06 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> > > >
> > > > > Maurice, you need to uncheck in Question 1, that there are new privacy risks, and also uncheck "internal flow". Then check "no new privacy risks".
> > > > >
> > > > > Also, you do collection PII from members of the public.
> > > > >
> > > > > Please make these changes and re send to me!
> > > > >
> > > > > thx Sarah
> > > > >
> > > > > On Wed, Nov 29, 2017 at 11:22 AM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
> > > > >
> > > > > > Ok, thank you.
> > > > > >
> > > > > > On Wed, Nov 29, 2017 at 11:18 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> > > > > >
> > > > > > > Thanks, in a meeting, back to you by noon.
> > > > > > >
> > > > > > > Sent from my iPhone
> > > > > > >
> > > > > > > On Nov 29, 2017, at 11:17 AM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
> > > > > > >
> > > > > > > > As requested.
> > > > > > > >
> > > > > > > > On Wed, Nov 29, 2017 at 10:19 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> > > > > > > >
> > > > > > > > > Just noticed your 2017 PTA is overdue, last one was 9 12 16. Please do a

new one with no changes, so it's consistent with the last PIA, and send to me in Word for review before you get signatures. I need to send this to DOC along with the other docs.

thx Sarah

On Wed, Nov 29, 2017 at 10:17 AM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:

> Thank you.
>
> On Wed, Nov 29, 2017 at 10:16 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
>
> > Now sending to Mark for signatures. sb
> >
> > On Tue, Nov 28, 2017 at 4:13 PM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
> >
> > > Excellent, thank you.
> > >
> > > On Tue, Nov 28, 2017 at 4:08 PM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:
> > >
> > > > Thanks, Maurice! This is two in one day! Will do quick review and send to Mark in the am.
> > > >
> > > > sb
> > > >
> > > > On Tue, Nov 28, 2017 at 4:06 PM, Maurice Mcleod NOAA Federal <maurice.mcleod@noaa.gov> wrote:
> > > >
> > > > > Attached are the PIA Annual Review Certification Form, previously approved PIA with new signatures, and the link to the latest version of NOAA6205's security controls assessment:

> > > > > On Thu, Oct 19, 2017 at 10:02 AM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:
> > > > >
> > > > > > All,
> > > > > >
> > > > > > NOAA Guidance on PIA Annual Review Process:
> > > > > >
> > > > > > 1. Download the **NOAA6NNN PIA Annual Review Certification Form** located at (remove extra spaces):
> > > > > >   - **http:// business.nos.noaa/cio/ITOB/Sec Com/Shared Documents/Policies/NOAA Policies/NOAA Privacy Guidance-PIA-PTA**

Templates

2. Complete the DOC PIA Annual Review Certification Form
    - PIA Reviewer can be any of the following individuals: ISSO, SO, AO, ITSO
3. PIA Reviewer digitally sign as the "Name of Reviewer"
4. The previously approved PIA must be resigned. No other changes must occur to the previously approved PIA other than new signatures.
    - You will need to create a new PDF of the previously approved PIA without signatures
    - Then circulate the new PDF of the previously approved PIA for signatures.
5. You will need to provide Mark and Sarah the latest version of your security controls assessment results.
    - I recommend you post the file to CSAM and include the link in the email.
    - Do not use Google email to send the security control assessment results, only use Accellion.
6. Send email and attached the **NOAA6NNN PIA Annual Review Certification Form,** previously approved PIA with new signatures and include a link to your latest version of your security controls assessment (in CSAM) to:
    - Sarah Brabson <sarah.brabson@noaa.gov>
    - Mark Graff <mark.graff@noaa.gov>
    - cc: John D Parker <John.D.Parker@noaa.gov>

DOC Privacy Program Plan, September 2017 is available at (remove extra spaces):

http://www. osec.doc.gov/opog/privacy/Memorandums/PRIVACY_PROGRAM_PLAN_2017.pdf

As a reminder, in October 2012, Zach Goldstein issued a policy memorandum requiring annual review of Privacy Threshold Analysis (PTA). The memorandum is available at (*remove extra spaces from link below*):

http:// business.nos.noaa/cio/ITOB/SecCom/Shared%20Documents/Policies/NOAA%20Policies/Policy%20Memoradums/2012-11-01%20Memo-%20Annual%20review%20of%20NOAA%20FISMA%20Systems%20PTA.pdf

PTA annual review includes obtaining the latest template (NOAA Privacy web link below), completing the template, obtaining the

required approvals and having the independent assessor review the approved PTA. The PTA requires approval by:

- Information System Security Officer (ISSO) or System Owner (SO)
- Information Technology Security Officer (ITSO)
- Authorizing Official (AO)
- Bureau Chief Privacy Officer (BCPO)

NOAA Privacy web site (*remove extra spaces from link below*):

http://www. cio.noaa.gov/services_programs /privacy.html

NOAA IT Policies, Policy Memo and Guidance covering NOAA CIO and Privacy policies (*remove extra spaces from links below*):

https://www. csp.noaa.gov/policies/manual/212-1301-V5-6-final.pdf

https:// sites.google.com/a/noaa.gov/cio/internal-use-only/it-governance?pli=1

http://www. cio.noaa.gov/services_programs /privacy.html

https://www. csp.noaa.gov/policies/NOAA_Rules_of_Behavior.xhtml

DOC IT Policies, Policy Memos, Frequently Asked Questions and Guidance covering DOC CIO and DOC Privacy policies (*remove extra spaces from links below*):

http:// connection.commerce.gov/policy /20140528/it-security-program-policy-commerce-information-technology-requirements-and-policy

http:// connection.commerce.gov/collection/it-security-policy-and-fisma-reporting-program

http://www. osec.doc.gov/opog/privacy/laws_and_regs.html#DOCPolicies

http://www. osec.doc.gov/opog/privacy/compliance.html#approvedpias

http://www. osec.doc.gov/opog/privacy/Memorandums/PRIVACY_PROGRAM_PLAN_2017.pdf

NOS ITSP has posted DOC and NOAA Policies, Policy Memos, Frequently Asked Questions and Guidance (*remove extra spaces from links below*) at:

http:// business.nos.noaa/cio/ITOB/SecCom/Shared%20Documents/Policies/

If you have any question, please contact the NOS.ITSP@noaa.gov or call John Parker/John Dandy/Marie Murphy for assistance.

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

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471

Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (b)(6)

<PTA_NOAA6205_ 2017.docx>

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (b)(6)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (b)(6)

Maurice McLeod
Information System Security Officer (NOAA6205)
Center for Operational Oceanographic Products and Services, NOS, NOAA
Desk: 240-533-0471
Cel (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, December 6, 2017 7:55 AM
To:	Ann Madden NOAA Federal
Cc:	Robert Swisher NOAA Federal
Subject:	Fwd: DEPT 29 SORN Discussion
Attachments:	Discussion Points on DEPT 29 Path Forward.docx; SORN_DEPT 29_draft_(2017 09 07) DOC update.docx

Hello Ann,

The message below, with the attachments summarizes the issue for Zach we wanted to discuss this morning.

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, Dec 6, 2017 at 7:54 AM
Subject: DEPT 29 SORN Discussion
To: Kristen Gustafson NOAA Federal <kristen.l.gustafson@noaa.gov>
Cc: Robert Swisher NOAA Federal <robert.swisher@noaa.gov>, Ed Kearns NOAA Federal <ed.kearns@noaa.gov>

Hello Kristen,

(b)(5)

(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)

(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:	Wednesday, December 6, 2017 11:27 AM
To:	Mark Graff NOAA Federal
Cc:	John D. Parker; Maurice Mcleod NOAA Federal
Subject:	NOAA6205 certification, re signed PIA and updated PTA for signature
Attachments:	NOAA6205 PTA_ 2017 for mhg signature.pdf; NOAA6205 PIA Annual Review Certification Form for mhg signature.pdf; NOAA6205 PIA for MHG signature.pdf

I'll also ask about the SAR. thx

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

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

U.S. DEPARTMENT OF COMMERCE

Department of Commerce

Privacy Impact Assessment (PIA)
Annual Review Certification Form

September 2017

Prepared by:
Office of Privacy and Open Government (OPOG)
DOC Privacy Program Plan Appendix L

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

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

Name of PIA: NOAA6205 PIA

FISMA Name/ID (if different): NOAA6205

Name of IT System/ Program Owner: Marian Westley

Name of Information System Security Officer: Maurice McLeod

Name of Authorizing Official(s): Richard Edwing

Date of Last PIA Compliance Review Board (CRB): 12/1/2016

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

Date of PIA Review: 11/27/2017

Name of Reviewer: Maurice McLeod

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: MCLEOD.MAURICE.STGEORGE.1267033699

Digitally signed by MCLEOD.MAURICE.ST GEORGE.1267033699
Date: 2017.11.27 14:59:59 -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)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, December 6, 2017 7:54 AM
To:	Kristen Gustafson NOAA Federal
Cc:	Robert Swisher NOAA Federal; Ed Kearns NOAA Federal
Subject:	DEPT 29 SORN Discussion
Attachments:	Discussion Points on DEPT 29 Path Forward.docx; SORN_DEPT 29_draft_(2017 09 07) DOC update.docx

Hello Kristen,

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)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Purvis, Catrina (Federal)

Subject:	NOAA4020
Location:	Open Office 52017 (SMC) Md Conf Rm Dial in number: (b)(6) (b)(6)
Start:	Thursday, December 7, 2017 10:00 AM
End:	Thursday, December 7, 2017 10:30 AM
Recurrence:	(none)
Meeting Status:	Not yet responsed
Organizer:	Purvis, Catrina (Federal)
Attachments:	NOAA4020 PIA_20171128 for MHG signature mhg.pdf; NOAA4020 PTA 2017 revised description_for BCPO signature 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) 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
NOAA4020
Science and Technology

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/NOAA4020
Science and Technology

Unique Project Identifier: 006-48-01-14-02-3305-00

Introduction: System Description

The NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

1) The Financial Services Division collects information from applicants for the following programs and purposes: The Fisheries Finance Program (FFP), credit information, personal identification including social security number, and tax returns. The information is used to verify applicants for fisheries loans. Capital Construction Fund (CCF), personal identification including social security numbers and tax returns. The information is used to verify applicants for CCF accounts and projects. Fishermen's Contingency Fund (FCF), personal identification including social security numbers, and personal transaction information. The information is used to verify business losses and lost fishing gear for claims made by the fishermen. Information collected includes tax returns.

   Information collected: applicant's name and address, the amount of financing applied for, the purpose of loans, an appraisal of the vessel or facility involved, financial information including the last 3 tax returns (these are not stored electronically), a list of creditors and buyers with relevant credit terms, identification of authorized representatives (accountant, attorney, insurance agent), and legal history (status regarding bankruptcy, litigation, delinquency on and Federal debt, etc.). Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated. Loan applications are entered into the system from paper forms completed by the public, into an online application, which is managed by NMFS NOAA4020. Regional offices access the information in order to administer loans for applicants. The loan data is stored only in NOAA4020.

   When a United States (U.S.) commercial fisherman sustains losses and/or damages as a result of oil and gas activities on the U.S. Outer Continental Shelf (OCS), the fisherman may apply for compensation from the U.S. Federal government, using fillable pdf forms on the applicable Web site.

NMFS also has programs to reduce excess fishing capacity by paying fishermen to surrender their vessels/permits. These fishing capacity reduction programs, or buybacks, are conducted pursuant to the Magnuson-Stevens Fishery Conservation and Management Act, and the Magnuson-Stevens Reauthorization Act (Pub. L. 109-479). The buybacks can be funded by a Federal loan to the industry or by direct Federal or other funding. Buyback regulations are at 50 CFR Part 600. The information collected by NMFS involves the submission of buyback requests by industry, submission of bids, referenda of fishery participants and reporting of collection of fees to repay buyback loans. For Fishery Capacity Reduction Program Buyback Requests, certain forms are submitted on paper and entered into a database, and others are submitted online.

Information is not shared except within the program (NMFS Headquarters, West Coast Region and Southeast Region), or in the case of a breach, within the bureau, the Department and other federal agencies (Justice).

2) International Trade Data System (ITDS).

ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports and exports of fisheries products. Types of BII data collected are Name of business, Address and Contact information. The data is collected from the U.S. Customs and Border Control's ITDS database. Reasons for the NMFS database:
(1) The CBP's ITDS only grants access to a small group of people who can meet their security clearance requirements which will take time and it seems they do want to limit the number of users. (2) The CBP's ITDS can't meet the specific requirements of the NMFS programs. So we developed our own ITDS to support the NMFS programs. For example, one program needs to the functions to track the harvesting vessel trips, all programs need the functions to review the data and track issues; the programs need to search data relevant to their programs etc.

3) Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL)

The Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL) system will be a tool to load raw data from various sources, format them and run through various QA/QC processes. NOAA4020 collects PII and BII data from MRIP ETL only for the NSAR, see below. Types of PII collected are fishing license info, Name, Address, Driver's license, Phone, Email and Date of Birth of the angler. Some states have requested that their data cleansed by this process be sent back to them.

4) National Saltwater Angler Registry - NSAR

The National Saltwater Angler Registry system allows the integration of the state-provided saltwater angler license data with the existing national registration data into a database, which

can be used as a consolidated phone book of the nation's recreational salt-water anglers. The captured data is entered into the database and will be used to furnish frames for the MRIP survey. Types of PII collected are Name, Address, and Driver's license, Telephone, Email and Date of Birth of the angler.

5) NOAA Fisheries Committee on Scientific Stature.

The NOAA Fisheries Committee on Scientific Stature (NFCSS) is a national-level Performance Management Advisory Committee (PMAC) established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. There is a website and database to manage and record the results of NFCSS member reviews conducted for the purpose of evaluating a scientist's credentials and contributions to allow them to be assigned to a higher pay Band without being a supervisor and to produce a standard report for the committee chair (OST Science Director). In 2014, OST upgraded the NFCSS website and database to enable password protected, role-based secure storage and retrieval of review package documents. Access to the database is restricted to the OST Science Director, the six regional Deputy Science Directors, one Band V research scientist from each regional science center, the NOAA Fisheries HR Business Partner, and the NFCSS database administrator and is provided by the NFCSS database administrator only at the request of the NFCSS Chair. Information collected: name, work contact information, letters of reference and curricula vitae, performance plan, science director memoranda and name of immediate supervisor. The administrator uploads copies of a memorandum from the NFCSS Chair to the Science Center director of staff being reviewed. The data (name, email, documents) for staff being reviewed are entered by their Deputy Science Director. The review comments are entered by the NFCSS members.

6) Protected Resources National Inventory of Marine Mammals (NIMM) System.

National Inventory of Marine Mammals (NIMM) was rolled out to the marine mammal Owners and Facilities, on July 18, 2017, with an initial user base of 151 users. NIMM maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. NOAA4020 collects PII and BII data from this system. Types of BII collected are Institution Name, Mailing address, Contact email, Phone and Fax Numbers. No PII is collected.

7) Highly Migratory Species.

Effective July 1, 2005, all dealers importing, exporting, or re-exporting bluefin tuna, swordfish, southern bluefin tuna and frozen bigeye tuna must hold a Highly Migratory Species International Fishery Trade Permit (HMS IFTP) and follow the required reporting procedures established at 50 C.F.R. 300.183 through 300.187. The HMS IFTP is required to assist the United States implement international trade tracking programs addressing illegal, unreported, and unregulated fishing activities, improve conservation and management measures, and enhance the scientific evaluation of these stocks.

Under international agreements and domestic law, the United States implements recommendations of the International Commission for the Conservation of Atlantic Tunas (ICCAT) and Inter-American Tropical Tuna Commission (IATTC). Both IATTC and ICCAT have implemented a statistical document program for frozen bigeye tuna. In addition, ICCAT has implemented bluefin tuna and swordfish statistical document programs.

The NMFS Office of Science and Technology developed a legacy Highly Migratory Species Dealer Permit System more than 10 years ago to meet the requirements outlined in the purpose above. The system has since been migrated over to the NMFS National Permit System, whose information is stored in NOAA4000. For historical validating of permits, the system is currently being retained for its reporting functionality for viewing and validating permit information on dealers. Please note that once all permits have expired on these two reports, there will be no more need to maintain these interfaces and will therefore be deactivated. NOAA4020 collects PII and BII data from Highly Migratory Species. Types of PII and BII data collected and processed are Applicant Name, Social Security Number, Position Type, Birthdate, Mailing Address Street Name, Business Name, Federal ID No/SSN, Date Business Formed, Business Type, Mailing Address Street Name etc. *No new data is being collected through this legacy system.*

8) NOAA Emergency Contact List
NOAA collects the Emergency Contact List that is used to track and locate staff in the office of Science and Technology. This is PII data.

9) NOAA4020 collects system user ID information from employees and contractors accessing the system.

Authorities

From NOAA-19: 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 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 Western and Central Pacific Fisheries Convention Implementation Act, 16 U.S.C. 6901 et seq. (WCPFCIA); the Marine Mammal Protection Act, 16 U.S.C. 1361; and Taxpayer Identifying Number, 31 U.S.C. 7701.

From NOAA-21: Title XI of the Merchant Marine Act of 1936 as amended and codified, 46 U.S.C. 1177 and 46 U.S.C. 53701 et seq., the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq., and provisions of the Debt Collection Improvement Act as codified at 31 U.S.C. 7701.

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.

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. Types of PII data collected is Contact Name, Phone Number and Address.

The legal authority for the Emergency Contact List 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.

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.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*
__ This is an existing information system with no changes that create new privacy risks.

Changes That Create New Privacy Risks (CTCNPR) - NA					
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): New application (NIMM) rolled out in 7/17.					

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	X*	f. Driver's License		j. Financial Account	X
c. Employer ID		g. Passport		k. Financial Transaction	X
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Required for identification of the individual for payment purposes, and for verification of financial information.
* Sec. 53074(c)(4): for the loan programs, the analysis of an applicant's financial condition requires a credit examination, for which the SSN would be needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	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):					

Work-Related Data (WRD)					
a. Occupation	X	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): For **Fisheries Committee on Scientific Stature**
j. Performance Plan
k. Supervisor Justification
l. Science Director Memoranda
m. Letters of Reference
n. Curriculum Vitae
o. Position Description

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	X
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	X	Online	X*
Telephone		Email			
Other (specify):					

* For the ECL

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	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): To determine loan, compensation and buyback qualifications from fishing vessel owners; to maintain databases for tracking international seafood trading tracking, angler registration, for use in reviewing scientists' research products, and a Protected Resources marine mammal inventory.			

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, members of the public, Capital Construction Fund Agreement, the Fishermen's Contingency Fund, foreign national, visitor or other (specify).

The Fisheries Finance Program (FFP) provides direct loans for certain fisheries costs. Vessel financing is available for the purchase of used vessels or the reconstruction of vessels (limited to reconstructions that do not add to fishing capacity). Refinancing is available for existing debt obligations. FFP loans are not issued for purposes which could contribute to over capitalization of the fishing industry. Finance or refinance fisheries shore side facilities or Aqua cultural facilities. The program provides Individual Fishing Quota (IFQ) financing (at the request of a Fishery Management Council). IFQ financing is available to first time purchasers and small vessel operators in the Halibut Sablefish fisheries. FFP also provides long term fishery buy back financing (at the request of a Fishery Management Council or

Governor) to purchase and retire fishing permits and/or fishing vessels in overcapitalized fisheries. Also, a United States (U.S.) commercial fisherman who sustains losses and/or damages as a result of oil and gas activities on the U.S. Outer Continental Shelf (OCS), the fisherman may apply for compensation from the U.S. Federal government.

FFP financing offers the fishing industry slightly better interest rates and longer term loans than are available elsewhere. The longer-term loans allow the industry to amortize their capital investment over the actual economic life of the fisheries asset. Lower debt service reduces economic pressure, thus allowing the borrower to more easily accommodate more restrictive fishery management initiatives. FFP regulations ensure that FFP traditional lending will not increase harvesting capacity in the fisheries but will simply permit the financing of the acquisition of existing vessels/facilities or the refinancing of existing debt for vessels/facilities already in the fishery.

Applications are required in order to determine qualification for a loan, and to provide contact information with borrowers. Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated.

This information is collected from members of the public.

The Emergency Contact List (ECL) is used to track and locate staff in the office of Science and Technology: name, occupation, work address and email. This information is collected from employees and contractors.

International Trade Data System (ITDS).
ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports and exports of fisheries products. Types of BII data collected are Name of business, Address and Contact information. The data is collected from the U.S. Customs and Border Control's ITDS database, who originally collected it from members of the public.

MRIP ETL
The MRIP ETL is a tool to load raw data from various sources, format them and run through various QA/QC processes. NOAA4020 collects PII and BII data from MRIP ETL. Types of PII collected are fishing license info, Name, Address, Driver's license, Phone, Email and Date of Birth of the angler. The MRIP ETL collects data from the NSAR, below.

National Saltwater Angler Registry - NSAR
The National Saltwater Angler Registry system allows the integration of the state-provided saltwater angler license data with the existing national registration data into a database, which can be used as a consolidated phone book of the nation's recreational salt-water anglers. The captured data is entered into the database and will be used to furnish frames for the MRIP survey. Some states have requested that their data cleansed by this process be sent back to them. Types of PII collected are Name, Address, Driver's license, Telephone, Email and Date

of Birth of the angler.

The **NOAA Fisheries Committee on Scientific Stature (NFCSS)** is a national-level PMAC established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. Information is only shared among the members of the NFCSS. The information is collected from members of the public.

1) **Protected Resources National Inventory of Marine Mammals (NIMM) System**.
National Inventory of Marine Mammals (NIMM) was rolled out to the marine mammal Owners and Facilities, on July 18, 2017, with an initial user base of 151 users. NIMM maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. NOAA4020 collects PII and BII data from this system. Types of BII collected are Institution Name, Mailing address, Contact email, Phone and Fax Numbers. NO PII is collected.

2) **Highly Migratory Species**.
Effective July 1, 2005, all dealers importing, exporting, or re-exporting bluefin tuna, swordfish, southern bluefin tuna and frozen bigeye tuna must hold a Highly Migratory Species International Trade Permit (HMS ITP) and follow the required reporting procedures established at 50 C.F.R. 300.183 through 300.187. The HMS ITP is required to assist the United States implement international trade tracking programs addressing illegal, unreported, and unregulated fishing activities, improve conservation and management measures, and enhance the scientific evaluation of these stocks.
The legacy system has since been migrated over to the NMFS National Permit System, whose information is stored in NOAA4000. For historical validating of permits, the system is currently being retained for its reporting functionality for viewing and validating permit information on dealers. Please note that once all permits have expired on these two reports, there will be no more need to maintain these interfaces and will therefore be deactivated. *No new data is being collected through this legacy system.*

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	X**		
Public	X**		
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach

**NIMM

	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: NOAA4020 connects with NOAA4000. Technical boundary controls are in place to prevent BII leakage. NOAA4020 consists of servers that support the development and deployment of application offerings that facilitate the provision of mission related services to the general public, authorized organizational and non-organizational users. NOAA4000 provides general support system (GSS, i.e. LAN/WAN network connectivity) services to NOAA4020.
	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. NOAA Buyback Program Site with PAS (also on forms): http://www.nmfs.noaa.gov/mb/financial services/buyback.htm Capital Construction Fund: all forms collecting PII are linked on this page: http://www.nmfs.noaa.gov/mb/financial services/ccf docs and forms.htm Fishermen's Contingency Fund: PAS is on this page: http://www.nmfs.noaa.gov/mb/financial services/fcf.htm and will be added to the forms. NSAR Site and PAS: https://www.countmyfish.noaa.gov/register/ The ECL PAS: *Site not available to non NOAA staff. A screen shot with the PAS is included in the cover email for this PIA.*	
X	Yes, notice is provided by other means.	Specify how: The FFP forms specify which information is required. The ECL has a Privacy Act Statement: This information collection is voluntary. The purpose is to maintain an emergency contact list. The personally identifiable information will not be shared outside the S&T. ITDS: The data is collected from the U.S. Customs and Border Control's ITDS database, who provides notice at the time of collection. NSAR: Notice is provided on the registration Web site: Anglers are also notified on the Web site, that their PII/BII may be used as part of a phone survey regarding fishing activities, before purchasing a license. MRIP ETL: No data collected directly by the system. NIMM: Upon being added to an organization as a Responsible Official or a Primary Contact, an automatic email is sent from NIMM. NFCSS: A screen shot signed by the director and operations director is included in the cover email. HMS Legacy System – no new information is being 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 FFP, applicants may decline to provide PII/BII, but if required information is not provided, the applicant

		cannot receive the benefit. For the ECL application, employees and contractors may decline to their supervisors in writing, but they may then not be notified in case of emergencies. ITDS: the NMFS ITDS is not the original point of collection. NIMM: An individual can chose not to be the responsible official or the primary contact. NSAR: The individual will not register if he wishes to decline. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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 FFP, consent for the specified use is implied by completing and signing the loan application. Notice is also provided in NOAA-21. Above the signature is this text: The Applicant certifies that: (1) it is a citizen of the United States (if a corporation, at least 75% of the stock must be held by U.S. citizens), and (2) all information in this application is true and correct to the best of the applicant's knowledge and belief and is submitted to obtain a loan from the Fisheries Finance Program. For the ECL, emergency contact is the only use for the information. ITDS: the NMFS ITDS is not the original point of collection. NIMM: There is only one use for the information. NSAR: Participation in the phone survey is required. Anglers may choose not to purchase a license. There is no option to purchase a license and opt out of the survey if chosen. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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 FFP, applicants/borrowers may provide updates at any time to the program office, by mail, fax, telephone or email, including when annual financial statements are submitted. For ECL, users may log on to the application and update the information at any time. ITDS: the NMFS ITDS is not the original point of collection. NIMM: Those with NIMM user accounts have access rights to review and update their data. NSAR: Information may be updated at the time of registration renewal. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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: Audit log
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 1/9/2017 ☐ 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.

The general controls used to protect the loan PII in these applications, involve controlled physical and logical access: role based access control, proper data segmentation and protection via encryption at rest and proper audit logging of events. Adequate media marking, transport and storage and incident monitoring and response are also used. The levels of implementation for these technologies meet the criteria required by NIST 800-53, Rev 4 under the following controls: Access Enforcement (AC-3), Separation of Duties (AC-5), Least Privilege (AC-6), Remote Access (AC-17), User-Based Collaboration and Information Sharing (AC-21). , Auditable Events (AU-2), Audit Review, Analysis, and Reporting (AU-6), Identification and Authentication (Organizational Users) (IA-2), Media Access (MP-2) , Media Marking (MP-3), Media Storage (MP-4), Media Transport (MP-5), Media Sanitization (MP-6), Transmission Confidentiality (SC-9), Protection of Information at Rest (SC-28), Information System Monitoring (SI-4). In addition to following database CIS benchmarks and best practices, all Oracle tables that contain PII/BII data are stored in an encrypted tablespace.

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-19**, Permits and Registrations for United States Federally Regulated Fisheries **COMMERCE/NOAA-21**, Financial Services Division **DEPT-18**, Employees Personnel Files Not Covered By Notices of Other Agencies **DEPT-13**, Investigative and Security Records.
	Yes, a SORN has been submitted to the Department for approval.
	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: 1510-01 **Pending Application files.** Applications for loans or other forms of assistance. Subdivided by type of aid. **Disposition** 1. Approved applications: Transfer to appropriate code for case file. 2. Rejected applications: Destroy after 5 years. 1510-02 **Fishery Loan files.** Case files on loans made to finance or refinance costs relating to fishing vessels, including their purchase. Includes applications, case histories, insurance policies, mortgages, and related correspondence and forms. **Disposition** 1. Collateral documents: Return to borrower when loan is repaid. 2. Other documents: Cut off when loan is repaid. Destroy 3 years later. 1512-13: International Trade Data System: **TEMPORARY**. Cut off closed files at end of calendar year, and transfer to FRC. Destroy when 20 years old. 1502-03: MRIP ETL: **PERMANENT.** Transfer to FRC after 5 years. Offer to NARA when 25 year 1515-03: NSAR: **TEMPORARY.** Cut off at end of study. Destroy 6 years after the completion of study. NFCSS: Chapter 300 Personnel Management Files 301-09 Supervisors' Personnel Files. Records on positions, authorizations, pending actions, position descriptions, training records, individual development plans, telework agreements, award recommendations, and records on individual employees not duplicated in or not appropriate for the OPF. These records are sometimes called supervisors' working files, unofficial personnel files (UPFs), and employee work folders or "drop" files. DAA-GRS-2017-0007-0012 (GRS 2.2, item 080) Supersedes NOAA Schedule Items: 303-22a (GRS 1, item 18a) 303-22b (GRS 1, item 18b) **TEMPORARY**. Review annually and destroy superseded documents. Destroy remaining documents 1 year after employee separation or transfer. 1514-03: NIMM: **PERMANENT.** Cut off files annually and transfer to FRC when 3 years old. Transfer to the National Archives when 25 years old. HMS: 1513-11 Fishery Law Enforcement and Surveillance Files

	1504 Fishery Management and Coordination Files 1504-18 Permit Fee Files 1504-21 Dealer, Buyer, Processor or Receiver Permits. Although there are some specific time limits on these items listed above, the data for these permits are stored indefinitely in our database. However, after this year when the last set of permitsare due to expire in December, this application will no longer be available. It will be decommissioned. All other data will be handled by the National Permit System (NPS). ECL: DAA-GRS- 2013-0006-003. Disposition instruction: Temporary. Destroy when business need ceases.
	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: Loan data includes Tax ID Numbers, which. uniquely and directly identify individuals or businesses.
X	Quantity of PII	Provide explanation: Collective harm to individuals, but also harm to the organization's reputation and the cost to the organization in addressing a possible breach was considered.

X	Data Field Sensitivity	Provide explanation: There are sensitive data fields, including SSN/EIN.
X	Context of Use	Provide explanation The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated was considered. Whether disclosure of the mere fact that PII is being collected or used could cause harm to the organization or individual was considered.
X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801, Section 402b.
X	Access to and Location of PII	Provide explanation: The nature of authorized access to PII - The number and frequency of access was also considered. The degree to which PII is being stored on or accessed from teleworkers' devices or other systems, such as web applications, outside the direct control of the organization and whether PII is stored or regularly transported off-site by employees was considered.
	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 System Owner Name: Frank Schwing Office: Office of Science and Technology Phone: 301-427-8220 Email: franklin.schwing@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: SCHWING.FRANKLIN.B.DR.1365840748 Digitally signed by SCHW NG FRANKLIN B DR 1365840748 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=SCHWING FRANKLIN B DR 1365840748 Date: 2017 11 28 16:39:20 05'00' Date signed:	**Information Technology Security Officer** Name: Catherine Amores Office: Office of the Chief Information Officer 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: 2017.12.04 14:37:59 -05'00' Date signed:
Authorizing Official Name: Ned Cyr Office: Office of Science and Technology Phone: 301-427-8123 Email:ned.cyr@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: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 Date: 2017.12.04 12:55:24 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5358 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: 2017 12 04 16:23:35 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
National Oceanic and Atmospheric Administration
(NOAA)

Privacy Threshold Analysis
for the
NOAA4020
Office of Science and Technology

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Office of Science and Technology

Unique Project Identifier: 006-48-01-14-02-3305-00

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 and its purpose 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 NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

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): New application (NIMM) rolled out in 7/17.					

____ 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.

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

NOAA 4020 contains a variety of PII and BII, including permit application data and loan application data.

____ 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 [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: TAYLOR.GLEN.CLIFFORD.1365840934 Digitally signed by TAYLOR GLEN CLIFFORD 1365840934 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=TAYLOR GLEN CLIFFORD 1365840934 Date: 2017 11 15 12:48:07 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2017.12.04 12:03:34 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn CYR.EDWARD.C.DR.1365869436 Date: 2017.11.15 15:59:45 -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: 2017.12.04 12:47:03 -05'00' Date: _____

Purvis, Catrina (Federal)

Subject:	Canceled: CRB NOAA8884
Location:	Open Office 52017 (SMC) Md Conf Rm Dial in number: (b)(6) (b)(6)
Start:	Thursday, December 7, 2017 9:30 AM
End:	Thursday, December 7, 2017 10:00 AM
Recurrence:	(none)
Meeting Status:	Not yet responsed
Organizer:	Purvis, Catrina (Federal)
Attachments:	NOAA8884 PTA 032717 for MHG signature mhg.pdf; NOAA8884 PIA 11162017 Final mhg.pdf
Importance:	High

Per the bureau's request on December 6, this meeting will be rescheduled when a slot becomes available in the 2nd Qtr.

Mark/Sarah

Please provide the signed PIA/PTAs for the system identified above by 10am Tuesday, December 5 to avoid cancellation of this meetings.

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) 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.

The only personally identifiable information (PII) maintained in the system is in a local database at the local Weather Forecast Office/River Forecast Center that maintains information on volunteers who provide weather reports to them.

No information is shared except in the case of security or privacy breach (see Section 6.1)

The statutory authorities 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].

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.

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.
__X_ This is an existing information system with no new privacy risks.
____ 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):					

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): General description of volunteer's home location.					

Work-Related Data (WRD)					
a. Occupation		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):					

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)

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		Commercial Data Brokers	
Third Party Website or Application				
Other (specify):				

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		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 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.

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

	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.	
	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: Notice to volunteers is provided when information is collected, via the cooperative agreement 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: 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.
	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.

	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.
	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.
	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):_____**4/39/2017**_____ ☐ 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 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.

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.
	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	
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: Only name and contact information for volunteers, and names of employees, are in the system.
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields.
X	Context of Use	Provide explanation: Voluntary submission of PII for internal use only
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: 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: Gary Petroski
Office: NOAA/NWS/SRH
Phone: (682) 703-3717
Email: Gary.Petroski@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: PETROSKI.GARY.P.1196647984
Digitally signed by PETROSKI GARY P 1196647984
DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn PETROSKI GARY P 1196647984
Date 2017 11 16 14 20 23 06'00'

Information Technology Security Officer

Name: Beckie Koonge
Office: NOAA NWS Office of the CIO
Phone: 301-427-9020
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: KOONGE.BECKIE.A.1408306880
Digitally signed by KOONGE BECKIE A 1408306880
Date 2017 11 17 10 53 28 05'00'

Authorizing Official

Name: Steven Cooper
Office: NOAA/NWS/SRH
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: Steven G. Cooper
Digitally signed by COOPER STEVEN G 1365850930
Date: 2017 11 16 17:13:58 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 2017 11 20 09 15 57 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: 01-2016

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.*

____l 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 l 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.)."

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

____l Companies
____l Other business entities

__X l 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.)*

____1 DOC employees
____1 Contractors working on behalf of DOC
__X 1 Members of the public

____1 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 NOAA8884 and as a consequence of this applicability, I would perform and document a PIA for this IT system. However, there are no new changes creating privacy risks since the PIA was approved by DOC in December 2016.

____ I certify the criteria implied by the questions above **do not apply** to NOAAA8884 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_____

Signature of ISSO or SO: PETROSKI.GARY.P.1196647984 Digitally signed by PETROSKI GARY P 1196647984 DN: c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn PETROSKI GARY P 1196647984 Date: 2017 03 24 09:46:50 05'00' Date: _____

Name of Information Technology Security Officer (ITSO):

Beckie Koonge_____

Signature of ITSO: KOONGE.BECKIE.A.1408306880 Digitally signed by KOONGE.BECKIE.A.1408306880 Date: 2017.03.28 15:46:53 04'00' Date: _____

Name of Authorizing Official (AO):

Steven Cooper_____

Signature of AO: COOPER.STEVEN.G.1365850930 Digitally signed by COOPER.STEVEN.G.1365850930 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=COOPER.STEVEN.G.1365850930 Date: 2017.03.24 15:19:52 -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: 2017.04.11 10:24:43 -04'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, December 7, 2017 12:53 PM
To:	Gioffre, Kathy (Federal); Ferguson, Dorrie; CPO; Toland, Michael; Gitelman, Steve (Contractor)
Cc:	Mark Graff NOAA Federal; Franklin Schwing NOAA Federal; Glen Taylor; Scott Sauri; Amores, Catherine (Federal); Rick Miner NOAA Federal; Tahir Ismail; NMFS.InfoSec@noaa.gov
Subject:	PER NOAA4020 CRB: REVISED DOCs attached
Attachments:	NOAA4020(12 07 17)Final_noaa response.docx; NOAA4020 PIA_112817_revised per CRB 120717..pdf; NOAA4020 PTA 2017 revised description v2.pdf

Attached are the corrected NOAA4020 PTA and PIA, and the CRB minutes with NOAA responses.

For Section 2.2, at the beginning, there was a sentence fragment that I think should have been deleted (see my ???).

thx Sarah

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

NOAA OCIO
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
NOAA4020
Science and Technology

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/NOAA4020
Science and Technology

Unique Project Identifier: 006-48-01-14-02-3305-00

Introduction: System Description

The NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

1) The Financial Services Division collects information from applicants for the following programs and purposes: The Fisheries Finance Program (FFP), credit information, personal identification including social security number, and tax returns. The information is used to verify applicants for fisheries loans. Capital Construction Fund (CCF), personal identification including social security numbers and tax returns. The information is used to verify applicants for CCF accounts and projects. Fishermen's Contingency Fund (FCF), personal identification including social security numbers, and personal transaction information. The information is used to verify business losses and lost fishing gear for claims made by the fishermen. Information collected includes tax returns.

   Information collected: applicant's name and address, the amount of financing applied for, the purpose of loans, an appraisal of the vessel or facility involved, financial information including the last 3 tax returns (these are not stored electronically), a list of creditors and buyers with relevant credit terms, identification of authorized representatives (accountant, attorney, insurance agent), and legal history (status regarding bankruptcy, litigation, delinquency on and Federal debt, etc.). Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated. Loan applications are entered into the system from paper forms completed by the public, into an online application, which is managed by NMFS NOAA4020. Regional offices access the information in order to administer loans for applicants. The loan data is stored only in NOAA4020.

   When a United States (U.S.) commercial fisherman sustains losses and/or damages as a result of oil and gas activities on the U.S. Outer Continental Shelf (OCS), the fisherman may apply for compensation from the U.S. Federal government, using fillable pdf forms on the applicable Web site.

NMFS also has programs to reduce excess fishing capacity by paying fishermen to surrender their vessels/permits. These fishing capacity reduction programs, or buybacks, are conducted pursuant to the Magnuson-Stevens Fishery Conservation and Management Act, and the Magnuson-Stevens Reauthorization Act (Pub. L. 109-479). The buybacks can be funded by a Federal loan to the industry or by direct Federal or other funding. Buyback regulations are at 50 CFR Part 600. The information collected by NMFS involves the submission of buyback requests by industry, submission of bids, referenda of fishery participants and reporting of collection of fees to repay buyback loans. For Fishery Capacity Reduction Program Buyback Requests, certain forms are submitted on paper and entered into a database, and others are submitted online.

Information is not shared except within the program (NMFS Headquarters, West Coast Region and Southeast Region), or in the case of a breach, within the bureau, the Department and other federal agencies (Justice).

2) International Trade Data System (ITDS).

ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports and exports of fisheries products. Types of BII data collected are Name of business, Address and Contact information. The data is collected from the U.S. Customs and Border Control's ITDS database. Reasons for the NMFS database:
(1) The CBP's ITDS only grants access to a small group of people who can meet their security clearance requirements which will take time and it seems they do want to limit the number of users. (2) The CBP's ITDS can't meet the specific requirements of the NMFS programs. So we developed our own ITDS to support the NMFS programs. For example, one program needs to the functions to track the harvesting vessel trips, all programs need the functions to review the data and track issues; the programs need to search data relevant to their programs etc.

3) Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL)

The Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL) system will be a tool to load raw data from various sources, format them and run through various QA/QC processes. NOAA4020 collects PII and BII data from MRIP ETL only for the NSAR, see below. Types of PII collected are fishing license info, Name, Address, Driver's license, Phone, Email and Date of Birth of the angler. Some states have requested that their data cleansed by this process be sent back to them.

4) National Saltwater Angler Registry - NSAR

The National Saltwater Angler Registry system allows the integration of the state-provided saltwater angler license data with the existing national registration data into a database, which

can be used as a consolidated phone book of the nation's recreational salt-water anglers. The captured data is entered into the database and will be used to furnish frames for the MRIP survey. Types of PII collected are Name, Address, Driver's license, Telephone, Email and Date of Birth of the angler.

5) NOAA Fisheries Committee on Scientific Stature. This is not an outside advisory committee.

The NOAA Fisheries Committee on Scientific Stature (NFCSS) is a national-level Performance Management Advisory Committee (PMAC) established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. There is a website and database to manage and record the results of NFCSS member reviews conducted for the purpose of evaluating a scientist's credentials and contributions to allow them to be assigned to a higher pay Band without being a supervisor and to produce a standard report for the committee chair (OST Science Director). In 2014, OST upgraded the NFCSS website and database to enable password protected, role-based secure storage and retrieval of review package documents. Access to the database is restricted to the OST Science Director, the six regional Deputy Science Directors, one Band V research scientist from each regional science center, the NOAA Fisheries HR Business Partner, and the NFCSS database administrator and is provided by the NFCSS database administrator only at the request of the NFCSS Chair. Information collected: name, work contact information, letters of reference and curricula vitae, performance plan, science director memoranda and name of immediate supervisor. The administrator uploads copies of a memorandum from the NFCSS Chair to the Science Center director of staff being reviewed. The data (name, email, documents) for staff being reviewed are entered by their Deputy Science Director. The review comments are entered by the NFCSS members.

6) Protected Resources National Inventory of Marine Mammals (NIMM) System.

National Inventory of Marine Mammals (NIMM) was rolled out to the marine mammal Owners and Facilities, on July 18, 2017, with an initial user base of 151 users. NIMM maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. NOAA4020

collects PII and BII data from this system. Types of BII collected are Institution Name, Mailing address, Contact email, Phone and Fax Numbers.

7) Highly Migratory Species.

Effective July 1, 2005, all dealers importing, exporting, or re-exporting bluefin tuna, swordfish, southern bluefin tuna and frozen bigeye tuna must hold a Highly Migratory Species International Fishery Trade Permit (HMS IFTP) and follow the required reporting procedures established at 50 C.F.R. 300.183 through 300.187. The HMS IFTP is required to assist the United States implement international trade tracking programs addressing illegal, unreported, and unregulated fishing activities, improve conservation and management measures, and enhance the scientific evaluation of these stocks.

Under international agreements and domestic law, the United States implements recommendations of the International Commission for the Conservation of Atlantic Tunas (ICCAT) and Inter-American Tropical Tuna Commission (IATTC). Both IATTC and ICCAT have implemented a statistical document program for frozen bigeye tuna. In addition, ICCAT has implemented bluefin tuna and swordfish statistical document programs.

The NMFS Office of Science and Technology developed a legacy Highly Migratory Species Dealer Permit System more than 10 years ago to meet the requirements outlined in the purpose above. The system has since been migrated over to the NMFS National Permit System, whose information is stored in NOAA4000. For historical validating of permits, the system is currently being retained for its reporting functionality for viewing and validating permit information on dealers. Please note that once all permits have expired on these two reports, there will be no more need to maintain these interfaces and will therefore be deactivated. NOAA4020 collects PII and BII data from Highly Migratory Species. Types of PII and BII data collected and processed are Applicant Name, Social Security Number, Position Type, Birthdate, Mailing Address Street Name, Business Name, Federal ID No/SSN, Date Business Formed, Business Type, Mailing Address Street Name etc. *No new data is being collected through this legacy system.*

8) NOAA Emergency Contact List
NOAA collects the Emergency Contact List that is used to track and locate staff in the office of Science and Technology. This is PII data.

9) NOAA4020 collects system user ID information from employees and contractors accessing the system.

Authorities

From NOAA-19: 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

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 Western and Central Pacific Fisheries Convention Implementation Act, 16 U.S.C. 6901 et seq. (WCPFCIA); the Marine Mammal Protection Act, 16 U.S.C. 1361; and Taxpayer Identifying Number, 31 U.S.C. 7701.

From NOAA-21: Title XI of the Merchant Marine Act of 1936 as amended and codified, 46 U.S.C. 1177 and 46 U.S.C. 53701 et seq., the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq., and provisions of the Debt Collection Improvement Act as codified at 31 U.S.C. 7701.

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.

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. Types of PII data collected is Contact Name, Phone Number and Address.

The legal authority for the Emergency Contact List 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.

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.
_X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*
__ This is an existing information system with no changes that create new privacy risks.

Changes That Create New Privacy Risks (CTCNPR) - NA					
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): New application (NIMM) rolled out in 7/17.					

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	X*	f. Driver's License	X	j. Financial Account	X
c. Employer ID		g. Passport		k. Financial Transaction	X
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Required for identification of the individual for payment purposes, and for verification of financial information.
* Sec. 53074(c)(4): for the loan programs, the analysis of an applicant's financial condition requires a credit examination, for which the SSN would be needed.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	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	X	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		e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			

i. Other work-related data (specify): For **Fisheries Committee on Scientific Stature**
j. Performance Plan
k. Supervisor Justification
l. Science Director Memoranda
m. Letters of Reference
n. Curriculum Vitae
o. Position Description

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	X
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	X	Online	X*
Telephone		Email			
Other (specify):					

* For the ECL

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

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	X
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	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): To determine loan, compensation and buyback qualifications from fishing vessel owners; to maintain databases for tracking international seafood trading tracking, angler registration, for use in reviewing scientists' research products, and a Protected Resources marine mammal inventory.			

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, members of the public, Capital Construction Fund Agreement, the Fishermen's Contingency Fund, foreign national, visitor or other (specify).

The Fisheries Finance Program (FFP) provides direct loans for certain fisheries costs. Vessel financing is available for the purchase of used vessels or the reconstruction of vessels (limited to reconstructions that do not add to fishing capacity). Refinancing is available for existing debt obligations. FFP loans are not issued for purposes which could contribute to over capitalization of the fishing industry. Finance or refinance fisheries shore side facilities or Aqua cultural facilities. The program provides Individual Fishing Quota (IFQ) financing (at the request of a Fishery Management Council). IFQ financing is available to first time purchasers and small vessel operators in the Halibut Sablefish fisheries. FFP also provides long term fishery buy back financing (at the request of a Fishery Management Council or Governor) to purchase and retire fishing permits and/or fishing vessels in overcapitalized fisheries. Also, a United States (U.S.) commercial fisherman who sustains losses and/or damages as a result of oil and gas activities on the U.S. Outer Continental Shelf (OCS), the fisherman may apply for compensation from the U.S. Federal government.

FFP financing offers the fishing industry slightly better interest rates and longer term loans than are available elsewhere. The longer-term loans allow the industry to amortize their capital investment over the actual economic life of the fisheries asset. Lower debt service reduces economic pressure, thus allowing the borrower to more easily accommodate more restrictive fishery management initiatives. FFP regulations ensure that FFP traditional lending will not increase harvesting capacity in the fisheries but will simply permit the financing of the acquisition of existing vessels/facilities or the refinancing of existing debt for vessels/facilities already in the fishery.

Applications are required in order to determine qualification for a loan, and to provide contact information with borrowers. Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated.

This information is collected from members of the public.

The Emergency Contact List (ECL) is used to track and locate staff in the office of Science and Technology: name, occupation, work address and email. This information is collected from employees and contractors.

International Trade Data System (ITDS).
ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports and exports of fisheries products. Types of BII data collected are Name of business, Address and Contact information. The data is collected from the U.S. Customs and Border Control's ITDS database, who originally collected it from members of the public.

MRIP ETL
The MRIP ETL is a tool to load raw data from various sources including states, format them and run through various QA/QC processes. NOAA4020 collects PII and BII data from MRIP ETL. Types of PII collected are fishing license info, Name, Address, Driver's license, Phone,

Email and Date of Birth of the angler. The MRIP ETL collects data from the NSAR, below.

National Saltwater Angler Registry - NSAR
The National Saltwater Angler Registry system allows the integration of the state-provided saltwater angler license data with the existing national registration data into a database, which can be used as a consolidated phone book of the nation's recreational salt-water anglers. The captured data is entered into the database and will be used to furnish frames for the MRIP survey. Some states have requested that their data cleansed by this process be sent back to them. Types of PII collected are Name, Address, Driver's license, Telephone, Email and Date of Birth of the angler.

The **NOAA Fisheries Committee on Scientific Stature (NFCSS)** is a national-level PMAC established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. Information is only shared among the members of the NFCSS. The information is collected from members of the public.

1) **Protected Resources National Inventory of Marine Mammals (NIMM) System**.
National Inventory of Marine Mammals (NIMM) was rolled out to the marine mammal Owners and Facilities, on July 18, 2017, with an initial user base of 151 users. NIMM maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS' jurisdiction (dolphins, porpoises, whales, seals and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. NOAA4020 collects PII and BII data from this system. Types of BII collected are Institution Name, Mailing address, Contact email, Phone and Fax Numbers. NO PII is collected.

2) **Highly Migratory Species**.
Effective July 1, 2005, all dealers importing, exporting, or re-exporting bluefin tuna, swordfish, southern bluefin tuna and frozen bigeye tuna must hold a Highly Migratory Species International Trade Permit (HMS ITP) and follow the required reporting procedures established at 50 C.F.R. 300.183 through 300.187. The HMS ITP is required to assist the United States implement international trade tracking programs addressing illegal, unreported, and unregulated fishing activities, improve conservation and management measures, and enhance the scientific evaluation of these stocks.
The legacy system has since been migrated over to the NMFS National Permit System, whose information is stored in NOAA4000. For historical validating of permits, the system is

currently being retained for its reporting functionality for viewing and validating permit information on dealers. Please note that once all permits have expired on these two reports, there will be no more need to maintain these interfaces and will therefore be deactivated. *No new data is being collected through this legacy system.*

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	X**		
Public	X**		
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*In case of breach

**NIMM

	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: NOAA4020 connects with NOAA4000. Technical boundary controls are in place to prevent BII leakage. NOAA4020 consists of servers that support the development and deployment of application offerings that facilitate the provision of mission related services to the general public, authorized organizational and non-organizational users. NOAA4000 provides general support system (GSS, i.e. LAN/WAN network

	connectivity) services to NOAA4020.
	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. NOAA Buyback Program Site with PAS (also on forms): http://www.nmfs.noaa.gov/mb/financial_services/buyback.htm Capital Construction Fund: all forms collecting PII are linked on this page: http://www.nmfs.noaa.gov/mb/financial_services/ccf_docs_and_forms.htm Fishermen's Contingency Fund: PAS is on this page: http://www.nmfs.noaa.gov/mb/financial_services/fcf.htm and will be added to the forms. NSAR Site and PAS: https://www.countmyfish.noaa.gov/register/ The ECL PAS: *Site not available to non NOAA staff. A screen shot with the PAS is included in the cover email for this PIA.*	
X	Yes, notice is provided by other means.	Specify how: The FFP forms specify which information is required. The ECL has a Privacy Act Statement: This information collection is voluntary. The purpose is to maintain an emergency contact list. The personally identifiable information will not be shared outside the S&T. ITDS: The data is collected from the U.S. Customs and Border Control's ITDS database, who provides notice at the time of collection.

		NSAR: Notice is provided on the registration Web site: Anglers are also notified on the Web site, that their PII/BII may be used as part of a phone survey regarding fishing activities, before purchasing a license. MRIP ETL: No data collected directly by the system. NIMM: Upon being added to an organization as a Responsible Official or a Primary Contact, an automatic email is sent from NIMM. NFCSS: A screen shot signed by the director and operations director is included in the cover email. HMS Legacy System – no new information is being 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 FFP, applicants may decline to provide PII/BII, but if required information is not provided, the applicant cannot receive the benefit. For the ECL application, employees and contractors may decline to their supervisors in writing, but they may then not be notified in case of emergencies. ITDS: the NMFS ITDS is not the original point of collection. NIMM: An individual can chose not to be the responsible official or the primary contact. NSAR: The individual will not register if he wishes to decline. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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 FFP, consent for the specified use is implied by completing and signing the loan application. Notice is also provided in NOAA-21. Above the signature is this text: The Applicant certifies that: (1) it is a citizen of the United States (if

		a corporation, at least 75% of the stock must be held by U.S. citizens), and (2) all information in this application is true and correct to the best of the applicant's knowledge and belief and is submitted to obtain a loan from the Fisheries Finance Program. For the ECL, emergency contact is the only use for the information. ITDS: the NMFS ITDS is not the original point of collection. NIMM: There is only one use for the information. NSAR: Participation in the phone survey is required. Anglers may choose not to purchase a license. There is no option to purchase a license and opt out of the survey if chosen. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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 FFP, applicants/borrowers may provide updates at any time to the program office, by mail, fax, telephone or email, including when annual financial statements are submitted. For ECL, users may log on to the application and update the information at any time. ITDS: the NMFS ITDS is not the original point of collection. NIMM: Those with NIMM user accounts have access rights to review and update their data. NSAR: Information may be updated at the time of registration renewal. MRIP ETL: No data collected directly by the system. HMS Legacy System – no new information is being collected.
	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: Audit log
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 1/9/2017 ☐ 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.

The general controls used to protect the loan PII in these applications, involve controlled physical and logical access: role based access control, proper data segmentation and protection via encryption at rest and proper audit logging of events. Adequate media marking, transport and storage and incident monitoring and response are also used.

The levels of implementation for these technologies meet the criteria required by NIST 800-53, Rev 4 under the following controls: Access Enforcement (AC-3), Separation of Duties (AC-5), Least Privilege (AC-6), Remote Access (AC-17), User-Based Collaboration and Information Sharing (AC-21). , Auditable Events (AU-2), Audit Review, Analysis, and Reporting (AU-6), Identification and Authentication (Organizational Users) (IA-2), Media Access (MP-2) , Media Marking (MP-3), Media Storage (MP-4), Media Transport (MP-5), Media Sanitization (MP-6), Transmission Confidentiality (SC-9), Protection of Information at Rest (SC-28), Information System Monitoring (SI-4).

In addition to following database CIS benchmarks and best practices, all Oracle tables that contain PII/BII data are stored in an encrypted tablespace.

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-19**, Permits and Registrations for United States Federally Regulated Fisheries **COMMERCE/NOAA-21**, Financial Services Division **DEPT-18**, Employees Personnel Files Not Covered By Notices of Other Agencies **DEPT-13**, Investigative and Security Records.
	Yes, a SORN has been submitted to the Department for approval.
	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: 1510-01 **Pending Application files.** Applications for loans or other forms of assistance. Subdivided by type of aid. **Disposition** 1. Approved applications: Transfer to appropriate code for case file. 2. Rejected applications: Destroy after 5 years. 1510-02 **Fishery Loan files.** Case files on loans made to finance or refinance costs relating to fishing vessels, including their purchase. Includes applications, case histories, insurance policies, mortgages, and related correspondence and forms. **Disposition** 1. Collateral documents: Return to borrower when loan is repaid. 2. Other documents: Cut off when loan is repaid. Destroy 3 years later. 1512-13: International Trade Data System: **TEMPORARY**. Cut off closed files at end of calendar year, and transfer to FRC. Destroy when 20 years old. 1502-03: MRIP ETL: **PERMANENT.** Transfer to FRC after 5 years. Offer to NARA when 25 year 1515-03: NSAR: **TEMPORARY.** Cut off at end of study. Destroy 6 years after the completion of study.

	NFCSS: Chapter 300 Personnel Management Files 301-09 Supervisors' Personnel Files. Records on positions, authorizations, pending actions, position descriptions, training records, individual development plans, telework agreements, award recommendations, and records on individual employees not duplicated in or not appropriate for the OPF. These records are sometimes called supervisors' working files, unofficial personnel files (UPFs), and employee work folders or "drop" files. DAA-GRS-2017-0007-0012 (GRS 2.2, item 080) Supersedes NOAA Schedule Items: 303-22a (GRS 1, item 18a) 303-22b (GRS 1, item 18b) **TEMPORARY**. Review annually and destroy superseded documents. Destroy remaining documents 1 year after employee separation or transfer. 1514-03: NIMM: **PERMANENT.** Cut off files annually and transfer to FRC when 3 years old. Transfer to the National Archives when 25 years old. HMS: 1513-11 Fishery Law Enforcement and Surveillance Files 1504 Fishery Management and Coordination Files 1504-18 Permit Fee Files 1504-21 Dealer, Buyer, Processor or Receiver Permits. Although there are some specific time limits on these items listed above, the data for these permits are stored indefinitely in our database. However, after this year when the last set of permits are due to expire in December, this application will no longer be available. It will be decommissioned. All other data will be handled by the National Permit System (NPS). ECL: DAA-GRS- 2013-0006-003. Disposition instruction: Temporary. Destroy when business need ceases.
	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: Loan data includes Tax ID Numbers, which. uniquely and directly identify individuals or businesses.
X	Quantity of PII	Provide explanation: Collective harm to individuals, but also harm to the organization's reputation and the cost to the organization in addressing a possible breach was considered.
X	Data Field Sensitivity	Provide explanation: There are sensitive data fields, including SSN/EIN.
X	Context of Use	Provide explanation The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated was considered. Whether disclosure of the mere fact that PII is being collected or used could cause harm to the organization or individual was considered.
X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801, Section 402b.
X	Access to and Location of PII	Provide explanation: The nature of authorized access to PII - The number and frequency of access was also considered. The degree to which PII is being stored on or accessed from teleworkers' devices or other systems, such as web applications, outside the direct control of the organization and whether PII is stored or regularly transported off-site by employees was considered.
	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 System Owner Name: Frank Schwing Office: Office of Science and Technology Phone: 301-427-8220 Email: franklin.schwing@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: SCHWING.FRANKLIN.B.DR.1365840748 Digitally signed by SCHWING.FRANKLIN.B.DR.1365840748 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SCHWING.FRANKLIN.B.DR.1365840748 Date: 2017.11.28 16:39:20 05'00' Date signed:	**Information Technology Security Officer** Name: Catherine Amores Office: Office of the Chief Information Officer 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: 2017.12.04 14:37:59 -05'00' Date signed:
Authorizing Official Name: Ned Cyr Office: Office of Science and Technology Phone: 301-427-8123 Email:ned.cyr@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: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 Date: 2017.12.04 12:55:24 -05'00' Date signed:	**Bureau Chief Privacy Officer** Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5358 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: 2017.12.04 16:23:35 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
National Oceanic and Atmospheric Administration
(NOAA)

Privacy Threshold Analysis
for the
NOAA4020
Office of Science and Technology

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Office of Science and Technology

Unique Project Identifier: 006-48-01-14-02-3305-00

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 and its purpose 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 NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

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): New application (NIMM) rolled out in 7/17.					

____ 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.)."

_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 [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: TAYLOR.GLEN.CLIFFORD.1365840934 Digitally signed by TAYLOR GLEN CLIFFORD 1365840934 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=TAYLOR GLEN CLIFFORD 1365840934 Date: 2017 11 15 12:48:07 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2017.12.04 12:03:34 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: CYR.EDWARD.C.DR.1365869436 Digitally signed by CYR.EDWARD.C.DR.1365869436 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn CYR.EDWARD.C.DR.1365869436 Date: 2017.11.15 15:59:45 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____MARK GRAFF_____

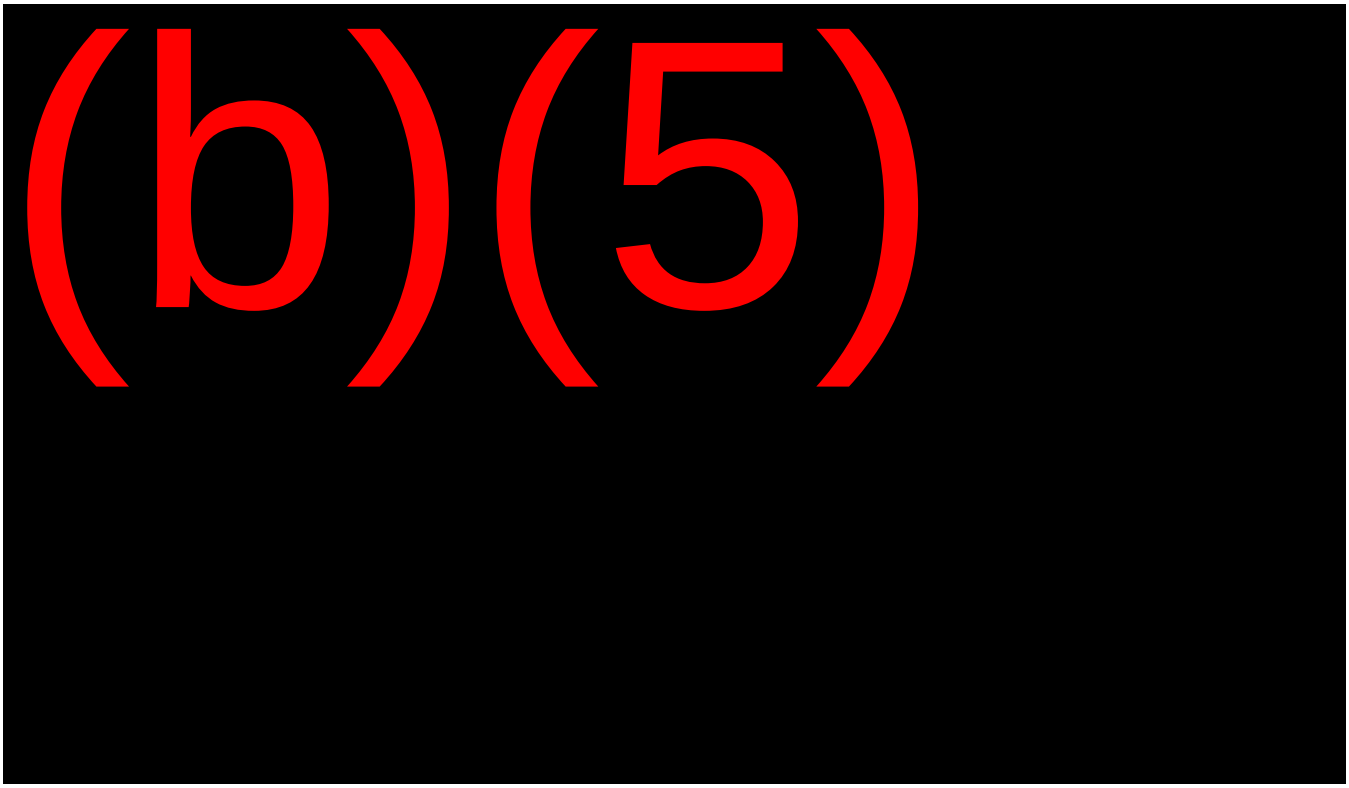
Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn GRAFF.MARK.HYRUM.1514447892 Date: 2017.12.04 12:47:03 -05'00' Date: _____

Privacy Impact Assessment (PIA) Compliance Review Board (CRB) Meeting Minutes
NOAA Office of Science and Technology (NOAA4020)
December 7, 2017

Attendees:

Privacy Team
Kathy Gioffre
Steve Gitelman
Dorrie Ferguson
Christin Brown (OCIO)
Eric Cline (OCIO)

NOAA
Mark Graff
Sarah Brabson
Tahir Ismail
Glenn Taylor
Frank Schwing
Nancy Majower
Kathy Amores
Rick Miner
Scott Sauri




(b)(5)

Cathy Readinger

From:	Cathy Readinger
Sent:	Monday, December 11, 2017 10:22 AM
To:	Mark Graff NOAA Federal
Cc:	foia@noaa.gov; Lola Stith NOAA Affiliate
Subject:	Re: Privacy Act Exemptions
Attachments:	Records request to Bosarge.docx

Dear Mr. Graff,

The records that you have cited were not included in my FOIA request. The records request for items 1 through 10 of the attached document are records that I requested from the Gulf Council exclusive of the FOIA request.

Please explain why the provisions of the FOIA are being applied to these records.

Thank you,

Cathy Readinger
813.846.8170

On Thu, Nov 30, 2017 at 1:47 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

> Hello Ms. Readinger,
>
> The exempt "Categories of Records" can be found within the SORNs that apply to records identified in your request. For your specific request, these include DOC SORNs DEPT 1 (attendance, leave, and payroll records), DEPT 13 (investigative and security records), and DEPT 18 (Employees Personnel Files Not Covered by Notices of Other Agencies).
>
> The Categories of Records identified in these SORNs you have requested each are subject to Exemptions (k)(2) and (j)(2). However, the applicability of a Privacy Act Exemption does not preclude disclosure globally. Your request will continue to be processed and the non exempt portions will be disclosed pursuant to the FOIA. Please let me know if you have any further questions as your request proceeds.
>
> Mark H. Graff
> FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> National Oceanic and Atmospheric Administration
> (301) 628 5658 (O)
> (b)(6) (C)
>
>

On Thu, Nov 30, 2017 at 1:16 PM, Cathy Readinger <cathyreadinger@gmail.com> wrote:

Dear Mr. Graff:

Can you please provide me with a list of records that you have determined are exempt from the Access provisions of the Privacy Act based on Privacy Act Exemptions 5 USC 552a(k)(2) and 5 USC 552a(j)(2) as referenced in 15 CFR 4.25(g)(2)(iii)?

I discussed the issue with Beverly Smith of the SERO, and she suggested that I contact you.

Thank you,

Cathy Readinger
813.846.8170

On Tue, Nov 21, 2017 at 9:45 AM, foia@noaa.gov <foia@noaa.gov> wrote:

11/21/2017 09:29 AM
FOIA Request: DOC NOAA 2018 000070

This is in response to your request for records regarding yourself that you submitted on October 3, 2017. Your request has first been processed pursuant to the Privacy Act to determine whether or not you are eligible for access to the records based on 5 USC 552a(d)(1).

Upon review, I have determined that the records you are seeking are exempt from the Access provisions of the Privacy Act based on Privacy Act Exemptions 5 USC 552a(k)(2) and 5 USC 552a(j)(2) as referenced in 15 CFR 4.25(g)(2)(iii). However, you are still entitled to disclosure of the records subject to the provisions of the FOIA. Your request will be processed, and you will be provided any non exempt portions pursuant to the disclosure provisions of the FOIA.

You are entitled to review of this decision consistent with 15 CFR 4.25(g)(3)(i) or you may challenge the validity of the Exemption itself pursuant to 5 USC 553(e).

You have the right to appeal this denial of the Privacy Act request. An appeal must be received within 90 calendar days of the date of this response letter by the Assistant General Counsel for Administration (Office), Room 5898 C, U.S. Department of Commerce, 14th and Constitution Avenue, N.W., Washington, D.C. 20230. An appeal may also be sent by e mail to FOIAAppeals@doc.gov, or by FOIAonline, if you have an account in FOIAonline, at https://foiaonline.regulations.gov/foia/action/public/home#. The appeal should include a copy of the original request and initial denial, if any. The appeal should include a statement of the reasons why the Privacy Act request should not be denied and why the adverse determination was in error.

The appeal letter, the envelope, and the e mail subject line, should be clearly marked "Privacy Act Appeal." The e mail, FOIAonline, and Office are monitored only on working days during normal business hours (8:30 a.m. to 5:00 p.m., Eastern Time, Monday through Friday). Appeals posted to the e mail box, FOIAonline, or Office after normal business hours will be deemed received on the next normal business day. If the 90th calendar day for submitting an appeal falls on a Saturday, Sunday or legal public holiday, an appeal received by 5:00 p.m., Eastern Time, the next business day will be deemed timely.

If you have any questions concerning this response, please call (301) 628 5658.

Sincerely,

Mark Graff

NOAA FOIA Officer/Bureau Chief Privacy Officer

From: Cathy Readinger <cathyreadinger@gmail.com>
To: leann@bosargeboats.com
Cc: Roy Crabtree <roy.crabtree@noaa.gov>; Greg.Stunz@tamucc.edu; rshipp@southalabama.edu; pbanks@wlf.la.gov; phil.dyskow@gmail.com; robin.riechers@tpwd.texas.gov;edswindell@aol.com; frazer@ufl.edu; Douglass Boyd <douglassboyd@yahoo.com>; john@blaylockoil.com; Kevin Anson <kevin.anson@dcnr.alabama.gov>; Johnny Greene <fishorangebeach@gmail.com>; saltwaterlife@live.com; martha.guyas@myfwc.com; cematens@yahoo.com; paul.mickle@dmr.ms.gov; Chris.W.Oliver@noaa.gov; "Krishnan, Vishant" <vkrishnan@oig.doc.gov>; mMcClelland@doc.gov; "Guenther, John (Federal)" <JGuenther@doc.gov>; bDiGiaco@doc.gov
Sent: Tuesday, September 26, 2017 11:48 AM
Subject: Information Request

I am requesting the following:

1) Copy of Cathy Readinger's personnel file from October 27, 1982 to present in its entirety, including documents that are retained in separate employee files;
2) Copy of Cathy Readinger's time and attendance records for the 24-month period preceding March 8, 2016;
3) Copy of Cathy Readinger's time and attendance records from March 8, 2016 through June 27, 2017;
4) Listing of administrative hours provided to Council staff from March 8, 2016 through June 27, 2017;
5) Confirmation from the Council's contracted Information Technology Company regarding the date of termination of service from their inventory for the MacBrook Pro laptop identified as "Infinity Number 6085" and the last date the machine was remotely accessed;
6) Copy of all relative invoices and checks that were issued after 8:00 a.m. March 8, 2016 that bore Cathy Readinger's signature;
7) Written confirmation from employee Beth Hager regarding any and all directives given to her by the Executive Director or Deputy Director to monitor Cathy Readinger's emails, including the initial date the directive was given and written confirmation of any directive to monitor any other employee emails;
8) Confirmation from the Executive Director as to the specific PII that was used to conduct an unauthorized investigation of Cathy Readinger prior to or after her termination;
9) A copy of the Gulf Council's written disciplinarian policy relative to violations of the US Department of Commerce's Fishery Management Councils Rules Of Conduct For Employees and Advisors 2016; and
10) A copy of the Gulf Council's policy regarding use and safeguards relative to its employees' PII, including disciplinarian action for violation of such policy.

Through the Freedom of Information Act, I am requesting the following:

1) Copy of the email threads exchanged between Executive Director, Doug Gregory, and the former Public Information Officer, Charlene Ponce, relative to employee Emily Muehlsteins' 2015/2016 performance evaluation whereby the Executive Director's ratings of her major elements were "2", and the specific remedial action(s) that were taken. A copy of the final performance evaluation, and the remedial action that was taken.
2) The specific disciplinarian action that was taken relative to a Council employee who was detained by TSA for possessing a firearm when attempting to clear security at Tampa International Airport en route to a meeting of the Council.
3) A copy of the summary minutes including the date of the meeting and names or participants of the Pension Plan Trustees regarding approval of changes made to the Council's 401K retirement plan for staff in 2016. Copies of the approval page(s) of the revised document including the Summary of Material Modifications and other signature pages.
4) A list of amounts of bonuses and merit pays that were issued to staff in 2016.
5) A copy of the file that lists historical staff raises including bonuses and merit pay.
6) A list of employees and amounts of any IRS Section 415 retirement annual additions issued to staff in 2016.
7) A listing of files, including dates and times of creation, that were archived on the Gulf Council's terabyte drive that was surrendered by Cathy Readinger to employee Beth Hager and witnessed by employee Bernadine Roy on March 22, 2016. The files include documents on the terabyte drive that were created by employee Beth Hager for work performed by her as a contractor for another employer, during Council working

hours. The files also contain names, addresses, social security numbers, and other PII of contractors and employees of the employer.

8) Copy of the DOC/NOAA's written approval of the Council's Administrative Handbook; and

9) A copy of email exchanges between Doug Gregory and former Council member Harolyn Kay Williams from the date Doug Gregory's Council email was activated in 2013 until the present date. The emails requested are to be retrieved from the Council's permanent email message archiver since Council employees are allowed to delete emails from their local computers.

10) A copy of email exchanges between Doug Gregory and Dennis O'Hern, Executive Director of Fishing Rights Alliance, from the date Doug Gregory's Council email was activated in 2013 until the present date. The emails requested are to be retrieved from the Council's permanent email message archiver since Council employees are allowed to delete emails from their local computers.

11) A listing of email exchanges between Doug Gregory and Carrie Simmons from the date Doug Gregory's Council email was activated in 2013 until the present date. The emails requested are to be retrieved from the Council's permanent email message archiver since Council employees are allowed to delete emails from their local computers.

12) A listing of email exchanges between Doug Gregory and Beth Hager from the date Doug Gregory's Council email was activated in 2013 until the present date. The emails requested are to be retrieved from the Council's permanent email message archiver since Council employees are allowed to delete emails from their local computers.

13) A copy of email exchanges between Doug Gregory and Charlotte Schiaffo from the date Doug Gregory's Council email was activated in 2013 until the present date. The emails requested are to be retrieved from the Council's permanent email message archiver since Council employees are allowed to delete emails from their local computers.

14) A copy of email exchanges between Charlotte Schiaffo and Karen Hoak from the date the Council announced the selection of Doug Gregory as Executive until the present date. The emails requested are to be retrieved from the Council's permanent email message archiver since Council employees are allowed to delete emails from their local computers.

15) A list of emails from the date of activation in 2013 of the Council email account of the Executive Director, Doug Gregory, that were deleted by the Executive Director through June 27, 2017. The list of deleted emails is to include emails on his local computers in comparison with emails on the Council's permanent email message archiver as certified by the Council's contracted Information Technology Company.

16) Copy of Federal salary surveys that were conducted as justification for each staff salary increase exceeding 3.0% for any staff member as required by 50 CFR CFR 600.120(b) for the period June 16, 2013 through July 31, 2017.

17) A list by year, by staff, and amounts of staff who received tuition reimbursements from January 1, 2006 through July 31, 2017.

18) The name of the authorized Council representative who rescinded the Gulf Council's settlement agreement offered to Cathy Readinger as outlined in emails from DOC attorney John Guenther.

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, December 11, 2017 3:18 PM
To:	CPO; Brown, Christian (Contractor)
Cc:	Rob Swisher; Mark Graff NOAA Federal
Subject:	Re NOAA4920 docs for 12 14 17 CRB
Attachments:	NOAA4920_PTA_20171211 for BCP signature Signed RS.pdf; NOAA4920_PI_FedFish_Application_04Dec17 _with PA statement.pdf; NOAA4920 PIA_121117 for BCP signature Signed RS.pdf

Here are the NOAA4920 PIA and PTA and the Privacy Act Statement for the permits site.

I will send the SAR and SAR workbook via Accellion; they are also in CSAM in the artifacts for this system.

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

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

Version Number: 01-2015

U.S. Department of Commerce
NOAA NMFS

Privacy Impact Assessment
for the
Pacific Islands Regional Office (PIRO)
Local Area Network
NOAA4920

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
PIRO LAN – NOAA4920

Unique Project Identifier: 006-48-01-14-02-3305-00

Introduction: System Description

The NOAA Fisheries Pacific Islands Regional Office (PIRO) Local Area Network (LAN) functions as the overall General Support System (GSS) for PIRO located in Honolulu, Hawaii. Additional remote sites exist in Samoa, Guam and Saipan. The information system is used to provide administrative support typically found in administrative offices within the federal government as well as supplemental operational services.

PIRO consists of the following divisional units:

- PIR Regional Administrators Office
- NOAA Office of General Counsel
- PIR Habitat Conservation Division
- PIR International Fisheries Division
- PIR Observer Program
- PIR Office of Management and Information
- PIR Protected Resources Division
- PIR Sustainable Fisheries Division

The categories of data collected, stored and disseminated include administrative, human resources, operations, statistical, economic, and technical.

NOAAA4920 is located at the following locations: Honolulu, HI, American Samoa, the Commonwealth of the Northern Mariana Islands, and Guam. **There is information stored onsite at the Saipan location on a full disk FIPS encrypted laptop and hardware FIPS encrypted removable drive. The location is not directly connected to NOAA 4920; they connect directly to the internet via a DSL connection. The single user located in Saipan connects to the secure NOAA4920 VPN to access NOAA/DOC corporate services and NOAA4920 applications/data. If sensitive PII/BII is transmitted the user is aware to use Accellion.**

The primary functions of the NOAA4920 information system are:

- File and printer sharing
- Web applications and database services
- Access to NOAA/DOC web services via wide area network connections

· Pacific region fisheries permit data repository

No major application systems are supported on NOAA4920.

Information collected within the system includes employee personnel data: names, phone numbers, and addresses to support contact rosters, access to facilities, stored official documents such as travel documents, performance plans, etc. by the employees supervisors and the pay pool manger, and 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.

Additional information collected: Federal civil servants and private contractors working for the Fisheries Service, and volunteers working on behalf of PIRO access parts of the system in support of job requirements and mission objectives. Volunteers do not have access to PII/BII on the information system. Supervisors collect and maintain information from visitors and foreign nationals for permission to access federal facilities. Government Passports are required for international travelers, which may include staff, members of the public and foreign visitors.

Finally, the permit data repository consists of contents of permit applications and related documents, such as permit holder name, date of birth or incorporation, Taxpayer Identification Number (TIN), business contact information. The application is downloaded from the PIRO website or obtained from a PIRO office, submitted it to a PIRO office by mail or hand delivery, along with any required supporting documentation and non-refundable application processing fee payment. The National Permit System supports online submission and fee payment (through a link to pay.gov) of permit applications and related information, via secure Web pages. After PIRO reviews and approves the online submission, PIRO issues the permit to the applicant.

Information Sharing:
With regards to the transmission of human resource related data, staff utilize the U.S. Department of Commerce (Department) Accellion Secure File Transfer service. Human resource data and Federal purchaser credit card information is sent to NOAA Human Resources Workforce Division. Human resources staff at PIRO (within NOAA4920) transmit PII (credentials only) to the Army to facilitate access to the NOAA Inouye Regional Center (IRC), using the Army's secured AMRDEC SAFE (Safe Access File Exchange).

Information may be shared within the bureau, with DOC bureaus and other Federal agencies in case of breach.

NOAA4920 shares BII and PII with the following independent, private, state and/or foreign entities:

<u>Regional Fisheries Management Organizations:</u>

At the state or interstate level within the applicable Marine Fisheries Commission for the purpose of co-managing a fishery or for making determinations about eligibility for permits when state data are all or part of the basis for the permits.

Additionally, permit-related information may also be disclosed to the applicable Pacific region or international fisheries management body for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by a regional or international fisheries management body, such as:

- At the Pacific region level within the applicable Marine Fisheries Commission for the purpose of co-managing a fishery or for making determinations about eligibility for permits when Pacific region data are all or part of the basis for the permits, such as: The Western and Central Pacific Fisheries Commission, the South Pacific Regional Fisheries Commission; regional fisheries organizations such as the International Scientific Committee for Tuna and Tuna-like Species in the North Pacific Ocean; and regional intergovernmental organizations such as the Secretariat of the Pacific Community, the Pacific Islands Forum Fisheries Agency, and the Parties to the Nauru Agreement. At the applicable international level within the applicable fisheries management body for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by an international fisheries management body, such as: The Food and Agriculture Organization of the United Nations, Commission for the Conservation of Antarctic Marine Living Resources, Inter-American Tropical Tuna Commission, International Pacific Halibut Commission, and International Commission for the Conservation of Atlantic Tunas.
- To foreign governments with whose regulations U.S. fishermen must comply.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the Department. These records or information contained therein may specifically be disclosed as a routine use as stated below. The Department will, when so authorized, make the determination as to the relevancy of a record prior to its decision to disclose a document. These routine uses are listed in the System of Records Notices (SORNs) COMMERCE/NOAA-6, Fishermen's Statistical Data, and COMMERCE/NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries.

Sources of information include the permit applicant/holder, other NMFS offices, the U.S. Coast Guard, and State or Regional Marine Fisheries Commissions.

5 U.S.C. § 301 authorizes the operations of an executive agency including the creation, custodianship, maintenance and distribution of records.

From NOAA-19: Applications for permits and registrations are collected from individuals under

the authority of the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C 1801 et. seq., the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Western and Central Pacific Fisheries Convention Implementation Act (WCPFCIA; 16 U.S.C. 6901 et seq), The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.

From NOAA-6: Fish and Wildlife Act as amended (16 U.S.C. 742 et seq.). Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C 1801 et. seq.

From DEPT-1: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309.

From DEPT-6: 5 U.S.C. 301; 44 U.S.C. 3101.

From DEPT-9: Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

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.

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.

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 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*.

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 without changes that 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	X	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): Captain's license, State and Federal Dealer Numbers (if applicable), permit or license numbers for Federal or state permit/licenses issued and start and end dates and other permit status codes, vessel registration number					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: SSNs are collected as part of human resources-related documents. There is currently an outstanding litigation hold requiring NOAA offices to retain documents and other information and evidence, including "*all records and other information in NOAA's possession, custody or control related to promotions, lateral transfers, employment enhancing assignments, performance ratings, bonuses, cash awards, and quality step increases from January 1, 2007 to the present.*" (Source: Janet Howard v. U.S. Department of Commerce, Agency Case No. 08-67-00082 (NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION OPEN LITIGATION HOLDS), (Jun. 29, 2015). In addition, as stated in COMMERCE/NOAA-19, a Taxpayer ID is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a Federal agency including, but not limited to, if the person is an applicant for, or recipient of, a Federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c) (2) (B) of this statute. ** Taxpayer ID is collected on vessel permit applications: may be either EIN or SSN.					

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	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	
s. Other general personal data (specify): Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, spouse, former spouse, decedent.					

*These are government purchase cards only

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	X		
i. Other work-related data (specify): Vessel name, vessel length overall. Name of corporation, state and date of incorporation of business and articles of incorporation. For federal employees, pay plan, occupational code, grade/level and state/rate for personnel actions.					

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

*These are recorded on a stand-along station and retained only until receipt is confirmed by OSY.

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	X
g. Other system administration/audit data (specify):					

h. **Other Information (specify)** Species, aggregate catch data and statistics, quota share balance, quota pound balance, quota pound limits, listings of endorsements and designations (i.e., gear endorsement, size endorsement, sector endorsement, permit tier) associated with the permit, name of physical IFQ landing site, Exemptions (i.e., Owner on Board - Grandfathered Exemption, Owner on Board, as stated in code of federal regulations) and exemption status, contact persons, Catch/Observer Discard Data, Quota Share/Quota Pound Transfer Data, Business Operation Information (Business Processes, Procedures, Physical Maps).

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: X Mail/Fax	X	Online	X
Telephone	X*	Email	X		
Other (specify):					

*If someone needs a base pass we have them call us and provide the information because sometimes they can't email it to us securely.

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
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) buidls	
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.

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	X
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)	X	For web measurement and customization technologies (multi-session)	
Other (specify): (litigation above refers to the litigation hold), determination of qualification for fisheries permits.			

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).

PII/BII is used in a variety of ways, many of which are unique to each individual division as determined by the division chief in accordance with record management, functional, operational or litigation requirements. The information collected and how it is used is broken down by each division.

Information collected from federal employees and contractors

PII is collected for the purposes of hiring and conducting performance reviews.

PII is collected from employees and contractors: for emergency management communication and safety (Continuity of Operations Plan (COOP)).

PII is collected for both contractor and federal employee personnel designated to work with PIRO. This is information collected for several administration and business functions for the PIRO including organizational charts, integrated resource planning and outage notification/escalation, purchasing and tracking of Travel Cards, tracking of training, and litigation holds.

A copy of each employee's forms submitted to PIRO is stored in a personnel folder on the network. This includes background checks, Employee Address CD-525, Declaration for Federal Employment OF-306, Health Benefits Election Form OPM SF-2809, Direct Deposit Sign-Up Form SF-1199A, Designation of Beneficiary SF-1152, Self-Identification of Handicap SF-256, Designation of Beneficiary - FERS SF-3102, Statement of Prior Service SF-144, Instructions for Employment Eligibility Verification Form I-9 (with copies of identification), and employee benefits. T*hese are duplicates of forms in WFMO. The ISSO will aggressively pursue the removal of these documents from NOAA4920 during the AO briefing.*

Contract managers collect and maintain information from contractors at the time of service to coordinate work orders and to communicate the needs of the agency.

Supervisors collect and maintain employees' information from doctors during extended sick leave to validate legitimacy of absence. Individuals requesting reasonable accommodation also provide medical information that supervisors maintain to process reasonable accommodation requests.

GDP and IN: Supervisors collect and maintain information from visitors, volunteers and foreign nationals during passport application and for permission to access federal facilities. See NAO 207-12 (http://www.corporateservices.noaa.gov/ames/administrative_orders/chapter_207/207-12.html)

Permitting

The Protected Species Workshop Coordinator collects name, vessel name, mailing address and phone number from vessel owners and operators to register for Hawaii longline protected species training.
Fisheries permit related BII (Vessel Name, Vessel Operator, Vessel Identifier, Fishing Locations, Catch Information, Observer Incidents, and Observer Post Cruise Log data are covered under Non-Disclosure Agreements and Magnuson/Stevens. Permit related information is stored, depending on the related fishery, either in the Permit application database covered under the NOAA4000 PIA or in the PIRO Permit application Database, both of which are covered under the System of Records Notice (SORN) Commerce/NOAA-19, *Permits and Registrations for United States Federally Regulated Fisheries.*

This information is maintained locally within PIRO and is used primarily for regulatory and administrative purposes. This information may be shared with other agencies as listed in the Introduction, having a legitimate business need and authorization. All information collected is extracted from paper records supplied by the individual or derived from other sources listed in the Introduction, scanned to the network and stored in a shared file.

Public
The Division may collect and maintain name, address, email address, and phone number from the public for comments on proposed actions, published in the Federal Register. This information is entered into regs.gov. The ISSO has suggested that we do not need to maintain the information; there is no such requirement related to regs.gov.

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.)*

	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	X		
Public			
Private sector			
Foreign governments			
Foreign entities	X	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.

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: NOAA4920 maintains a Microsoft Active Directory Domain, providing authentication and authorization services for employees. The system is not available publicly and remote sites are connected via secure encrypted VPN links. NOAA4920 interconnects for network transit purposes with NOAA1200, National Oceanic and Atmospheric Administration Corporate Services Local Area Network. PIRO has a dedicated WAN link to NOAA4000 to facilitate data interconnection between other systems within the bureau. Any PII/BII transmitted outside the system is done so using Accellion Secure File Transfer.
	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.fpir.noaa.gov/Library/SFD/PI_FedFish_Application_NoEx_Fillable_02Feb15.pdf (this is the Federal Fisheries Permit Application).	
X	Yes, notice is provided by other means.	Specify how: System Wide: Authorized users of NOAA4920 information technology systems are notified both in the NOAA rules of behavior and system usage consent warning banner that there is no expectation of privacy while using these systems which includes SAAD and directly associated WRD, and GPD information. Unauthorized users have no reasonable expectation of notification. Employees' performance reviews are uploaded to their electronic Official Personnel File (eOPF), which is accessible to all Federal employees. Upon hire, all employees are informed about their eOPF and how to access it during their onboarding process. Also, EOPF notifies employees when a document has been uploaded.

		Supervisors are required to ask for supporting documents when there is a lengthy sick leave request documentation that is tied to the sick leave request made by the employee through WebTA. The DOC Web TA sick leave request includes a Privacy Act Statement. For personnel management data, all employee, general public and contractor PII is collected directly from the individual through personal contact, by phone, email or mail. Potential employee PII is willingly provided to the division during the application process. All federal forms have Privacy Act Notices. Permit holders: Notice is given on permit applications.
	No, notice is not provided.	

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 personnel actions, individuals may decline to provide PII, in writing, to their supervisor or to the Human Resources Office; however, their employment status may be affected. Individuals may decline to provide emergency contact notification to their supervisors, in writing; however, their employment status may be affected. Permit applicants: The personal information is collected when the individual completes the appropriate application. On the application, the individual is advised that NMFS will not be able to issue a permit if the individual does not provide each item of information requested. The individual may choose to decline to provide the required personal information at that time, by not completing the application, but will not be able to receive a permit.
	No, individuals do not have an opportunity to decline to provide 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: System Wide: By supplying the PII/BII, the individual/entity consents to the use of the information for one particular use only (each type of information collection has a specific purpose). An employee that does not consent to use of PII/BII for user credentials would be unable to access the system, and if not consenting to the use of their PII for COOP, their employment might be affected. Permit applicants and holders: Permittees are provided with the

		link to NOAA's privacy policy where it states: "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose."
	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: Supervisors review individuals' PII occasionally to ensure that the emergency contact list is accurate. Employees may review PII in their eOPF file at any time. Employees can also review and update their information on the intranet page. Employees are also made aware via annual data calls that their personal contact information will be maintained as an emergency contact list/COOP plan. The HR personnel folders containing scans of federal employee application forms is restricted to only HR and management personnel with need to know. The information can be updated on request to HR. Permit applicants and holders: Information may be reviewed or updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time (information is on permits and permit applications).
	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: NOAA4920 uses centralized logging which can log and alert when sensitive files and folders are accessed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 1/9/2017 ☐ 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.

Identification and authentication (multifactor, CAC) before accessing PII Access control to PII through access control lists Separation of duties involving access to PII Enforcement of least privilege File system auditing, review, analysis and reporting Encryption of removable media, laptops and mobile devices Labeling of digital media to secure handling and distribution Sanitization of digital and non-digital media containing PII Use of encryption to securely transmit PII

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-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons. DEPT-6, Visitor Logs and Permits for Facilities Under Department Control DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons DEPT-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. COMMERCE/NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries COMMERCE/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: NOAA Records Schedules: Chapter 100 – General Chapter 200-Adminstrative and Housekeeping Records Chapter 300 - Personnel Chapter 400 – Finance Chapter 500 – Legal Chapter 600– International Chapter 900-Facilities Security and Safety Chapter 1200 – Scientific Research Chapter 1500 – Marine Fisheries
	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.

	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 with the

		information stored in the system.
X	Quantity of PII	Provide explanation: Total quantity of information is minimal and primarily pertains to local Federal employees and contractors.
X	Data Field Sensitivity	Provide explanation: There is sensitive PII for employees and fishermen, and sensitive BII for fishermen.
X	Context of Use	Provide explanation: Permits information and employee/contractor information is stored securely as described in Sections 8.1 and 8.2.
X	Obligation to Protect Confidentiality	Provide explanation: The Magnuson-Stevens Act authorizes confidentiality of fisheries data. The Health Insurance Portability and Accountability Act protects medical information received in relation to a prolonged illness or self-designation of disability, if applicable.
X	Access to and Location of PII	Provide explanation: System is not publicly accessible.
	Other:	Provide explanation:

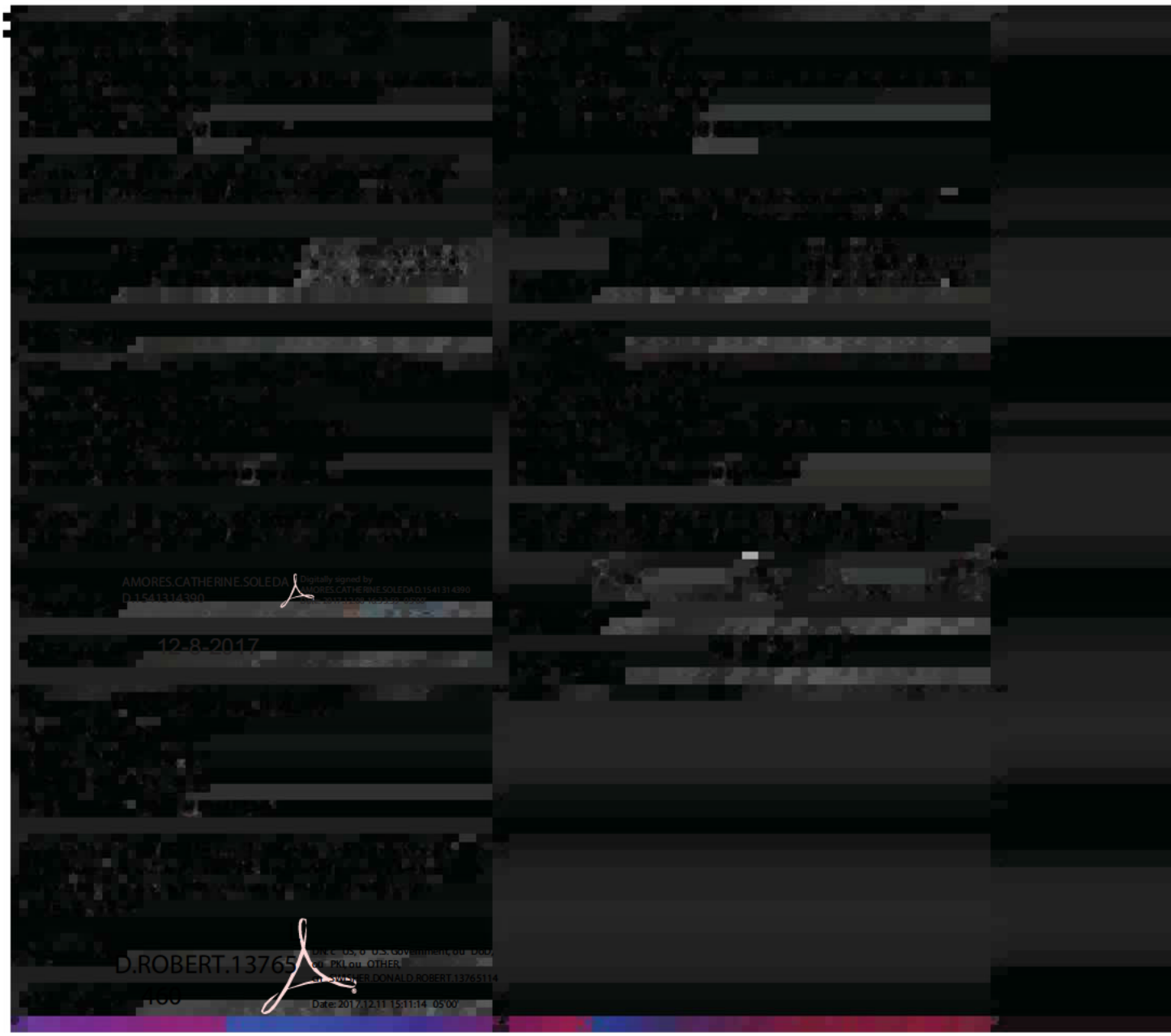
Section 12: Analysis

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: The findings indicate cases where PII is being collected without a bona fide mission/operational requirement. Personnel who work with PII/BII must examine processes and determine if reduction, sanitization or elimination of unneeded PII can be performed. Changes in business processes are administrative and will need to be reviewed and modified through management. (from last PIA but still pending) The ISSO will advocate to remove the duplicate HR forms and to delete public comments once entered into regs.gov.
	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: Based on the amount of sensitive PII in the system, additional technological controls need to be implemented. Repositories need to be defined and secured with encrypted file services. Network protocols for transmittal of sensitive information inside the LAN need to be encrypted. Perimeter and software solutions shall identify PII/BII in transit or in use without authorization. (from last PIA but still pending)
	No, the conduct of this PIA does not result in any required technology changes.


AMORES.CATHERINE.SOLEDAD.1541314390
Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390
12-8-2017
D.ROBERT.13765
Date: 2017.12.11 15:11:14 -05'00'

U.S. DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
NATIONAL MARINE FISHERIES SERVICE
Pacific Islands Regional Office SFD Permits
1845 Wasp Blvd., Bldg 176
Honolulu, Hawaii 96818
(808) 725 5000 • Fax: (808) 725 5215

OMB Control No: 0648-0490
Expires: 01/31/2018

PACIFIC ISLANDS FEDERAL FISHERIES PERMIT APPLICATION

PERMIT TYPE (Submit a separate application for each permit)

1. **PELAGIC:**
   - ☐ **Hawaii Longline Limited Entry Permit** – Renewal or Transfer (**$52.00** Non-refundable Application Processing Fee for Hawaii longline permit only. Make checks or money orders payable to: **Department of Commerce, NOAA**)
     For **Hawaii Closed Area Exemption** (contact Pacific Islands Region for form)
   - ☐ **Western Pacific General Longline Permit** (Guam, Northern Mariana Islands, PRIA) (No Fee)
   - ☐ **Western Pacific Receiving Vessel Permit** (all areas) (No Fee)
   - ☐ **Pacific Remote Island Areas Troll & Handline** (No Fee)

LOBSTER and DEEPWATER SHRIMP (Use the Western Pacific Crustacean Permit application form, OMB Control No. 0648-0586)

2. **BOTTOMFISH:** ☐ **Guam (large vessel)** ☐ **Pacific Remote Island Areas** (No Fee)
   (CNMI: Use the Northern Mariana Islands Bottomfish Permit application form, OMB Control No. 0648-0584)

3. **PRECIOUS CORAL:** ☐ (No Fee) **Permit Area (see instructions):**

Please Print Legibly. All Fields Required. Note required documents in instructions on side two.

VESSEL NAME: **VESSEL OFFICIAL NO:**

VESSEL OWNER(s): **RADIO CALL SIGN:**
First, Middle, & Last Name or Business Name

PERMIT HOLDER(s):
First, Middle, & Last Name or Name of Business to be designated Permit Holder **Taxpayer ID Number** (SSN or EIN)

DATE OF BIRTH (Individual) **OR INCORPORATION** (Business) **OF PERMIT HOLDER:**

BUSINESS CONTACT: **TITLE:**
First, Middle, & Last Name, if not same as permit holder Corporate officer, business owner, partner

BUSINESS MAILING ADDRESS:
Street/PO Box City State ZIP Code

BUSINESS PHONE ( ) **CELL** ( )

EMAIL:

Under penalty of perjury, I hereby declare that I, the undersigned, am the applicant or authorized to complete and certify this application on behalf of the applicant, and the information contained herein is true, correct, and complete to the best of my knowledge.

APPLICANT: **DATE:**
Printed Name and **Signature** of Permit Holder, Corporate Officer, Partner, or Designated Agent

APPLICANT TITLE: ◯ Permit holder; ◯ Corporate member or officer, or partner; ◯ Designated agent; or ◯ Other
(Check only one)

***For Hawaii Longline Permit Transfer:* to be completed and signed by originating permit holder (transferer).** Under penalty of perjury, I hereby declare that I, the undersigned, am the current permit holder or authorized to complete and certify this application on behalf of the current permit holder, and the information contained herein is true, correct, and complete to the best of my knowledge.

PERMIT TRANSFERER: **DATE:**
Printed Name & Signature of Permit Holder Transferring Permit

Permit Number to be Transferred:

OMB Control No. 0648-0490
Expires: 01/31/2018

Instructions for the Pacific Islands Federal Fisheries Permit Application:

Permit Type: Check which permit you are applying for. Note: for the Hawaii longline permit, only renewal or transfer is allowed. A non-refundable application processing fee is required only for the Hawaii longline permit.

Permit Area (for Precious Coral)**:** X-P-AS (American Samoa Exploratory Area), E-B-1 (Makapu'u Established Bed, Hawaii), E-B-2 (Au'au Channel Established Bed, HI), C-B-1 (Keahole Pt. Conditional Bed, HI), C-B-2 (Kaena Pt. Conditional Bed, HI), X-P-H (Hawaii Exploratory Area – all other HI areas except NWHI), X-P-G (Guam Exploratory Area), and X-P-CNMI (Northern Marianas Exploratory Area). See regulations at 50 CFR 665 for details.

Vessel Information: Fill in the vessel name, official number (USCG documented vessel number or registered number for undocumented vessels), radio call sign, and name of vessel owner. If the vessel has no name, please draw a line in the vessel name field. Registration of a new or replacement vessel to the Hawaii longline permit is a transfer.

Permit Holder Information: Fill in the name of the person(s) or business(es) to whom the permit will be issued. The permit will be issued to this permit holder. Provide the taxpayer ID number: SSN for individual, or EIN for a business. Fill in the date of birth of the individual or the date of incorporation for the business. Any change in the name of the permit holder for a Hawaii longline permit is a transfer.

Fill in the name of the person who will be the main contact for the permit holder, if not the same person as the permit holder, or if the permit holder is a business. Provide the mailing address, phone numbers, and email of the permit holder. This will be the address of record.

Applicant: The person who submits the application must print their name and sign the form. Fill in application date and applicant title. If the applicant is not the permit holder or is not a member or officer of the business that holds the permit, the permit holder must provide a signed letter of authorization designating the applicant as the agent.

For Hawaii Longline Permit Transfers: This section must be completed by the current permit holder who is transferring the permit (transferer) to another person or business (transferee). The current permit holder(s) must write their name, their signature, and date it. The permit number being transferred must be provided. If there is more than one permit holder, all permit holders must confirm the transfer. NMFS may request additional documentation to verify the transfer.

Required Documents to provide with the application:
1) a copy of the vessel's current U.S. Coast Guard Certificate of Documentation (documented vessel) or registration certificate from a state/territorial agency (undocumented vessel) showing current vessel owner,
2) payment for the processing fee, if required, and
3) if the applicant is a designated agent, attach a signed letter from the permit holder authorizing the applicant as the agent.

The person or officer or member of the business who owns the vessel must have a current Protected Species Workshop (PSW) certificate to renew the Hawaii longline permit. Contact piropsw@noaa.gov for workshop information.

Submit Complete Application to: The address printed in the upper left corner of the first page or at the NMFS Honolulu Service Center, Pier 38, Honolulu, HI 96817 (M-F, 8 am – 4 pm). Contact the Permits Program at piro-permits@noaa.gov for information on online renewals of Hawaii longline permits, and other permits as available.

An application that is lacking required information, vessel registration or documentation, or payment will be considered incomplete. An incomplete application will be abandoned if it is not completed within 30 days after reception (50 CFR 665.13). You must inform PIRO within 15 days of any change of information on the application form (50 CFR 665.13). It is prohibited to file false information on any application for a fishing permit (50 CFR 665.15(b)).

PRIVACY ACT STATEMENT

Authority: The collection of this information is authorized under the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C 1801 et seq., the Western and Central Pacific Fisheries Convention Implementation Act (WCPFCIA; 16 U.S.C. 6901 et seq), the Marine Mammal Protection Act, and the Endangered Species Act. The authority for the mandatory collection of the Tax Identification Number (TIN) is 31 U.S.C. 7701.

Purpose: In order to manage U.S. fisheries, the NOAA National Marine Fisheries Service (NMFS) requires the use of permits or registrations by participants in the United States. Information on NOAA Fisheries permit applicants and renewing holders includes vessel owner contact information, date of birth, TIN and vessel descriptive information. Permit holder information may be used as sampling frames for surveys.

Routine Uses: The Department will use this information to determine permit eligibility and to identify fishery participants. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)**, to be shared within NMFS offices, in order to coordinate monitoring and management of sustainability of fisheries and protected resources, as well as with the applicable State or Regional Marine Fisheries Commissions and International Organizations. 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/NOAA-19, Permits and Registrations for the United States Federally Regulated Fisheries.

Disclosure: Furnishing this information is voluntary; however, failure to provide complete and accurate information will prevent the determination of eligibility for a permit.

PAPERWORK REDUCTION ACT INFORMATION

Public reporting burden for this collection is estimated as follows: 30 minutes for Hawaii longline limited access permit renewal/transfer, WP general longline permits and receiving vessel permits; 30 minutes for Guam bottomfish large vessel permits; 30 minutes for precious coral permits (established, conditional, refugia, exploratory areas), Pacific remote island areas (PRIA) troll and handline and bottomfish permits; and 2 hours for all permit denial appeals. Each burden includes time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspects of this collection of information, including suggestions for reducing this burden, to NMFS Pacific Islands Regional Administrator, 1845 Wasp Blvd., Bldg. 176, Honolulu, Hawaii 96818.

This information is being collected to ensure accurate and timely records about the persons licensed to participate in fisheries under Federal regulations in the Pacific Islands Region. This will enable NOAA Fisheries Service and the Western Pacific Fishery Management Council to (a) determine who would be affected by changes in management; (b) inform license holders of changes in fishery regulations; and (c) determine whether the objectives of the fishery program are being achieved by monitoring entry and exit patterns and other aspects of the fisheries. The information is used in analyzing and evaluating the potential impacts of regulatory changes on persons in the regulated fisheries as well as in related fisheries. Responses to the collection are required to obtain the benefit of a permit for the fishery involved (ref. 50 CFR 665.13). Data provided concerning the proprietary business of the respondents are handled as confidential under the Magnuson-Stevens Fishery Conservation and Management Act (Sec. 402(b)). Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Version Number: 01-2015

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

Privacy Threshold Analysis
for the
NOAA4920 – Pacific Islands Region Office (PIRO)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA – PIRO LAN

Unique Project Identifier: 006-48-01-14-02-3305-00

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 NOAA Fisheries Pacific Islands Regional Office (PIRO) Local Area Network (LAN) functions as the overall General Support System (GSS) for PIRO located in Honolulu, Hawaii. Additional remote sites exist in Samoa, Guam and Saipan. The information system provides administrative support typically found in administrative offices within the federal government as well as supplemental operational services.

PIRO consists of the following divisional units:

- PIR Regional Administrators Office
- NOAA Office of General Counsel
- PIR Habitat Conservation Division
- PIR International Fisheries Division
- PIR Observer Program
- PIR Office of Management and Information
- PIR Protected Resources Division
- PIR Sustainable Fisheries Division

The categories of data collected, stored and disseminated include administrative, human resources, operations, statistical, economic, and technical.

NOAA4920 is located at the following locations: Honolulu, HI, American Samoa, the Commonwealth of the Northern Mariana Islands, and Guam. The primary functions of the NOAA4920 information system are:

- File and printer sharing
- Web applications and database services
- Access to NOAA/DOC web services via wide area network connections
- Pacific region fisheries permit data repository

No major application systems exist within NOAA4920.

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.)."

___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.

AMORES.CATHERINE.SOLEDAD.1

Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390

SWISHER.DONALD.ROBERT.1376511460

Digitally signed by SWISHER.DONALD.ROBERT.1376511460
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SWISHER.DONALD.ROBERT.1376511460
Date: 2017.12.11 14:17:14 -05'00'

Purvis, Catrina (Federal)

Subject:	CRB meeting NOAA4920
Location:	Open Office 52017 (SMC) Md Conf R (b)(6) [redacted]
Start:	Thursday, December 14, 2017 2:00 PM
End:	Thursday, December 14, 2017 2:30 PM
Recurrence:	(none)
Meeting Status:	Not yet responsed
Organizer:	Purvis, Catrina (Federal)
Attachments:	NOAA4920 PIA_121117 for BCP signature Signed RS.pdf; NOAA4920_PTA_20171211 for BCP signature Signed RS.pdf

Mark/Sarah

Please provide the signed PIA/PTA for the system identified above by COB Monday, December 11.

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 NMFS

Privacy Impact Assessment
for the
Pacific Islands Regional Office (PIRO)
Local Area Network
NOAA4920

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
PIRO LAN – NOAA4920

Unique Project Identifier: 006-48-01-14-02-3305-00

Introduction: System Description

The NOAA Fisheries Pacific Islands Regional Office (PIRO) Local Area Network (LAN) functions as the overall General Support System (GSS) for PIRO located in Honolulu, Hawaii. Additional remote sites exist in Samoa, Guam and Saipan. The information system is used to provide administrative support typically found in administrative offices within the federal government as well as supplemental operational services.

PIRO consists of the following divisional units:

- PIR Regional Administrators Office
- NOAA Office of General Counsel
- PIR Habitat Conservation Division
- PIR International Fisheries Division
- PIR Observer Program
- PIR Office of Management and Information
- PIR Protected Resources Division
- PIR Sustainable Fisheries Division

The categories of data collected, stored and disseminated include administrative, human resources, operations, statistical, economic, and technical.

NOAAA4920 is located at the following locations: Honolulu, HI, American Samoa, the Commonwealth of the Northern Mariana Islands, and Guam. **There is information stored onsite at the Saipan location on a full disk FIPS encrypted laptop and hardware FIPS encrypted removable drive. The location is not directly connected to NOAA 4920; they connect directly to the internet via a DSL connection. The single user located in Saipan connects to the secure NOAA4920 VPN to access NOAA/DOC corporate services and NOAA4920 applications/data. If sensitive PII/BII is transmitted the user is aware to use Accellion.**

The primary functions of the NOAA4920 information system are:

- File and printer sharing
- Web applications and database services
- Access to NOAA/DOC web services via wide area network connections

· Pacific region fisheries permit data repository

No major application systems are supported on NOAA4920.

Information collected within the system includes employee personnel data: names, phone numbers, and addresses to support contact rosters, access to facilities, stored official documents such as travel documents, performance plans, etc. by the employees supervisors and the pay pool manger, and 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.

Additional information collected: Federal civil servants and private contractors working for the Fisheries Service, and volunteers working on behalf of PIRO access parts of the system in support of job requirements and mission objectives. Volunteers do not have access to PII/BII on the information system. Supervisors collect and maintain information from visitors and foreign nationals for permission to access federal facilities. Government Passports are required for international travelers, which may include staff, members of the public and foreign visitors.

Finally, the permit data repository consists of contents of permit applications and related documents, such as permit holder name, date of birth or incorporation, Taxpayer Identification Number (TIN), business contact information. The application is downloaded from the PIRO website or obtained from a PIRO office, submitted it to a PIRO office by mail or hand delivery, along with any required supporting documentation and non-refundable application processing fee payment. The National Permit System supports online submission and fee payment (through a link to pay.gov) of permit applications and related information, via secure Web pages. After PIRO reviews and approves the online submission, PIRO issues the permit to the applicant.

Information Sharing:
With regards to the transmission of human resource related data, staff utilize the U.S. Department of Commerce (Department) Accellion Secure File Transfer service. Human resource data and Federal purchaser credit card information is sent to NOAA Human Resources Workforce Division. Human resources staff at PIRO (within NOAA4920) transmit PII (credentials only) to the Army to facilitate access to the NOAA Inouye Regional Center (IRC), using the Army's secured AMRDEC SAFE (Safe Access File Exchange).

Information may be shared within the bureau, with DOC bureaus and other Federal agencies in case of breach.

NOAA4920 shares BII and PII with the following independent, private, state and/or foreign entities:

<u>Regional Fisheries Management Organizations:</u>

At the state or interstate level within the applicable Marine Fisheries Commission for the purpose of co-managing a fishery or for making determinations about eligibility for permits when state data are all or part of the basis for the permits.

Additionally, permit-related information may also be disclosed to the applicable Pacific region or international fisheries management body for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by a regional or international fisheries management body, such as:

- At the Pacific region level within the applicable Marine Fisheries Commission for the purpose of co-managing a fishery or for making determinations about eligibility for permits when Pacific region data are all or part of the basis for the permits, such as: The Western and Central Pacific Fisheries Commission, the South Pacific Regional Fisheries Commission; regional fisheries organizations such as the International Scientific Committee for Tuna and Tuna-like Species in the North Pacific Ocean; and regional intergovernmental organizations such as the Secretariat of the Pacific Community, the Pacific Islands Forum Fisheries Agency, and the Parties to the Nauru Agreement. At the applicable international level within the applicable fisheries management body for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by an international fisheries management body, such as: The Food and Agriculture Organization of the United Nations, Commission for the Conservation of Antarctic Marine Living Resources, Inter-American Tropical Tuna Commission, International Pacific Halibut Commission, and International Commission for the Conservation of Atlantic Tunas.
- To foreign governments with whose regulations U.S. fishermen must comply.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the Department. These records or information contained therein may specifically be disclosed as a routine use as stated below. The Department will, when so authorized, make the determination as to the relevancy of a record prior to its decision to disclose a document. These routine uses are listed in the System of Records Notices (SORNs) COMMERCE/NOAA-6, Fishermen's Statistical Data, and COMMERCE/NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries.

Sources of information include the permit applicant/holder, other NMFS offices, the U.S. Coast Guard, and State or Regional Marine Fisheries Commissions.

5 U.S.C. § 301 authorizes the operations of an executive agency including the creation, custodianship, maintenance and distribution of records.

From NOAA-19: Applications for permits and registrations are collected from individuals under

the authority of the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C 1801 et. seq., the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Western and Central Pacific Fisheries Convention Implementation Act (WCPFCIA; 16 U.S.C. 6901 et seq), The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.

From NOAA-6: Fish and Wildlife Act as amended (16 U.S.C. 742 et seq.). Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C 1801 et. seq.

From DEPT-1: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309.

From DEPT-6: 5 U.S.C. 301; 44 U.S.C. 3101.

From DEPT-9: Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

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.

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.

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 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*.

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 without changes that 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	X	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): Captain's license, State and Federal Dealer Numbers (if applicable), permit or license numbers for Federal or state permit/licenses issued and start and end dates and other permit status codes, vessel registration number					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: SSNs are collected as part of human resources-related documents. There is currently an outstanding litigation hold requiring NOAA offices to retain documents and other information and evidence, including "*all records and other information in NOAA's possession, custody or control related to promotions, lateral transfers, employment enhancing assignments, performance ratings, bonuses, cash awards, and quality step increases from January 1, 2007 to the present.*" (Source: Janet Howard v. U.S. Department of Commerce, Agency Case No. 08-67-00082 (NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION OPEN LITIGATION HOLDS), (Jun. 29, 2015). In addition, as stated in COMMERCE/NOAA-19, a Taxpayer ID is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a Federal agency including, but not limited to, if the person is an applicant for, or recipient of, a Federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c) (2) (B) of this statute. ** Taxpayer ID is collected on vessel permit applications: may be either EIN or SSN.					

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	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	
s. Other general personal data (specify): Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, spouse, former spouse, decedent.					

*These are government purchase cards only

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	X		
i. Other work-related data (specify): Vessel name, vessel length overall. Name of corporation, state and date of incorporation of business and articles of incorporation. For federal employees, pay plan, occupational code, grade/level and state/rate for personnel actions.					

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

*These are recorded on a stand-along station and retained only until receipt is confirmed by OSY.

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	X
g. Other system administration/audit data (specify):					

h. **Other Information (specify)** Species, aggregate catch data and statistics, quota share balance, quota pound balance, quota pound limits, listings of endorsements and designations (i.e., gear endorsement, size endorsement, sector endorsement, permit tier) associated with the permit, name of physical IFQ landing site, Exemptions (i.e., Owner on Board - Grandfathered Exemption, Owner on Board, as stated in code of federal regulations) and exemption status, contact persons, Catch/Observer Discard Data, Quota Share/Quota Pound Transfer Data, Business Operation Information (Business Processes, Procedures, Physical Maps).

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: X Mail/Fax	X	Online	X
Telephone	X*	Email	X		
Other (specify):					

*If someone needs a base pass we have them call us and provide the information because sometimes they can't email it to us securely.

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
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) buidls	
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.

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	X
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)	X	For web measurement and customization technologies (multi-session)	
Other (specify): (litigation above refers to the litigation hold), determination of qualification for fisheries permits.			

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).

PII/BII is used in a variety of ways, many of which are unique to each individual division as determined by the division chief in accordance with record management, functional, operational or litigation requirements. The information collected and how it is used is broken down by each division.

Information collected from federal employees and contractors

PII is collected for the purposes of hiring and conducting performance reviews.

PII is collected from employees and contractors: for emergency management communication and safety (Continuity of Operations Plan (COOP)).

PII is collected for both contractor and federal employee personnel designated to work with PIRO. This is information collected for several administration and business functions for the PIRO including organizational charts, integrated resource planning and outage notification/escalation, purchasing and tracking of Travel Cards, tracking of training, and litigation holds.

A copy of each employee's forms submitted to PIRO is stored in a personnel folder on the network. This includes background checks, Employee Address CD-525, Declaration for Federal Employment OF-306, Health Benefits Election Form OPM SF-2809, Direct Deposit Sign-Up Form SF-1199A, Designation of Beneficiary SF-1152, Self-Identification of Handicap SF-256, Designation of Beneficiary - FERS SF-3102, Statement of Prior Service SF-144, Instructions for Employment Eligibility Verification Form I-9 (with copies of identification), and employee benefits. T*hese are duplicates of forms in WFMO. The ISSO will aggressively pursue the removal of these documents from NOAA4920 during the AO briefing.*

Contract managers collect and maintain information from contractors at the time of service to coordinate work orders and to communicate the needs of the agency.

Supervisors collect and maintain employees' information from doctors during extended sick leave to validate legitimacy of absence. Individuals requesting reasonable accommodation also provide medical information that supervisors maintain to process reasonable accommodation requests.

GDP and IN: Supervisors collect and maintain information from visitors, volunteers and foreign nationals during passport application and for permission to access federal facilities. See NAO 207-12 (http://www.corporateservices.noaa.gov/ames/administrative_orders/chapter_207/207-12.html)

Permitting

The Protected Species Workshop Coordinator collects name, vessel name, mailing address and phone number from vessel owners and operators to register for Hawaii longline protected species training.
Fisheries permit related BII (Vessel Name, Vessel Operator, Vessel Identifier, Fishing Locations, Catch Information, Observer Incidents, and Observer Post Cruise Log data are covered under Non-Disclosure Agreements and Magnuson/Stevens. Permit related information is stored, depending on the related fishery, either in the Permit application database covered under the NOAA4000 PIA or in the PIRO Permit application Database, both of which are covered under the System of Records Notice (SORN) Commerce/NOAA-19, *Permits and Registrations for United States Federally Regulated Fisheries.*

This information is maintained locally within PIRO and is used primarily for regulatory and administrative purposes. This information may be shared with other agencies as listed in the Introduction, having a legitimate business need and authorization. All information collected is extracted from paper records supplied by the individual or derived from other sources listed in the Introduction, scanned to the network and stored in a shared file.

Public
The Division may collect and maintain name, address, email address, and phone number from the public for comments on proposed actions, published in the Federal Register. This information is entered into regs.gov. The ISSO has suggested that we do not need to maintain the information; there is no such requirement related to regs.gov.

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.)*

	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	X		
Public			
Private sector			
Foreign governments			
Foreign entities	X	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.

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: NOAA4920 maintains a Microsoft Active Directory Domain, providing authentication and authorization services for employees. The system is not available publicly and remote sites are connected via secure encrypted VPN links. NOAA4920 interconnects for network transit purposes with NOAA1200, National Oceanic and Atmospheric Administration Corporate Services Local Area Network. PIRO has a dedicated WAN link to NOAA4000 to facilitate data interconnection between other systems within the bureau. Any PII/BII transmitted outside the system is done so using Accellion Secure File Transfer.
	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.fpir.noaa.gov/Library/SFD/PI_FedFish_Application_NoEx_Fillable_02Feb15.pdf (this is the Federal Fisheries Permit Application).	
X	Yes, notice is provided by other means.	Specify how: System Wide: Authorized users of NOAA4920 information technology systems are notified both in the NOAA rules of behavior and system usage consent warning banner that there is no expectation of privacy while using these systems which includes SAAD and directly associated WRD, and GPD information. Unauthorized users have no reasonable expectation of notification. Employees' performance reviews are uploaded to their electronic Official Personnel File (eOPF), which is accessible to all Federal employees. Upon hire, all employees are informed about their eOPF and how to access it during their onboarding process. Also, EOPF notifies employees when a document has been uploaded.

		Supervisors are required to ask for supporting documents when there is a lengthy sick leave request documentation that is tied to the sick leave request made by the employee through WebTA. The DOC Web TA sick leave request includes a Privacy Act Statement. For personnel management data, all employee, general public and contractor PII is collected directly from the individual through personal contact, by phone, email or mail. Potential employee PII is willingly provided to the division during the application process. All federal forms have Privacy Act Notices. Permit holders: Notice is given on permit applications.
	No, notice is not provided.	

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 personnel actions, individuals may decline to provide PII, in writing, to their supervisor or to the Human Resources Office; however, their employment status may be affected. Individuals may decline to provide emergency contact notification to their supervisors, in writing; however, their employment status may be affected. Permit applicants: The personal information is collected when the individual completes the appropriate application. On the application, the individual is advised that NMFS will not be able to issue a permit if the individual does not provide each item of information requested. The individual may choose to decline to provide the required personal information at that time, by not completing the application, but will not be able to receive a permit.
	No, individuals do not have an opportunity to decline to provide 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: System Wide: By supplying the PII/BII, the individual/entity consents to the use of the information for one particular use only (each type of information collection has a specific purpose). An employee that does not consent to use of PII/BII for user credentials would be unable to access the system, and if not consenting to the use of their PII for COOP, their employment might be affected. Permit applicants and holders: Permittees are provided with the

		link to NOAA's privacy policy where it states: "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose."
	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: Supervisors review individuals' PII occasionally to ensure that the emergency contact list is accurate. Employees may review PII in their eOPF file at any time. Employees can also review and update their information on the intranet page. Employees are also made aware via annual data calls that their personal contact information will be maintained as an emergency contact list/COOP plan. The HR personnel folders containing scans of federal employee application forms is restricted to only HR and management personnel with need to know. The information can be updated on request to HR. Permit applicants and holders: Information may be reviewed or updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time (information is on permits and permit applications).
	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: NOAA4920 uses centralized logging which can log and alert when sensitive files and folders are accessed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 1/9/2017 ☐ 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.

Identification and authentication (multifactor, CAC) before accessing PII Access control to PII through access control lists Separation of duties involving access to PII Enforcement of least privilege File system auditing, review, analysis and reporting Encryption of removable media, laptops and mobile devices Labeling of digital media to secure handling and distribution Sanitization of digital and non-digital media containing PII Use of encryption to securely transmit PII

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-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons. DEPT-6, Visitor Logs and Permits for Facilities Under Department Control DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons DEPT-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. COMMERCE/NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries COMMERCE/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: NOAA Records Schedules: Chapter 100 – General Chapter 200-Adminstrative and Housekeeping Records Chapter 300 - Personnel Chapter 400 – Finance Chapter 500 – Legal Chapter 600– International Chapter 900-Facilities Security and Safety Chapter 1200 – Scientific Research Chapter 1500 – Marine Fisheries
	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.

	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 with the

		information stored in the system.
X	Quantity of PII	Provide explanation: Total quantity of information is minimal and primarily pertains to local Federal employees and contractors.
X	Data Field Sensitivity	Provide explanation: There is sensitive PII for employees and fishermen, and sensitive BII for fishermen.
X	Context of Use	Provide explanation: Permits information and employee/contractor information is stored securely as described in Sections 8.1 and 8.2.
X	Obligation to Protect Confidentiality	Provide explanation: The Magnuson-Stevens Act authorizes confidentiality of fisheries data. The Health Insurance Portability and Accountability Act protects medical information received in relation to a prolonged illness or self-designation of disability, if applicable.
X	Access to and Location of PII	Provide explanation: System is not publicly accessible.
	Other:	Provide explanation:

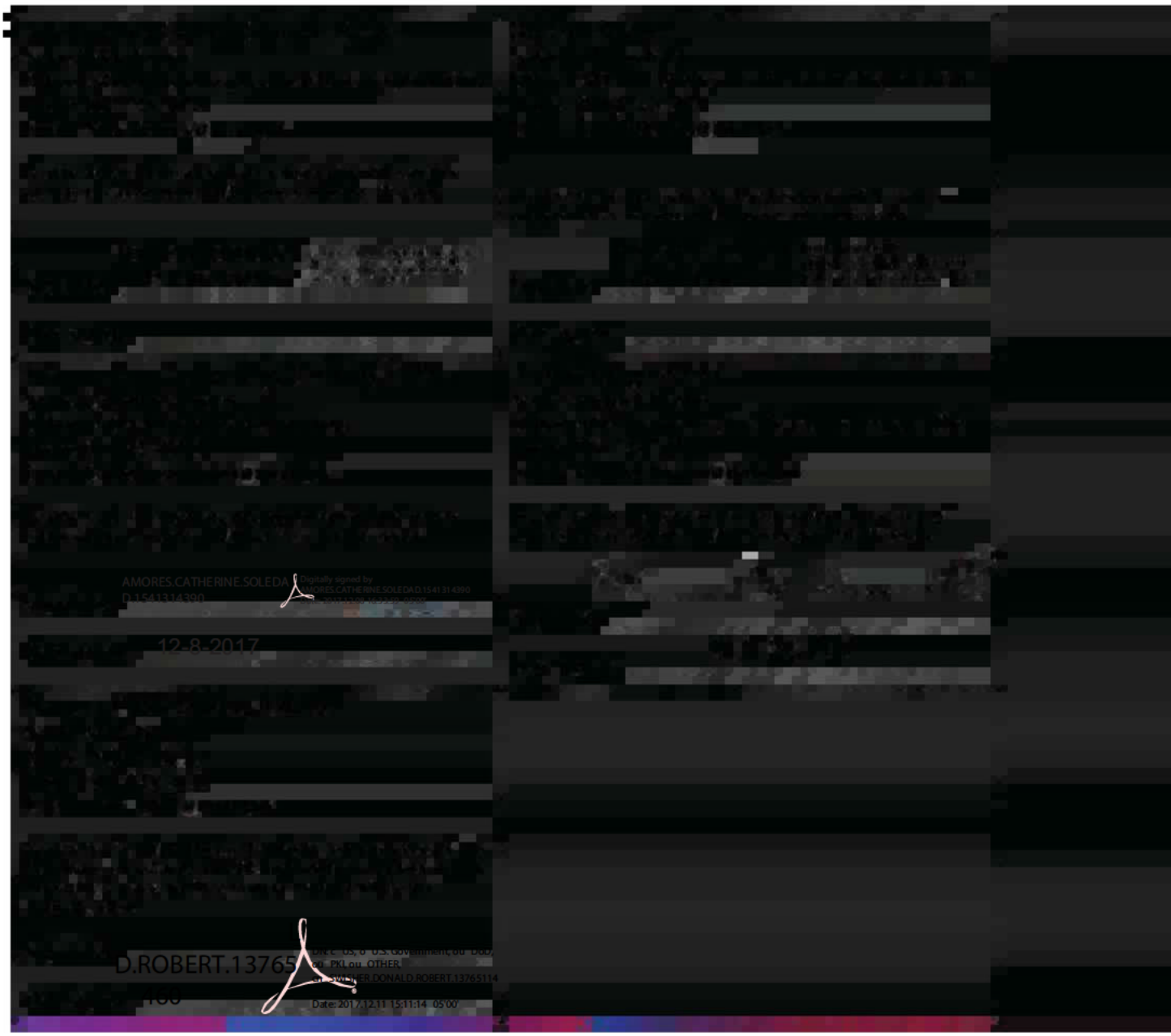
Section 12: Analysis

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: The findings indicate cases where PII is being collected without a bona fide mission/operational requirement. Personnel who work with PII/BII must examine processes and determine if reduction, sanitization or elimination of unneeded PII can be performed. Changes in business processes are administrative and will need to be reviewed and modified through management. (from last PIA but still pending) The ISSO will advocate to remove the duplicate HR forms and to delete public comments once entered into regs.gov.
	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: Based on the amount of sensitive PII in the system, additional technological controls need to be implemented. Repositories need to be defined and secured with encrypted file services. Network protocols for transmittal of sensitive information inside the LAN need to be encrypted. Perimeter and software solutions shall identify PII/BII in transit or in use without authorization. (from last PIA but still pending)
	No, the conduct of this PIA does not result in any required technology changes.


AMORES.CATHERINE.SOLEDAD.1541314390
Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390
12-8-2017
D.ROBERT.13765
Date: 2017.12.11 15:11:14 -05'00'

Version Number: 01-2015

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

Privacy Threshold Analysis
for the
NOAA4920 – Pacific Islands Region Office (PIRO)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA – PIRO LAN

Unique Project Identifier: 006-48-01-14-02-3305-00

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 NOAA Fisheries Pacific Islands Regional Office (PIRO) Local Area Network (LAN) functions as the overall General Support System (GSS) for PIRO located in Honolulu, Hawaii. Additional remote sites exist in Samoa, Guam and Saipan. The information system provides administrative support typically found in administrative offices within the federal government as well as supplemental operational services.

PIRO consists of the following divisional units:

- PIR Regional Administrators Office
- NOAA Office of General Counsel
- PIR Habitat Conservation Division
- PIR International Fisheries Division
- PIR Observer Program
- PIR Office of Management and Information
- PIR Protected Resources Division
- PIR Sustainable Fisheries Division

The categories of data collected, stored and disseminated include administrative, human resources, operations, statistical, economic, and technical.

NOAA4920 is located at the following locations: Honolulu, HI, American Samoa, the Commonwealth of the Northern Mariana Islands, and Guam. The primary functions of the NOAA4920 information system are:

- File and printer sharing
- Web applications and database services
- Access to NOAA/DOC web services via wide area network connections
- Pacific region fisheries permit data repository

No major application systems exist within NOAA4920.

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.)."

___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.

AMORES.CATHERINE.SOLEDAD.1

Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390

SWISHER.DONALD.ROBERT.1376511460

Digitally signed by SWISHER.DONALD.ROBERT.1376511460
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SWISHER.DONALD.ROBERT.1376511460
Date: 2017.12.11 14:17:14 -05'00'

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Tuesday, December 12, 2017 10:00 AM
To:	Nancy DeFrancesco
Cc:	Mark Graff NOAA Federal
Subject:	Re: November Monthly Privacy Report
Attachments:	NOAA5044 PTA for consistency with PIA v2.pdf

The PTA was revised to be consistent with the PIA, after the CRB. See attached. I thought I had cc'd you all when I sent the revised docs to DOC, but here it is.

On Tue, Dec 12, 2017 at 9:52 AM, Nancy DeFrancesco <nancy.defrancesco@noaa.gov> wrote:

> With regard to the PTA date for NOAA5044 (cell G49 of file "PTA PIA Management Report (16).xlsx), the PTA I have has a date of 11/6/2017 for Mark's approval. Sarah sent the attached to us on 11/6/2017 at 8:40am. Your sheet says 11/17/2017 for the CPO approval date.
>
> If you have a PTA approved 11/17/2017, please send it to me so I can update CSAM. If not, please update the PTA date in your sheet to 11/6/2017.
>
> thanks.
>
> Nancy A. DeFrancesco, CISSP, CISA, CRISC
> NESDIS Cyber Security Program & Solutions Branch Chief
> NESDIS Cyber Security Program Manager
> DOC/NOAA/NESDIS/ACIO S
> (240)429 0285/ Nancy.DeFrancesco@noaa.gov
>
> On 12/12/2017 8:50 AM, Mark Graff NOAA Federal wrote:
> > Good Morning,
> >
> > This is a report regarding the activities of the NOAA Privacy Program
> > from November 1 November 30, 2017. Attached are two spreadsheets
> > outlining the status of SORNs, PIAs, and PTAs within NOAA.
> >
> > Some of highlights of the Program's activities for the month include:
> >
> > * NOAA Privacy has continued to try to bring the status of PIA reviews
> > for all FISMA systems containing PII to be consistent with the
> > November 2014 DOC Memorandum requiring a current SAOP approved PIA
> > as a pre requisite to the issuance of an ATO. There are currently 2
> > remaining FISMA systems without an approved PIA that collect PII
> > (NOAA6401 and NOAA6702).

> * SORN approvals have been delayed at OMB. As such, DOC, along with
> other Federal Agencies, have faced a SORN review logjam preventing
> the timely approval of SORNs. NOAA currently is awaiting OMB's
> approval of DEPT 29 (a new SORN governing UAS collections), which
> was submitted to DOC in March. NOAA has several other more recent
> SORN submissions that have also been delayed, which are seeking
> amendments to existing SORNs.
>
> NOAA Privacy, in collaboration with CSD, prepared and briefed the CIO
> Council, as well as the ITSC, on a draft of NOAA's first Insider Threat
> Plan (Attached). The plan was required by the Presidential Memorandum
> regarding Insider Threat Programs that followed Executive Order 13587.
> The plan outlines NOAA's recommendations for program structure in the
> alternative funding becomes available to organize an Insider Threat
> Program within NOAA. The plan also recommends next steps to address
> potential risk mitigation actions consistent with the Presidential
> Memorandum that NOAA could potentially carry out absent additional
> funding. NOAA Privacy will brief the ECC on the draft prior to
> presenting a finalized plan to the NOAA CIO Council in January for a
> decision briefing.
>
> NOAA continued to roll out the 1st phase of the DLP solution,
> implementing the SSN filter on email traffic within all Staff Offices.
> Emails within the Staff Offices that contain SSNs whether in clear text
> or in an attachment as well as blank attachments with fillable SSN
> fields, will be rejected, and the sender will receive a single kickback
> notification instructing them to properly transmit Sensitive PII only
> through encrypted transmissions. Subsequent repeat attempts to transmit
> this material will be blocked, but will not receive multiple kickback
> notifications, and may be construed as deliberate attempts to circumvent
> DOC Privacy Policy governing the Electronic Transmission of PII.
>
> 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

NOAA OCIO
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 Threshold Analysis for the
NOAA Satellite Operations Facility (NSOF) Administrative LAN
NOAA5044

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NSOF Administrative LAN

Unique Project Identifier: 006-000351101 00-00-02-00-02-00

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 NSOF Administrative (Admin) Local Area Network (LAN) 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 NSOF Admin LAN provides endto-end connectivity and network access to all NSOF Admin LAN 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 with 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.

Detailed System Description for NOAA5044 is contained in its System Security Plan Appendix C in CSAM.

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): Building entry readers and electronic purchase transactions.					

_ 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.

__X__ Yes. *Please describe the activities which may raise privacy concerns.* There are electronic purchase transactions and building entry card readers.

___ 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 [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): Brian Little

Signature of ISSO or SO: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=LITTLE.BRIAN.WILLIAM.1365841230 Date: 2017.11.02 13:35:18 -04'00' Date: 11/02/2017

Name of Information Technology Security Officer (ITSO): Nancy 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: 2017.11.06 08:49:28 -05'00' Date: 11/06/2017

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: 2017.11.02 13:59:31 -04'00' Date: 11/02/2017

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: 2017.11.06 09:29:26 -05'00' Date: _____

Nancy DeFrancesco

From:	Nancy DeFrancesco
Sent:	Tuesday, December 12, 2017 9:53 AM
To:	Mark Graff NOAA Federal; Sarah Brabson
Subject:	Re: November Monthly Privacy Report
Attachments:	NOAA5044 PTA for consistency with PIA BL VG ND mhg.pdf

With regard to the PTA date for NOAA5044 (cell G49 of file "PTA PIA Management Report (16).xlsx), the PTA I have has a date of 11/6/2017 for Mark's approval. Sarah sent the attached to us on 11/6/2017 at 8:40am. Your sheet says 11/17/2017 for the CPO approval date.

If you have a PTA approved 11/17/2017, please send it to me so I can update CSAM. If not, please update the PTA date in your sheet to 11/6/2017.

thanks.

Nancy A. DeFrancesco, CISSP, CISA, CRISC
NESDIS Cyber Security Program & Solutions Branch Chief NESDIS Cyber Security Program Manager
DOC/NOAA/NESDIS/ACIO S
(240)429 0285/ Nancy.DeFrancesco@noaa.gov

On 12/12/2017 8:50 AM, Mark Graff NOAA Federal wrote:
> Good Morning,
>
> This is a report regarding the activities of the NOAA Privacy Program > from November 1 November 30, 2017. Attached are two spreadsheets > outlining the status of SORNs, PIAs, and PTAs within NOAA.
>
> Some of highlights of the Program's activities for the month include:
>
> * NOAA Privacy has continued to try to bring the status of PIA reviews > for all FISMA systems containing PII to be consistent with the > November 2014 DOC Memorandum requiring a current SAOP approved PIA > as a pre requisite to the issuance of an ATO. There are currently 2 > remaining FISMA systems without an approved PIA that collect PII > (NOAA6401 and NOAA6702).
> * SORN approvals have been delayed at OMB. As such, DOC, along with > other Federal Agencies, have faced a SORN review logjam preventing > the timely approval of SORNs. NOAA currently is awaiting OMB's > approval of DEPT 29 (a new SORN governing UAS collections), which > was submitted to DOC in March. NOAA has several other more recent > SORN submissions that have also been delayed, which are seeking > amendments to existing SORNs.
>
> NOAA Privacy, in collaboration with CSD, prepared and briefed the CIO > Council, as well as the ITSC, on a draft of NOAA's first Insider Threat > Plan (Attached). The plan was required by the Presidential Memorandum > regarding Insider Threat Programs that followed Executive Order 13587.
> The plan outlines NOAA's recommendations for program structure in the > alternative funding becomes available to organize an Insider Threat > Program within NOAA. The plan also recommends next steps to

address > potential risk mitigation actions consistent with the Presidential > Memorandum that NOAA could potentially carry out absent additional > funding. NOAA Privacy will brief the ECC on the draft prior to > presenting a finalized plan to the NOAA CIO Council in January for a > decision briefing.
>
> NOAA continued to roll out the 1st phase of the DLP solution, > implementing the SSN filter on email traffic within all Staff Offices.
> Emails within the Staff Offices that contain SSNs whether in clear text > or in an attachment as well as blank attachments with fillable SSN > fields, will be rejected, and the sender will receive a single kickback > notification instructing them to properly transmit Sensitive PII only > through encrypted transmissions. Subsequent repeat attempts to transmit > this material will be blocked, but will not receive multiple kickback > notifications, and may be construed as deliberate attempts to circumvent > DOC Privacy Policy governing the Electronic Transmission of PII.
>
> Mark H. Graff
> FOIA Officer/Bureau Chief Privacy Officer (BCPO) > National Oceanic and Atmospheric Administration > (301) 628 5658 (O) (b)(6) (C)
>

>

Version Number: 01-2015

U.S. Department of Commerce
National Oceanic and Atmospheric Administration
(NOAA)

Privacy Threshold Analysis for the
NOAA Satellite Operations Facility (NSOF) Administrative LAN
NOAA5044

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NSOF Administrative LAN

Unique Project Identifier: 006-000351101 00-00-02-00-02-00

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 NSOF Administrative (Admin) Local Area Network (LAN) 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 NSOF Admin LAN provides endto-end connectivity and network access to all NSOF Admin LAN 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 with 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.

Detailed System Description for NOAA5044 is contained in its System Security Plan Appendix C in CSAM.

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): Building entry readers and electronic purchase transactions.					

_ 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.)."

___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 [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): Brian Little

Signature of ISSO or SO: LITTLE.BRIAN.WILLIAM.1365841230 Digitally signed by LITTLE.BRIAN.WILLIAM.1365841230 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=LITTLE.BRIAN.WILLIAM.1365841230 Date: 2017.11.02 13:35:18 -04'00' Date: 11/02/2017

Name of Information Technology Security Officer (ITSO): Nancy 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: 2017.11.06 08:49:28 -05'00' Date: 11/06/2017

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: 2017.11.02 13:59:31 -04'00' Date: 11/02/2017

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: 2017.11.06 09:29:26 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, December 13, 2017 10:36 AM
To:	Toland, Michael; Gitelman, Steve (Contractor); PrivacyAct
Cc:	Mark Graff NOAA Federal
Subject:	NOAA 12 SORN in new template
Attachments:	NOAA 12 updated and in new template_121317.docx

There are no changes except to add the two latest routine uses.

thx Sarah

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

NOAA OCIO
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)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, December 18, 2017 1:00 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA 11 updated and in new template
Attachments:	NOAA 11 updated and in new template_121817.docx

Mar (b)(5) [redacted]

[redacted].

Feel free to review this. I know Mike is out through Jan 8.

I still have to do NOAA 1, 3, 14, 15, 20, 21 and 22. For 14 and 15, I have the updates. I've contacted the last three, but still need to contact 1 and 3.

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

NOAA OCIO
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)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, December 18, 2017 1:36 PM
To:	Toland, Michael; Gitelman, Steve (Contractor); PrivacyAct
Cc:	Mark Graff NOAA Federal
Subject:	NOAA 11 SORN updated and in new template
Attachments:	NOAA 11 updated and in new template_121817.docx

Mik (b)(5) [redacted].

I went ahead and added all the systems which we had not previous included in this SORN.

thx Sarah

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

NOAA OCIO
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)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, December 27, 2017 9:26 AM
To:	Mark Graff NOAA Federal
Cc:	Sallie.M.Ahlert@noaa.gov
Subject:	NOAA8877 certification, PIA and PTA and SAR is in PIA folder
Attachments:	NOAA8877 FY18 PIA 20171206.pdf; NOAA8877 FY18 PTA 20171206 (1).pdf

Mark, Sallie Ahlert attached the signed Certification to the front of the re signed PIA. This doc and the PTA are attached. As with the NOAA6205 certification docs I re sent this am, the SAR is in the PIA folder, but I can also send to you via Accellion.

thx Sarah

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

NOAA OCIO
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)

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, December 27, 2017 10:08 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA8877 certification, PIA and PTA and SAR is in PIA folder
Attachments:	NOAA8877 FY18 PTA 20171206 (1) mhg.pdf

No problem the "Deletion" would be new since the last approval because of the new scanners referenced in Sec. 12, but it's not urgent, and the approval can stand without it for now. PTA is 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, Dec 27, 2017 at 10:04 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> This means I have to detach and save signatures on the certification in addition to saving the PIA signatures. If this was approved without "deletion" last time around, can we not let it stand? Doesn't seem like the best use of one's time at this point. Also my fingers are almost too cold to type.
>
> Are you also signing the PTA? And can you review the SAR in the folder?
>
> Thanks, Sarah
>
> On Wed, Dec 27, 2017 at 9:59 AM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:
>
> > Looks good
> >
> > Signed and attached. Just for accuracy, please check "Deleting" on Sec. 10.2. Considering the added scanners (Sec. 12), used to upload sensitive PII for WMFO system processing, any disposal of scanned PII would require deletion or overwriting.
> >
> > Mark H. Graff
> > FOIA Officer/Bureau Chief Privacy Officer (BCPO)
> > National Oceanic and Atmospheric Administration
> > (301) 628 5658 (O)
> > (b)(6) (C)
> >
> >

On Wed, Dec 27, 2017 at 9:26 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, Sallie Ahlert attached the signed Certification to the front of the re signed PIA. This doc and the PTA are attached. As with the NOAA6205 certification docs I re sent this am, the SAR is in the PIA folder, but I can also send to you via Accellion.
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> NOAA OCIO
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (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) [redacted]

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Radar Operations Center Local Area Network (ROC LAN)
NOAA8877
December 06, 2017

U.S. Department of Commerce Privacy Threshold Analysis

NOAA ROC LAN

Unique Project Identifier: NOAA8877

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: NOAA8877 is a General Support System (GSS), which provides a small to medium enterprise LAN for the NOAA\NWS ROC and its tri-agency personnel. The ROC's primary mission is to support operations, maintenance, and sustainment of the tri-federal agency (DOC, DOD, and DOT) NEXRAD weather radar fleet. NOAA8877 provides general office collaboration software and tools together with highly specialized software and hardware systems, which enable ROC's personnel in four branches (Operations, Engineering, Program Support, and Applications) to perform their respective System Development Life Cycle (SDLC) functional roles. Operations Branch runs a 24x7 radar hotline, performs independent testing of modifications and software, and provides on-site technical field support for specialized and particularly difficult radar modifications. Engineering Branch does multi-year planning, project management, development, unit and integration testing, security design, and implementation for all the hardware and software modifications to the radar systems. Program Support Branch provides logistics support, contract maintenance, configuration management, and documentation. Applications Branch leads data quality analysis and improvement initiatives. In addition, this branch leads the scientific groups that make determination on readiness of new science for integration into the radar. 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. *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 ROC LAN 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 ROC LAN 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): Michael W. Miller

Signature of ISSO or SO: MILLER.MICHAEL.W.1180644136 Digitally signed by MILLER MICHAEL W 1180644136 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn MILLER MICHAEL W 1180644136 Date 2017 12 06 16 35 34 06'00' Date: 12/6/2017

Name of Information Technology Security Officer (ITSO): Joy Baker

Signature of ITSO: BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER JOY ALLISON 1269758577 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BAKER JOY ALLISON 1269758577 Date 2017 12 07 07 39 04 06'00' Date: 12/7/2017

Name of Authorizing Official (AO): Joseph A. Pica

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.12.21 08:48:20 05'00' Date: 12/21/2017

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 2017 12 27 10 06 54 05'00' Date: 12.27.17

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Wednesday, December 27, 2017 10:20 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: FOR NOAA6205 certification
Attachments:	NOAA6205 PIA Annual Review Certification Form for mhg signature mhg.pdf; NOAA6205 PIA for MHG signature mhg.pdf; NOAA6205 PTA_ 2017 for mhg signature mhg.pdf

Here you go

PTA, PIA, and Re Cert form all signed and attached. All of them look good

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

On Wed, Dec 27, 2017 at 8:52 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark Somehow this slipped through the cracks. Please sign when you have a chance and let me know if you will review the SAR and SRTR in the PIA folder or need me to send to you via Accellion.
>
> thx Sarah
>
> Forwarded message
> From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
> Date: Thu, Dec 7, 2017 at 1:12 PM
> Subject: FOR NOAA6205 certification
> To: Mark Graff NOAA Federal <mark.graff@noaa.gov>
>
> Mark, I sent you the docs yesterday but hadn't yet checked into the security/privacy assessment docs. Next time I'll do it all at once (they had to be uploaded).
>
> The NOAA6205 SAR and SRTR are now in the PIA folder. You can review them there, or go to CSAM system specific appendices d and o, or I can send to you via Accellion. Privacy controls look good.
>
> thx Sarah
>
> Sarah D. Brabson

IT Infrastructure Investment Program Manager
PRA Clearance Officer

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

U.S. DEPARTMENT OF COMMERCE

Department of Commerce

Privacy Impact Assessment (PIA)
Annual Review Certification Form

September 2017

Prepared by:
Office of Privacy and Open Government (OPOG)
DOC Privacy Program Plan Appendix L

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

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

Name of PIA: NOAA6205 PIA

FISMA Name/ID (if different): NOAA6205

Name of IT System/ Program Owner: Marian Westley

Name of Information System Security Officer: Maurice McLeod

Name of Authorizing Official(s): Richard Edwing

Date of Last PIA Compliance Review Board (CRB): 12/1/2016

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

Date of PIA Review: 11/27/2017

Name of Reviewer: Maurice McLeod

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: MCLEOD.MAURICE.STGEORGE.1267033699

Digitally signed by MCLEOD.MAURICE.ST GEORGE.1267033699
Date: 2017.11.27 14:59:59 -05'00'

Date of BCPO Review: 12.27.17

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 2017 12 27 10 17 17 05'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Center for Operational Oceanographic Products and Services
PORTS® and NWLON IT System (NOAA6205)

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
Center for Operational Oceanographic Products and Services PORTS® and NWLON IT System (NOAA6205)

Unique Project Identifier: 006-48-01-15-01-3402-00

Introduction: System Description

The National Ocean Service (NOS) Center for Operational Oceanographic Products and Services (CO-OPS) collects and distributes observations and predictions of water levels and currents to ensure safe, efficient and environmentally sound maritime commerce. CO-OPS establishes standards for the collection and processing of water level and current data, collects and documents user requirements which serve as the foundation for all resulting program activities, designs new and/or improved oceanographic observing systems, designs software to improve CO-OPS' data processing capabilities, maintains and operates oceanographic observing systems, performs operational data analysis/quality control, and produces/disseminates oceanographic products. CO-OPS is divided into four Divisions to address various functionally important areas. The divisions are Engineering (ED), Field Operations (FOD), Oceanographic (OD) and Information Systems (ISD). These users are internal to the system including federal employees and contractors.

The CO-OPS PORTS® and NWLON System (NOAA6205) and the infrastructure components that stores, processes and transmits the information are the focus of this document and play an important role in NOAA's strategic goals to promote safe navigation and sustain healthy coasts. This system provides CO-OPS and its four divisions with general office automation, application management, network connectivity, file storage, process and workflow management, and application development functionality. NOAA6205 provides several applications for both in-house and external use. These applications run either on Linux or Windows-based platforms. All Linux or Windows-based platforms upon which these applications run are supported by NOAA6205. NOAA6205 has public web servers which provide limited external information to the public. This information has been reviewed and approved by CO-OPS.

The data received by CO-OPS is used to ensure safe, efficient and environmentally sound maritime commerce, and provides real-time data to government agencies such as the U.S. Coast Guard, National Weather Service, U.S. Geological Survey, NOAA 1 HAZMAT and FEMA which use the data when maritime events occur. Non-government entities such as commercial shippers and harbor pilots use the data to avoid groundings and collisions.

PII and BII:

NOAA6205 collects, stores, and processes basic identifying information about employees, contractors, volunteers and partner agency staff who use the system. The identifying information is collected and maintained for CO-OPS' COOP plan and other administrative processes. The information being collected is shared within the Bureau on a case by case basis.

This information is being collected to be able to manage administrative programs related to an employee or contractor's employment status, travel, and other human resources activities. PII is collected from employees as well for emergency purposes. *None of the administrative processes listed require SSNs. SSNs have been deliberately removed from CO-OPS' administrative processes for some time now.*

PII is also collected by NOAA6205 web applications for external users requesting access to public facing data. These users are required to provide information to CO-OPS for contact purposes. The information collected on external users requesting access to public facing data by NOAA6205 applications will only be accessible to CO-OPS users with appropriate roles and permissions to view the database table that contains these data elements. It will not be shared with any other organization or agency. This information is collected exclusively to determine eligibility to obtain access to certain data products.

Vendor provided BII is also collected in the form of contract Requests for Proposals (RFPs). These RFPs are stored electronically on the system and shared amongst the source selection team through the evaluation period and until completion of reviews at which time the RFPs that were shared with and reviewed by the source selection team, but not selected, are removed and the selected RFP is printed and stored in accordance with the record retention schedule.

Information is collected on CO-OPS users is automatically collected by the System for auditing purposes only when they access NOAA6205 systems. The audit logs generated during the access of NOAA6205 are shared with the NOS web administrators for evaluation purposes. The information that is stored in this system consists of the following: User ID, IP Address, and Date/Time of Access.

Statutory authorities:

5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. 1512, an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

The Federal Information Processing Standard (FIPS) 199 security impact category for NOAA6205 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		f. Driver's License		j. Financial Account	
c. Employer ID	X	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:					

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): Employee information is collected for emergency/disaster/COOP related contact needs. General inquiries related to information sharing consist of collecting name and telephone number in order to respond to the information requests. Certain subject matter experts agree explicitly to share contact information (name, phone, email) on CO-OPS' web site.					

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			
Other work-related data (specify): Work related data is also only collected for emergency/disaster/COOP related contact needs.					

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): User ID, IP Address, and Date/Time of Access is automatically collected by the System for auditing purposes only.					

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	X	Online	
Telephone		Email	X		
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	X
Other (specify): PIV cards are used for system access within NOAA6205. These cards are issued, managed, and terminated by the NOAA Security Office. The information located on these cards is not shared once the cards are generated by the Security Office. The information is NOT stored in the NOAA6205 system.			

	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	
Other (specify):			

Building entry readers recognize CAC cards used to gain entry, but do not store any of the data embedded on the card.

	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		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).

CO-OPS NOAA6205 collects, stores, and processes basic identifying information about employees, contractors, volunteers and partner agency staff who use the system. The identifying information is collected and maintained for CO-OPS' COOP plan and other administrative processes. This information consists of Name (First, Last), Home Address, Phone Numbers (Both Work and Personal Home), employer and employee ID, and passport number when needed. Emergency Contact Information is also collected and includes: Name (First, Last), Home Address, Work and or Home phone numbers.

This information is being collected to be able to manage administrative programs related to an employee or contractor's employment status, travel, and other human resources activities. PII is collected from employees as well for emergency purposes. This information is collected and disseminated to the Division Chiefs and Deputies within CO-OPS to aid in communicating with employees during emergencies and contingent events. *None of the administrative processes listed require SSNs. SSNs have been deliberately removed from CO-OPS' administrative processes for some time now.*

Information is also collected by NOAA6205 web applications for external users requesting access to public facing data. These users are required to provide information to CO-OPS for contact purposes. The information that is stored in this system consists of the following - For partner vendors: Name (First and Last), Business Street Address, City, State, Country, Email, Phone Number, Organization or Business Name, Occupation, Contract Number, Project Number, Account Status and Application Date. For general public: Name (First, Last), Street Address, City, State, Country, Email, Phone Number, Organization, if applicable.

The information collected on external users requesting access to public facing data by NOAA6205 applications will only be accessible to CO-OPS users with appropriate roles and permissions to view the database table that contains these data elements. It will not be shared with any other organization or agency. This information is collected exclusively to determine eligibility to obtain access to certain data products.

Vendor provided BII is also collected in the form of contract Requests for Proposals (RFPs). These RFPs are stored electronically on the system until completion of reviews at which time non-selected RFPs are removed and the selected RFP is printed and stored in accordance with the record retention schedule.

Information is collected on CO-OPS users is automatically collected by the System for auditing purposes only when they access NOAA6205 systems. The information that is stored in this system consists of the following: User ID, IP Address, and Date/Time of Access.

In addition, CO-OPS utilizes a VPN over the Internet to connect the Chesapeake office to the Seattle and Silver Spring offices. By using a VPN, CO-OPS ensures that all data is encrypted while in transit between the offices, and transmission integrity is maintained.

The overall collection and storage of PII/BII is part of accomplishing the legislated mission of within CO-OPS.

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	
Contractors	X
Other (specify): General public access is limited to posting comments on the Web page.	

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://tidesandcurrents.noaa.gov/privacy.html

X	Yes, notice is provided by other means.	Specify how: Visitors to the CO-OPS web site can request information by submitting an email through an information request contact form. Individuals are under no obligation to provide any identifying information, and the details of how this information is handled are readily available via the CO-OPS Privacy Policy and a Privacy Act statement. CO-OPS staff members (employees) are provided notice via email of how PII is used (i.e., emergency contact information in case of emergency or disasters), CO-OPS' employees are also pointed to the Privacy Act Statement and Policy on the public facing website upon hire. CO-OPS staff members (employees) are provided notice of information to be collected from them upon hire as well as via COOPS Privacy Policy on the public-facing Web site to which they are directed. Staff members are notified upon request for collection of identifying information that they may decline to provide the information, but that in some instances it may affect their employment. Vendor provided BII is collected in the form of contract Requests for Proposals (RFPs). In addition to the CO-OPS Privacy Policy which govern how vendor PII/BII is maintained, Contracting Officers also stipulate how vendor PII/BII is disseminated via non-disclosure agreement and in accordance with privacy notices placed by the vendors in their proposals.
	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: Visitors to the CO-OPS web site can request information by submitting an email through an information request contact form. Individuals are under no obligation to provide any identifying information, and the details of how this information is handled are readily available via the CO-OPS Privacy Policy and a Privacy Act statement. CO-OPS staff members (employees) are provided notice via email of how PII is used (i.e., emergency contact information in case of emergency or disasters) upon hire as well as via COOPS Privacy Policy on the public-facing Web site to which they are directed. Staff members are notified upon request for collection of identifying information that they may decline to provide the

		information via email or verbally, to their supervisors, but that in some instances it may affect their employment. Vendors are also under no obligation to provide any identifying information. Information provided is voluntary in the form of an RFP in response to a solicitation.
	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 visitors to the CO-OPS site, the one purpose of collecting the information is described in the Privacy Act Statement. COOPS does not collect personally-identifiable information unless visitors choose to provide it to us. If information is provided us with personally identifiable information, for example by sending an e-mail or by filling out a form and submitting it through our Web site, we use that information only to respond to the message and to help provide visitors with the information and services that they request. Submitting voluntary information constitutes consent to the use of the information for the stated purpose. When a user clicks 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. As information gathered only has one particular use, managing administrative programs related to an employee or contractor's employment status, individuals have the opportunity to consent or decline upon request of the information. Vendor provided BII is collected in the form of contract Requests for Proposals (RFPs). In addition to the CO-OPS Privacy Policy which govern how vendor PII/BII is maintained, contracting officers also stipulate how vendor PII/BII is disseminated via non-disclosure agreement and in accordance with privacy notices placed by the vendors on their proposals.
	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: Visitors to the CO-OPS site provide current information when contacting us. CO-OPS staff members are queried on a quarterly basis, during which they can provide updates. Members of the public are not required or asked to provide any identifying information. Members of the public have an opportunity to update their PII at any time by providing updated information via email, phone or fax. Vendors have an opportunity to update their PII/BII by providing updated physical or electronic invoices, phone call or by updating information through another RFP when there is a new solicitation
	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: Only authorized individuals have access to the safe in which physical PII is stored. All electronic forms of PII is strictly monitored, tracked, and recorded by access controls in place on the System.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): November 4, 2014 ☐ 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). The privacy controls assessment that was submitted with this PIA was reviewed by the BCPO.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	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.

NOAA implements various controls and technologies used to protect PII/BII on NOAA6205. These controls are in place to ensure that the confidentiality, integrity, and availability of how PII/BII information is collected, maintained, and transmitted within the NOAA6205 is in accordance with the System's categorization level. For example, NOAA has implemented technologies such as control lists and user authorizations for access control. Additionally, through the Media and Backup Plan, NOAA has implemented controls to limit the retention and transmission of PII. Encryption and access controls also both protect PII/BII 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 the Public Requesting or Providing Information Related to NOAA's Mission; DEPT-18, Employees Information Not Covered by Notices of Other Agencies. Also, DEPT-2, Accounts Receivable; DEPT-6, Visitor Logs and Permits for Facilities under Department Control; and DEPT-13, Investigative and Security 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: 1609-06 in the NOAA Disposition Handbook
	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	
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: There is enough information to identify an individual
X	Quantity of PII	Provide explanation: There are less than 1000 records in all.
X	Data Field Sensitivity	Provide explanation: Phone numbers and email addresses are the primary information collected and are used for communication purposes.
X	Context of Use	Provide explanation: The user information has been provided voluntarily: from people within the organization for administrative purposes, by visitors to the public Web site, and by vendors who wish to bid on a solicitation.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Users are required to log into the application with a user name and password. The database fields that contain PII are encrypted
	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 Statement to the public facing Web site.
	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: Addition of Privacy Act Statement to the public facing Web site.
	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: Marian Westley Office: CO-OPS Phone: 240-533-0481 Email: Marian.westley@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: WESTLEY.MARIAN.B.1365896638 Digitally signed by WESTLEY.MARIAN.B.1365896638 Date: 2017.11.15 15:22:37 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: NOS Phone: 240-533-0832 Email: john.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: 2017.12.06 02:24:19 -05'00' Date signed:
Authorizing Official Name: Richard Edwing Office: CO-OPS Phone: 240-533-0482 Email: Richard.edwing@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: EDWING.RICHARD.F.1365829620 Digitally signed by EDWING.RICHARD.F.1365829620 Date: 2017.11.27 14:37:36 -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: 2017 12 27 10:19:03 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: 02-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
For the
Center for Operational Oceanographic Products and Services PORTS®
and NWLON IT System (NOAA6205)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA6205

Unique Project Identifier: NOAA6205

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 Ocean Service (NOS) Center for Operational Oceanographic Products and Services (CO-OPS) collects and distributes observations and predictions of water levels and currents to ensure safe, efficient and environmentally sound maritime commerce. CO-OPS establishes standards for the collection and processing of water level and current data, collects and documents user requirements which serve as the foundation for all resulting program activities, designs new and/or improved oceanographic observing systems, designs software to improve CO-OPS' data processing capabilities, maintains and operates oceanographic observing systems, performs operational data analysis/quality control, and produces/disseminates oceanographic products. CO-OPS is divided into four Divisions to address various functionally important areas. The divisions are Engineering (ED), Field Operations (FOD), Oceanographic (OD) and Information Systems (ISD). These users are internal to the system including federal employees and contractors. The CO-OPS PORTS® and NWLON System (NOAA6205) and the infrastructure components that stores, processes and transmits the information are the focus of this document and play an important role in NOAA's strategic goals to promote safe navigation and sustain healthy coasts. This system provides CO-OPS and its four divisions with general office automation, application management, network connectivity, file storage, process and workflow management, and application development functionality. NOAA6205 provides several applications for both in-house and external use. These applications run either on Linux or Windows-based platforms. All Linux or Windows-based platforms upon which these applications run are supported by NOAA6205. NOAA6205 has public web servers which provide limited external information to the public. This information has been reviewed and approved by CO-OPS. The data received by CO-OPS is used to ensure safe, efficient and environmentally sound maritime commerce, and provides real-time data to government agencies such as the U.S. Coast Guard, National Weather Service, U.S. Geological Survey, NOAA 1 HAZMAT and FEMA which use the data when maritime events occur. Non-government entities such as commercial shippers and harbor pilots use the data to avoid groundings and collisions.

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.

____ 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 NOAA6205 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 NOAA6205 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): Maurice McLeod

Signature of ISSO or SO: MCLEOD.MAURICE.STGEORGE.1267033699 Digitally signed by MCLEOD.MAURICE.STGEORGE.1267033699 Date: 2017.11.30 08:15:28 -05'00' Date: _____

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

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2017.12.06 02:12:37 -05'00' Date: _____

Name of Authorizing Official (AO): Richard Edwing

Signature of AO: EDWING.RICHARD.F.1365829620 Digitally signed by EDWING.RICHARD.F.1365829620 Date: 2017.11.30 08:41:51 -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: 2017.12.27 10:16:35 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, December 29, 2017 12:43 PM
To:	Toland, Michael; Gitelman, Steve (Contractor); PrivacyAct
Cc:	Mark Graff NOAA Federal
Subject:	NOAA 15 with contact info amended and in new template
Attachments:	NOAA 15 updated and in new template_122917.docx

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

NOAA OCIO
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)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, December 28, 2017 3:04 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA 14 SORN for review
Attachments:	NOAA 14 updated and in new template_122717.docx

I found out one of the programs covered by this SORN is no longer in existence, and added one category of record for alumni. The rest was the template and the new routine use.

thx Sarah

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

NOAA OCIO
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)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, December 29, 2017 8:36 AM
To:	Toland, Michael; Gitelman, Steve (Contractor); PrivacyAct
Cc:	Mark Graff NOAA Federal
Subject:	NOAA 14 SORN updated and in new template
Attachments:	NOAA 14 updated and in new template_122717.docx

Please see the attached. I have not been doing the reports, since Mike said that we would have a meeting to discuss the last question in the report template.

thx Sarah

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

NOAA OCIO
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)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, December 29, 2017 1:03 PM
To:	Gioffre, Kathy (Federal); CPO
Cc:	John D. Parker; Maurice Mcleod NOAA Federal; Mark Graff NOAA Federal
Subject:	Certification documents for NOAA6205
Attachments:	NOAA6205 PTA_ 2017 for mhg signature mhg.pdf; NOAA6205 PIA for MHG signature mhg.pdf; NOAA6205 PIA Annual Review Certification Form for mhg signature mhg.pdf

Hi, Kathy, attached are the certification, the re signed PIA and a current PTA.

NOAA8877 certification docs to follow.

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

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

U.S. DEPARTMENT OF COMMERCE

Department of Commerce

Privacy Impact Assessment (PIA)
Annual Review Certification Form

September 2017

Prepared by:
Office of Privacy and Open Government (OPOG)
DOC Privacy Program Plan Appendix L

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

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

Name of PIA: NOAA6205 PIA

FISMA Name/ID (if different): NOAA6205

Name of IT System/ Program Owner: Marian Westley

Name of Information System Security Officer: Maurice McLeod

Name of Authorizing Official(s): Richard Edwing

Date of Last PIA Compliance Review Board (CRB): 12/1/2016

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

Date of PIA Review: 11/27/2017

Name of Reviewer: Maurice McLeod

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: MCLEOD.MAURICE.STGEORGE.1267033699

Digitally signed by MCLEOD.MAURICE.ST GEORGE.1267033699
Date: 2017.11.27 14:59:59 -05'00'

Date of BCPO Review: 12.27.17

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 2017 12 27 10 17 17 05'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Center for Operational Oceanographic Products and Services
PORTS® and NWLON IT System (NOAA6205)

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
Center for Operational Oceanographic Products and Services PORTS® and NWLON IT System (NOAA6205)

Unique Project Identifier: 006-48-01-15-01-3402-00

Introduction: System Description

The National Ocean Service (NOS) Center for Operational Oceanographic Products and Services (CO-OPS) collects and distributes observations and predictions of water levels and currents to ensure safe, efficient and environmentally sound maritime commerce. CO-OPS establishes standards for the collection and processing of water level and current data, collects and documents user requirements which serve as the foundation for all resulting program activities, designs new and/or improved oceanographic observing systems, designs software to improve CO-OPS' data processing capabilities, maintains and operates oceanographic observing systems, performs operational data analysis/quality control, and produces/disseminates oceanographic products. CO-OPS is divided into four Divisions to address various functionally important areas. The divisions are Engineering (ED), Field Operations (FOD), Oceanographic (OD) and Information Systems (ISD). These users are internal to the system including federal employees and contractors.

The CO-OPS PORTS® and NWLON System (NOAA6205) and the infrastructure components that stores, processes and transmits the information are the focus of this document and play an important role in NOAA's strategic goals to promote safe navigation and sustain healthy coasts. This system provides CO-OPS and its four divisions with general office automation, application management, network connectivity, file storage, process and workflow management, and application development functionality. NOAA6205 provides several applications for both in-house and external use. These applications run either on Linux or Windows-based platforms. All Linux or Windows-based platforms upon which these applications run are supported by NOAA6205. NOAA6205 has public web servers which provide limited external information to the public. This information has been reviewed and approved by CO-OPS.

The data received by CO-OPS is used to ensure safe, efficient and environmentally sound maritime commerce, and provides real-time data to government agencies such as the U.S. Coast Guard, National Weather Service, U.S. Geological Survey, NOAA 1 HAZMAT and FEMA which use the data when maritime events occur. Non-government entities such as commercial shippers and harbor pilots use the data to avoid groundings and collisions.

PII and BII:

NOAA6205 collects, stores, and processes basic identifying information about employees, contractors, volunteers and partner agency staff who use the system. The identifying information is collected and maintained for CO-OPS' COOP plan and other administrative processes. The information being collected is shared within the Bureau on a case by case basis.

This information is being collected to be able to manage administrative programs related to an employee or contractor's employment status, travel, and other human resources activities. PII is collected from employees as well for emergency purposes. *None of the administrative processes listed require SSNs. SSNs have been deliberately removed from CO-OPS' administrative processes for some time now.*

PII is also collected by NOAA6205 web applications for external users requesting access to public facing data. These users are required to provide information to CO-OPS for contact purposes. The information collected on external users requesting access to public facing data by NOAA6205 applications will only be accessible to CO-OPS users with appropriate roles and permissions to view the database table that contains these data elements. It will not be shared with any other organization or agency. This information is collected exclusively to determine eligibility to obtain access to certain data products.

Vendor provided BII is also collected in the form of contract Requests for Proposals (RFPs). These RFPs are stored electronically on the system and shared amongst the source selection team through the evaluation period and until completion of reviews at which time the RFPs that were shared with and reviewed by the source selection team, but not selected, are removed and the selected RFP is printed and stored in accordance with the record retention schedule.

Information is collected on CO-OPS users is automatically collected by the System for auditing purposes only when they access NOAA6205 systems. The audit logs generated during the access of NOAA6205 are shared with the NOS web administrators for evaluation purposes. The information that is stored in this system consists of the following: User ID, IP Address, and Date/Time of Access.

Statutory authorities:

5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

15 U.S.C. 1512, an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.

The Federal Information Processing Standard (FIPS) 199 security impact category for NOAA6205 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		f. Driver's License		j. Financial Account	
c. Employer ID	X	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:					

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): Employee information is collected for emergency/disaster/COOP related contact needs. General inquiries related to information sharing consist of collecting name and telephone number in order to respond to the information requests. Certain subject matter experts agree explicitly to share contact information (name, phone, email) on CO-OPS' web site.					

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			
Other work-related data (specify): Work related data is also only collected for emergency/disaster/COOP related contact needs.					

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): User ID, IP Address, and Date/Time of Access is automatically collected by the System for auditing purposes only.					

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	X	Online	
Telephone		Email	X		
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	X
Other (specify): PIV cards are used for system access within NOAA6205. These cards are issued, managed, and terminated by the NOAA Security Office. The information located on these cards is not shared once the cards are generated by the Security Office. The information is NOT stored in the NOAA6205 system.			

	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	
Other (specify):			

Building entry readers recognize CAC cards used to gain entry, but do not store any of the data embedded on the card.

	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		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).

CO-OPS NOAA6205 collects, stores, and processes basic identifying information about employees, contractors, volunteers and partner agency staff who use the system. The identifying information is collected and maintained for CO-OPS' COOP plan and other administrative processes. This information consists of Name (First, Last), Home Address, Phone Numbers (Both Work and Personal Home), employer and employee ID, and passport number when needed. Emergency Contact Information is also collected and includes: Name (First, Last), Home Address, Work and or Home phone numbers.

This information is being collected to be able to manage administrative programs related to an employee or contractor's employment status, travel, and other human resources activities. PII is collected from employees as well for emergency purposes. This information is collected and disseminated to the Division Chiefs and Deputies within CO-OPS to aid in communicating with employees during emergencies and contingent events. *None of the administrative processes listed require SSNs. SSNs have been deliberately removed from CO-OPS' administrative processes for some time now.*

Information is also collected by NOAA6205 web applications for external users requesting access to public facing data. These users are required to provide information to CO-OPS for contact purposes. The information that is stored in this system consists of the following - For partner vendors: Name (First and Last), Business Street Address, City, State, Country, Email, Phone Number, Organization or Business Name, Occupation, Contract Number, Project Number, Account Status and Application Date. For general public: Name (First, Last), Street Address, City, State, Country, Email, Phone Number, Organization, if applicable.

The information collected on external users requesting access to public facing data by NOAA6205 applications will only be accessible to CO-OPS users with appropriate roles and permissions to view the database table that contains these data elements. It will not be shared with any other organization or agency. This information is collected exclusively to determine eligibility to obtain access to certain data products.

Vendor provided BII is also collected in the form of contract Requests for Proposals (RFPs). These RFPs are stored electronically on the system until completion of reviews at which time non-selected RFPs are removed and the selected RFP is printed and stored in accordance with the record retention schedule.

Information is collected on CO-OPS users is automatically collected by the System for auditing purposes only when they access NOAA6205 systems. The information that is stored in this system consists of the following: User ID, IP Address, and Date/Time of Access.

In addition, CO-OPS utilizes a VPN over the Internet to connect the Chesapeake office to the Seattle and Silver Spring offices. By using a VPN, CO-OPS ensures that all data is encrypted while in transit between the offices, and transmission integrity is maintained.

The overall collection and storage of PII/BII is part of accomplishing the legislated mission of within CO-OPS.

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	
Contractors	X
Other (specify): General public access is limited to posting comments on the Web page.	

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://tidesandcurrents.noaa.gov/privacy.html

X	Yes, notice is provided by other means.	Specify how: Visitors to the CO-OPS web site can request information by submitting an email through an information request contact form. Individuals are under no obligation to provide any identifying information, and the details of how this information is handled are readily available via the CO-OPS Privacy Policy and a Privacy Act statement. CO-OPS staff members (employees) are provided notice via email of how PII is used (i.e., emergency contact information in case of emergency or disasters), CO-OPS' employees are also pointed to the Privacy Act Statement and Policy on the public facing website upon hire. CO-OPS staff members (employees) are provided notice of information to be collected from them upon hire as well as via COOPS Privacy Policy on the public-facing Web site to which they are directed. Staff members are notified upon request for collection of identifying information that they may decline to provide the information, but that in some instances it may affect their employment. Vendor provided BII is collected in the form of contract Requests for Proposals (RFPs). In addition to the CO-OPS Privacy Policy which govern how vendor PII/BII is maintained, Contracting Officers also stipulate how vendor PII/BII is disseminated via non-disclosure agreement and in accordance with privacy notices placed by the vendors in their proposals.
	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: Visitors to the CO-OPS web site can request information by submitting an email through an information request contact form. Individuals are under no obligation to provide any identifying information, and the details of how this information is handled are readily available via the CO-OPS Privacy Policy and a Privacy Act statement. CO-OPS staff members (employees) are provided notice via email of how PII is used (i.e., emergency contact information in case of emergency or disasters) upon hire as well as via COOPS Privacy Policy on the public-facing Web site to which they are directed. Staff members are notified upon request for collection of identifying information that they may decline to provide the

		information via email or verbally, to their supervisors, but that in some instances it may affect their employment. Vendors are also under no obligation to provide any identifying information. Information provided is voluntary in the form of an RFP in response to a solicitation.
	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 visitors to the CO-OPS site, the one purpose of collecting the information is described in the Privacy Act Statement. COOPS does not collect personally-identifiable information unless visitors choose to provide it to us. If information is provided us with personally identifiable information, for example by sending an e-mail or by filling out a form and submitting it through our Web site, we use that information only to respond to the message and to help provide visitors with the information and services that they request. Submitting voluntary information constitutes consent to the use of the information for the stated purpose. When a user clicks 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. As information gathered only has one particular use, managing administrative programs related to an employee or contractor's employment status, individuals have the opportunity to consent or decline upon request of the information. Vendor provided BII is collected in the form of contract Requests for Proposals (RFPs). In addition to the CO-OPS Privacy Policy which govern how vendor PII/BII is maintained, contracting officers also stipulate how vendor PII/BII is disseminated via non-disclosure agreement and in accordance with privacy notices placed by the vendors on their proposals.
	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: Visitors to the CO-OPS site provide current information when contacting us. CO-OPS staff members are queried on a quarterly basis, during which they can provide updates. Members of the public are not required or asked to provide any identifying information. Members of the public have an opportunity to update their PII at any time by providing updated information via email, phone or fax. Vendors have an opportunity to update their PII/BII by providing updated physical or electronic invoices, phone call or by updating information through another RFP when there is a new solicitation
	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: Only authorized individuals have access to the safe in which physical PII is stored. All electronic forms of PII is strictly monitored, tracked, and recorded by access controls in place on the System.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): November 4, 2014 ☐ 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). The privacy controls assessment that was submitted with this PIA was reviewed by the BCPO.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	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.

NOAA implements various controls and technologies used to protect PII/BII on NOAA6205. These controls are in place to ensure that the confidentiality, integrity, and availability of how PII/BII information is collected, maintained, and transmitted within the NOAA6205 is in accordance with the System's categorization level. For example, NOAA has implemented technologies such as control lists and user authorizations for access control. Additionally, through the Media and Backup Plan, NOAA has implemented controls to limit the retention and transmission of PII. Encryption and access controls also both protect PII/BII 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 the Public Requesting or Providing Information Related to NOAA's Mission; DEPT-18, Employees Information Not Covered by Notices of Other Agencies. Also, DEPT-2, Accounts Receivable; DEPT-6, Visitor Logs and Permits for Facilities under Department Control; and DEPT-13, Investigative and Security 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: 1609-06 in the NOAA Disposition Handbook
	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	
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: There is enough information to identify an individual
X	Quantity of PII	Provide explanation: There are less than 1000 records in all.
X	Data Field Sensitivity	Provide explanation: Phone numbers and email addresses are the primary information collected and are used for communication purposes.
X	Context of Use	Provide explanation: The user information has been provided voluntarily: from people within the organization for administrative purposes, by visitors to the public Web site, and by vendors who wish to bid on a solicitation.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Users are required to log into the application with a user name and password. The database fields that contain PII are encrypted
	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 Statement to the public facing Web site.
	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: Addition of Privacy Act Statement to the public facing Web site.
	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: Marian Westley Office: CO-OPS Phone: 240-533-0481 Email: Marian.westley@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: WESTLEY.MARIAN.B.1365896638 Digitally signed by WESTLEY.MARIAN.B.1365896638 Date: 2017.11.15 15:22:37 -05'00' Date signed:	**Information Technology Security Officer** Name: John Parker Office: NOS Phone: 240-533-0832 Email: john.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: 2017.12.06 02:24:19 -05'00' Date signed:
Authorizing Official Name: Richard Edwing Office: CO-OPS Phone: 240-533-0482 Email: Richard.edwing@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: EDWING.RICHARD.F.1365829620 Digitally signed by EDWING.RICHARD.F.1365829620 Date: 2017.11.27 14:37:36 -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: 2017 12 27 10:19:03 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: 02-2017

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
For the
Center for Operational Oceanographic Products and Services PORTS®
and NWLON IT System (NOAA6205)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA6205

Unique Project Identifier: NOAA6205

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 Ocean Service (NOS) Center for Operational Oceanographic Products and Services (CO-OPS) collects and distributes observations and predictions of water levels and currents to ensure safe, efficient and environmentally sound maritime commerce. CO-OPS establishes standards for the collection and processing of water level and current data, collects and documents user requirements which serve as the foundation for all resulting program activities, designs new and/or improved oceanographic observing systems, designs software to improve CO-OPS' data processing capabilities, maintains and operates oceanographic observing systems, performs operational data analysis/quality control, and produces/disseminates oceanographic products. CO-OPS is divided into four Divisions to address various functionally important areas. The divisions are Engineering (ED), Field Operations (FOD), Oceanographic (OD) and Information Systems (ISD). These users are internal to the system including federal employees and contractors. The CO-OPS PORTS® and NWLON System (NOAA6205) and the infrastructure components that stores, processes and transmits the information are the focus of this document and play an important role in NOAA's strategic goals to promote safe navigation and sustain healthy coasts. This system provides CO-OPS and its four divisions with general office automation, application management, network connectivity, file storage, process and workflow management, and application development functionality. NOAA6205 provides several applications for both in-house and external use. These applications run either on Linux or Windows-based platforms. All Linux or Windows-based platforms upon which these applications run are supported by NOAA6205. NOAA6205 has public web servers which provide limited external information to the public. This information has been reviewed and approved by CO-OPS. The data received by CO-OPS is used to ensure safe, efficient and environmentally sound maritime commerce, and provides real-time data to government agencies such as the U.S. Coast Guard, National Weather Service, U.S. Geological Survey, NOAA 1 HAZMAT and FEMA which use the data when maritime events occur. Non-government entities such as commercial shippers and harbor pilots use the data to avoid groundings and collisions.

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.

____ 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 NOAA6205 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 NOAA6205 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): Maurice McLeod

Signature of ISSO or SO: MCLEOD.MAURICE.STGEORGE.1267033699 Digitally signed by MCLEOD.MAURICE.STGEORGE.1267033699 Date: 2017.11.30 08:15:28 -05'00' Date: _____

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

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2017.12.06 02:12:37 -05'00' Date: _____

Name of Authorizing Official (AO): Richard Edwing

Signature of AO: EDWING.RICHARD.F.1365829620 Digitally signed by EDWING.RICHARD.F.1365829620 Date: 2017.11.30 08:41:51 -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: 2017.12.27 10:16:35 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Friday, December 29, 2017 1:11 PM
To:	Gioffre, Kathy (Federal); CPO
Cc:	Mark Graff NOAA Federal; Sallie Ahlert NOAA Federal; Joy Baker NOAA Federal
Subject:	NOAA8877 certification docs
Attachments:	NOAA8877 FY18 PTA 20171206 (1) mhg.pdf; NOAA8877 FY18 certification and PIA 20171206 mhg.pdf

Kathy, attached are a current PTA, and the certification with the re signed PIA attached to it.

ATO date is 5 31 18.

thx Sarah

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

NOAA OCIO
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: NOAA8877 FY18 PIA 20171206.pdf

FISMA Name/ID (if different): Radar Operations Cener Local Area Network (ROC LAN)/NOAA8877

Name of IT System/ Program Owner: Michael W. Miller

Name of Information System Security Officer: Sallie M. Ahlert

Name of Authorizing Official(s): Joseph A. Pica (NWS OBS) and Richard Varn (NWS ACIO)

Date of Last PIA Compliance Review Board (CRB): May 5, 2017

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

Date of PIA Review: December 6, 2017

Name of Reviewer: Sallie M. Ahlert, 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 (SO or ISSO):  Digitally signed by AHLERT.SALLIE.M.1365877706
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=AHLERT.SALLIE.M.1365877706
Date: 2017.12.07 13:12:37 -06'00'

Date of BCPO Review: 12.27.17

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: 2017.12.27 09:55:12 -05'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA8877
Radar Operations Center Local Area Network (ROC LAN)

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
NOAA8877 ROC LAN

Unique Project Identifier: 006-48-01-12-3103-00

Introduction: System Description

(a) General Description - NOAA8877 is a moderate impact General Support System (GSS), which provides a small to medium enterprise LAN for the National Oceanic and Atmospheric Administration (NOAA)/National Weather Service (NWS) Radar Operations Center (ROC) and its tri-agency personnel. The ROC's primary mission is to support operations, maintenance, and sustainment of the tri-federal agency (Department of Commerce (DOC), Department of Defense (DOD), and Department of Transportation (DOT)) Next Generation Weather Radar (NEXRAD) weather radar fleet. NOAA8877 provides general office collaboration software and tools together with highly specialized software and hardware systems, which enable ROC's personnel in four branches (Operations, Engineering, Program Support, and Applications) to perform their respective System Development Life Cycle (SDLC) functional roles. Operations Branch runs a 24x7 radar hotline, performs independent testing of modifications and software, and provides on-site technical field support for specialized and particularly difficult radar modifications. Engineering Branch does multi-year planning, project management, development, unit and integration testing, security design, and implementation for all the hardware and software modifications to the radar systems. Program Support Branch provides logistics support, contract maintenance, configuration management, and documentation. Applications Branch leads data quality analysis and improvement initiatives. In addition, this branch leads the scientific groups that make determination on readiness of new science for integration into the radar.

Information in the NOAA8877 ROC LAN general support system primarily consists of programmatic and technical documentation for the NOAA8104 NEXRAD, NOAA8212 Terminal Doppler Weather Radar Supplemental Product Generator (TDWR SPG), and NOAA3065 weather radar data major application programs. If any of the data is sensitive or For Official Use Only (FOUO) programmatic or technical data, then the data is restricted by drives and folders to only ROC personnel authorized to access the information.

(b) Typical Transaction - A typical transaction might be the initiation of a DOC or DOD performance evaluation. The appropriate forms are completed on the ROC team leader's P: drive. It will then be printed, hand-carried for signature, and then transferred as described via UPS. Alternately, the agency-specific secure electronic transfer procedure is followed.

Another transaction example might be the collection of an individual's or other entity's (member of the public, public organization, or private sector) name and email address (work or home, whichever is applicable), who visits the ROC website and voluntarily wishes to have a question answered. In addition, there are work-related secure ROC website databases that store radar system specific data, which may be accessed by tri-agency civilian and military personnel about the radar they are responsible to maintain and/or operate. Further, the field radar maintenance and/or operations personnel may voluntarily provide comments or corrections on technical

documentation. The information is collected only to the extent needed to answer the question(s) posed or to request clarifications, if necessary.

(c) Information Sharing\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 ROC LAN contains personally assigned network shares (P:\), which are accessible only by the person assigned the shared drive. Per ROC directives, DOC and DOD team leaders are required to use only their P: drive to initiate and prepare forms data necessary for awards and performance.

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.

DOD civilian and military performance and awards data initiated at the ROC is required per Air Force Directive-Instructions (AFIs) 36-2406, 36-2502, and 36-2606 to document the individual job performance. The transfer of the information is then submitted to the appropriate Air Force HR personnel via encrypted email or via UPS tracked package as per the applicable AFI.

In addition, the system collects PII of ROC personnel for purposes of emergency recall and ROC Continuity of Operations Planning (COOP). The emergency recall and COOP data is stored on a LAN shared drive only accessible by authorized personnel and on Federal Information Processing Standards (FIPS) 140-2 encrypted iron keys provided by the ROC LAN Information System Security Officer (ISSO) to the ROC director and branch chiefs for emergency recall.

The system collects information necessary to sponsor foreign visitors. The DOC International Affairs Office coordinates or provides oversight for these visits. The information collected includes the foreign visitor's name, date of birth, city and country of birth, and passport number. This information is stored, if required, on the P: drive only of the Program Branch Chief, who is the sponsor of foreign visitors. Foreign National visitors who have "Green Cards" are not required to submit this data. The information on foreign visitors is necessary to sponsor visitors to the ROC from foreign countries. The information on foreign visitors is required for obtaining approval from the Bureau Western Region Security Office (WRSO) in Seattle, Washington to ensure that the foreign visitor is authorized to enter the United States. This foreign visitor information is not disseminated or shared external to ROC.

(d) Authority - Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1151(Dissemination of Technological, Scientific, and Engineering Information)
- 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)
- DAO 207-12 Foreign Visitor and Guest Access Program

(e) Categorization - NOAA8877 ROC LAN 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):					

☒ 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		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 and credit card information, including truncated form: * Government only issued travel and purchase cards. ** DOD performance and award forms require the individual's SSN; DOC does not require it.					

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		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		f. Business Associates	x		
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	x	Online	
Telephone		Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus	x	Other Federal Agencies	x
State, Local, Tribal		Foreign (visitors)*	x		
Other (specify): * Foreign Visitors are foreign government representatives.					

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	
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):			

	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): For emergency recall and COOP			

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 information collected on DOD military and civilian personnel is used to complete military performance and promotion evaluation forms for Air Force personnel. The performance evaluations are required by Air Force Directive-Instruction (AFI) 36-2406 to document the individual's job performance. The performance or promotion evaluation is completed by the NWS or DOD supervisor, discussed with the military member, and securely emailed to Offutt Air Force Base (AFB) using the Common Access Card (CAC) Public Key Infrastructure (PKI) credentials or alternately via tracked UPS package. Once processed at Offutt, the form is returned to the ROC for final signatures and then emailed securely or hand-carried to Tinker Air Force Base (AFB), which has administrative responsibility for the DOD personnel at the ROC (*outside the ROC LAN boundary*). Tinker AFB electronically files a copy in the individual's personnel file and then sends the form to Randolph AFB for final disposition. Per Air Force direction, all forms are transmitted and signed electronically. This information is not shared with anyone beyond those that are required to process it within the respective agency.

Electronic personnel related forms of NOAA employees only are transferred to NOAA HR in bulk or on a case-by-case basis via DOC Accellion (for NOAA records only) or via tracked United Parcel Service (UPS) package. This information is not shared with anyone beyond those that are required to process it within the respective bureau.

The information on foreign visitors is required for obtaining approval from the Western Region Security Office (WRSO) in Seattle, Washington to ensure that the foreign visitor is authorized to enter the United States. This information is not shared outside of the system, by ROC.

NEXRAD technical documentation and telecommunications information is FOUO. The tri-agency (DoD, FAA, and DOC) maintenance or operations field personnel must request access and be authorized to access site specific data, which is maintained at the ROC. Their identifying information (name, work email, and work telephone number) are used to create an account.

Name and email (work or home, whichever is applicable) contact information is collected on a voluntary basis from anyone who makes a web query about the NEXRAD system on the ROC website feedback form. The information is requested in order to provide a response directly to the requestor or make clarifications, when necessary (members of the public, public organizations, private sector).

ROC collects PII of ROC personnel on a voluntary basis for purposes of emergency recall. Employees may decline. ROC collects PII of ROC personnel assigned by the director to the ROC COOP team for COOP recall purposes. COOP employees must provide their PII recall information to be assigned a COOP team role. The employee recall and employee COOP data is stored on a LAN shared drive only accessible by authorized personnel and on FIPS 140-2 encrypted iron keys provided by the ROC LAN ISSO to the ROC director and branch chiefs for emergency recall.

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			
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 WMFO Recruitment Analysis Data System (RADS). NOAA8877 uploads data in specified formats to RADS. Locally, data is segregated on the ROC LAN in specified LAN data stores. ROC LAN shared stores have media protection controls and user procedures in place to keep the data on the ROC LAN.
	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): DoD Military personnel for DoD Personnel Data.			

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.roc.noaa.gov/WSR88D/PAStatement_NOAA8877.aspx .	
x	Yes, notice is provided by other means.	Specify how: a. Web Inquiries –Notice is provided by a privacy statement on the Web site. b. Written notice is included on all personnel forms that employees complete. 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 ROC emergency recall and COOP, employees are asked permission in person when collecting the applicable information. All ROC personnel are informed of the intended purpose. d. Notice is provided verbally to a foreign visitor, by the U.S. sponsor or the DOC person staffing the DOC International Affairs Office, at the time of his/her appearance at the office, that completion of the information on the Foreign National Visitor and Guest Access request form is required for obtaining authorization for a visit.
	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. For web queries, providing PII/BII is voluntary to those wishing to receive a response. Feedback only to the ROC Webmaster may be provided anonymously. c. For the emergency recall roster, ROC personnel can inform their supervisor or administrative officer in person or in writing that they decline to provide PII/BII. COOP team employees must provide their recall information. If a COOP team member declines, they would not be able to perform the duties of this function for the ROC, and they would be removed from this

		role. b. For DOD personnel data, employees may opt not to provide PII/BII – at the time of the request, and 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 can be added without contacting employees. The performance record/information is required in order to conduct performance evaluations. d. Foreign visitors may, at the time of appearance at the DOC International Affairs Office, verbally decline to provide the information requested of them, either to their U.S. sponsor who completes the form, or to the DOC personnel staffing the office. However, refusal to supply the required data will result in being denied access to the Department or any of its bureaus.
	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. ROC web queries (requests for data or for access to site specific radar data): a Privacy Policy statement, stating that provision of the information implies consent to its use, is provided on the Web site. b. Employees may opt not to consent to use of PII/BII – at the time of the request to the personnel administration representative who is assisting them - but this information is needed for processing awards. c. For ROC employees' emergency recall and COOP, the information is used for only one the stated emergency recall purpose. d. Foreign visitors may, at the time of appearance at the DOC International Affairs Office, verbally decline consent to provide the information requested of them, either to their U.S. sponsor who completes the form, or to the DOC personnel staffing the office, but this information is needed for sponsoring them in the Department or any of its bureaus.
	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. Web queries: An individual can review a query before sending, but cannot review or update after submitting. b. Personnel records are obtained/reviewed through the respective DOD and DOC electronic official personnel folder secured repositories but updates must be provided to the servicing HR office.

		c. For Emergency and COOP information, the employee may not review the information, because it contains other staff's PII, but may provide updates to the assigned administrative staff. d. Foreign visitors may submit requests to review and update to the DOC International Affairs Office.
	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: Windows file system auditing monitors, tracks, and records changes to the files containing PII/BII. This does not track content changes.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): **5/26/2017 with DOC PO approved PIA 5/12/2017.** ☐ 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.
	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): As stated in the ROC 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 ROC Rules of Behavior (ROB) indicating that they have read and understand the ROB. In addition, as of September 2015, ROC LAN users review and acknowledge the current ROC ROB annually in concurrence with the release of the NOAA annual IT security awareness training. The Feb 2016 ROB update includes a section for PII definition, storage, sharing, and how to report PII incidents. To protect mobile information, all ROC 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.

Segregation of data with granularity of control on data shares to the user or group level, as appropriate. Controlled access for servers and data storage areas limited to only ROC LAN system administrators. FIPS 140-2 encryption for all mobile laptop devices. Rules of Behavior annual supplemental training on where to store PII and how to handle transfers locally and via DOC Accellion. Two specific scanner locations for PII that are not network connected and to ensure PII data is not emailed with multi-function scanner/copier.

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)*: For employee information, the applicable SORN is COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies. This covers all ROC employees. NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission. Specifically, the SORN covering the Foreign Visitor/Guest Information: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons--COMMERCE/DEPT-9.
	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 Specific Records Schedule 100-24 IT Operations and Management Records, General Record Schedule GRS-20 for general IT related data, NOAA 302-03 Personnel Actions, NOAA 600-07 Foreign Visitors, NOAA 1301-05 Sensors and Equipment Project Case Files, NOAA 1301-07 Radar Project Case Files
	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	
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: NOAA8877 ROC LAN does not have an aggregation of individual PII data, as would NOAA or DoD personnel systems and DOC financial and travel systems. There are no ROC personnel specific datasets on the ROC LAN that would expose all employees or make all employees easily identifiable. NOAA8877 does not have aggregations of PII on members of the public to support identifiability.
x	Quantity of PII	Provide explanation: NOAA8877 ROC LAN has fewer than 160 users total. Breakdown of ROC personnel is < 42% DOC and < 10% DoD. The impact as a result of loss of employee PII at the ROC is estimated to be minor and is anticipated to have limited adverse effect on continued performance of primary mission function.

x	Data Field Sensitivity	Provide explanation: Examples of the most sensitive situation examples would be ROC employee names and phone numbers on an emergency call roster, a list of the few ROC employee names and government purchase card numbers, or foreign government visitor information that is required to be kept by the ROC employee host. Release of employee or foreign visitors names and contact information would not likely cause harm to the individuals.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: End users do not access data (PII or otherwise) on NOAA8877, except with NOAA secured and encrypted assets approved for the specific purpose. Per rules of behavior, PII is accessed or used for its intended purpose on the system via directly connected nodes, and is not transferred to or transported on NOAA mobile devices. PII is established in designated/protected shared access folders and is made accessible only to those with a need to know.
x	Other:	Provide explanation: All end of life cycle NOAA8877 disks servers, multi-function copier/printers/faxes, and end user desktop/laptop components are wiped and shredded per policy and not reused in any manner.

Section 12: Analysis

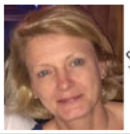
12.1 Indicate whether the conduct of this PIA results in any required business process changes.

x	Yes, the conduct of this PIA results in required business process changes. Explanation: More stringent privacy data related procedures were put in place to address gaps identified in NOAA8877 processes and technologies. Summary of adjustments is given below: • Administrative personnel were trained on use of two local PC/non-networked scanners to control transfer of personnel related PII into ROC LAN for eventual upload to NOAA WMFO or other appropriate HR systems. This avoids problems with PII on paper copies being scanned via multi-function copier, which can only send as email attachments to recipient. • Primary users of PII are administrative personnel, branch chiefs, and team leaders. They occasionally have need to share data in folders with others to continue processing of the paperwork, for submission, and/or for peer review purposes. These folders are designated on the ROC LAN as PII-Secured and locked down to specific users.
	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: USB connected scanners were added in two specific building locations to facilitate the transfer of potentially sensitive personnel data (awards, ratings, hiring, etc.) from paper copies to the system for processing in NOAA WMFO systems.
	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: Sallie M. Ahlert Office: DOC\NOAA\NWS\OBS1 (ROC) Phone: (405) 573-8870 Email: Sallie.M.Ahlert@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.  Sallie M. Ahlert Digitally signed by AHLERT.SALLIE.M.1365877706 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=AHLERT.SALLIE.M.1365877706 Date: 2017.12.07 13:12:06 -06'00'	**Information Technology Security Officer** Name: Joy Baker Office: DOC\NOAA\NWS\ACIO Phone: (228) 688-2801 Email: Joy.Baker@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. BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER.JOY.ALLISON.1269758577 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BAKER.JOY.ALLISON.1269758577 Date: 2017.12.07 13:30:44 -06'00'
Authorizing Official Name: Joseph A. Pica Office: DOC\NOAA\NWS\OBS Phone: (301) 427-9778 Email: Joseph.A.Pica@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. PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.12.21 08:49:58 05'00'	**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. 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: 2017.12.27 09:55:57 -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: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Radar Operations Center Local Area Network (ROC LAN)
NOAA8877
December 06, 2017

U.S. Department of Commerce Privacy Threshold Analysis

NOAA ROC LAN

Unique Project Identifier: NOAA8877

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: NOAA8877 is a General Support System (GSS), which provides a small to medium enterprise LAN for the NOAA\NWS ROC and its tri-agency personnel. The ROC's primary mission is to support operations, maintenance, and sustainment of the tri-federal agency (DOC, DOD, and DOT) NEXRAD weather radar fleet. NOAA8877 provides general office collaboration software and tools together with highly specialized software and hardware systems, which enable ROC's personnel in four branches (Operations, Engineering, Program Support, and Applications) to perform their respective System Development Life Cycle (SDLC) functional roles. Operations Branch runs a 24x7 radar hotline, performs independent testing of modifications and software, and provides on-site technical field support for specialized and particularly difficult radar modifications. Engineering Branch does multi-year planning, project management, development, unit and integration testing, security design, and implementation for all the hardware and software modifications to the radar systems. Program Support Branch provides logistics support, contract maintenance, configuration management, and documentation. Applications Branch leads data quality analysis and improvement initiatives. In addition, this branch leads the scientific groups that make determination on readiness of new science for integration into the radar. 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. *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 ROC LAN 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 ROC LAN 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): Michael W. Miller

Signature of ISSO or SO: MILLER.MICHAEL.W.1180644136 Digitally signed by MILLER MICHAEL W 1180644136 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn MILLER MICHAEL W 1180644136 Date 2017 12 06 16 35 34 06'00' Date: 12/6/2017

Name of Information Technology Security Officer (ITSO): Joy Baker

Signature of ITSO: BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER JOY ALLISON 1269758577 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BAKER JOY ALLISON 1269758577 Date 2017 12 07 07 39 04 06'00' Date: 12/7/2017

Name of Authorizing Official (AO): Joseph A. Pica

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.12.21 08:48:20 05'00' Date: 12/21/2017

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 2017 12 27 10 06 54 05'00' Date: 12.27.17

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, January 3, 2018 4:54 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA4500 certification, re signed PIA and current PTA which you don't need to sign
Attachments:	NOAA4500 PIA_12152017_MM (1).pdf; NOAA4500 Annual Review Certification Form_12062017 (1).pdf; NOAA4500_PTA_09122017_MM+smr+RM mhg.pdf

and the SAR Q4 FY17 and the Q1 FY17 SAR workbook (privacy only done in Q1) are in the PIA folder.

thx Sarah

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

NOAA OCIO
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: NOAA4500

FISMA Name/ID (if different): NOAA4500

Name of IT System/ Program Owner: NMFS West Coast Region

Name of Information System Security Officer: Michael McCully

Name of Authorizing Official(s): Scott Rumsey

Date of Last PIA Compliance Review Board (CRB): 11/29/2016

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

Date of PIA Review: 12/6/2017

Name of Reviewer: Michael McCully

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 (SO or ISSO): Digitally signed by MCCULLY.MICHAEL.JAMAAL.1380349554
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=MCCULLY.MICHAEL.JAMAAL.1380349554
Date: 2017.12.06 16:49:22 -08'00'

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: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
West Coast Region
NOAA4500

U.S. Department of Commerce Privacy Threshold Analysis

West Coast Region / NOAA4500

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:

NOAA Fisheries is dedicated to protecting and preserving our nation's living marine resources through scientific research, fisheries management, enforcement, and habitat conservation. The West Coast Region of NOAA Fisheries administers fisheries programs along the coasts of Washington, Oregon and California; and in the vast inland habitats of Washington, Oregon, California and Idaho. We work to conserve, protect, and manage salmon and marine mammals under the Endangered Species Act and Marine Mammal Protection Act, and sustainably manage West Coast fisheries as guided by the Magnuson-Stevens Fisheries Conservation Act. To achieve this mission and advance sound stewardship of these resources, we work closely with tribes, local, state and federal agencies, our stakeholders, and partners to find science-based solutions to complex ecological issues.

The NOAA4500 (West Coast Region [WCR] LAN) functions as the overall office automation support system for WCR, National Marine Fisheries Service (NMFS), National Oceanic Atmospheric Administration (NOAA) in multiple physical locations throughout the western United States.

The purpose of the NOAA4500 Information System is to provide access to automated systems typically found in administrative offices within the federal government. The Information System supports all offices within the WCR.

Authorizations and Permits for Protected Species (APPS)
The web based system contains applications for permits required by the Marine Mammal Protection Act (MMPA)and the Endangered Species Act (ESA). Researchers use the system to submit applications which contain PII (Employment and Education Information) prior to receiving research permit.

NOAA4500 System Maintenance Information

PII and BII information contained within the NOAA4500 system boundary provide the System Owner, ISSO, and administrators with the identity and contact information of all authorized users of the system. This information is used to reset passwords, notify users of outages, and support NOAA4500 COOP operations.

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.

____ 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.) Endangered Species Research Application Information.*

__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 NOAA4500 IT System.

- NOAA4500 will conduct a PIA.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA4500 IT 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): Michael McCully

Signature of ISSO or SO: Digitally signed by MCCULLY.MICHAEL.JAMAAL.1380349554 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=MCCULLY.MICHAEL.JAMAAL.1380349554 Date: 2017.09.12 09:33:00 -07'00' Date: 09/12/2017

Name of Information Technology Security Officer (ITSO): Richard Miner

Signature of ITSO: Digitally signed by MINER RICHARD SCOTT 13986 04519 Date: 2017 09 21 08:08:03 04'00' Date: 9/21/2017

Name of Authorizing Official (AO): Scott Rumsey

Signature of AO: Digitally signed by RUMSEY SCOTT M 1365888341 Date: 2017 09 20 10:27:40 07'00' Date: 09/20/2017

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 2017 09 21 10 10 10 04'00' Date: 9.21.17

Justin May - NOAA Affiliate

From:	Justin May NOAA Affiliate
Sent:	Thursday, January 4, 2018 12:49 PM
To:	Sarah Brabson NOAA Federal
Cc:	Frank Indiviglio; Hadona Diep NOAA Affiliate; Mark Graff NOAA Federal; Jean Apedo NOAA Federal
Subject:	Re: Status of NOAA0500 certification?
Attachments:	NOAA0500_PTA_Updated_14Dec17 fmi.pdf; NOAA0500 PIA_Annual_Review_Certification_Form 14Dec17_ISSO Signed.pdf

Sarah,

Please find the NOAA500 related PIA/PTA documents.

On Thu, Jan 4, 2018 at 10:38 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> NOAA0500 will be reviewed in a DOC CRB on jan 18 unless we can produce the certification. Does Doug have this one to (that is, the PIA to re sign)?
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> NOAA OCIO
> Governance and Portfolio Division
> Office 301 628 5751
> Ce (b)(6)

Justin May, CISSP
Engility
RDHPCS ISSO (Acting)
(m (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 Research & Development High Performance Computing System (R&D HPCS)

FISMA Name/ID (if different): R&D HPCS - NOAA0500

Name of IT System/ Program Owner: Frank Indiviglio

Name of Information System Security Officer: Justin May

Name of Authorizing Official(s): Zachary Goldstein

Date of Last PIA Compliance Review Board (CRB): 14 Mar 17

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

Date of PIA Review: 14 Dec 17

Name of Reviewer: Justin May

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 (SO or ISSO): MAY.JUSTIN.NATHANIEL.1039635980

Digitally signed by MAY.JUSTIN.NATHANIEL.1039635980
DN: c=MAY.JUSTIN.NATHANIEL.1039635980, c US, o U S Government, ou /CONTRACTOR
Reason I am the author of this document
Date 2017.12.14 22:29:20 -07'00'

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)

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, January 4, 2018 2:43 PM
To:	Gioffre, Kathy (Federal); CPO
Cc:	Mark Graff NOAA Federal
Subject:	NOAA4500 certification
Attachments:	NOAA4500 Annual Review Certification Form_12062017 (1) mhg.pdf; NOAA4500 PIA_12152017_MM (1) mhg.pdf; NOAA4500_PTA_09122017_MM+smr+RM mhg.pdf

Attached are the certification, the re signed PIA and the current PTA for NOAA4500.

thx Sarah

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

NOAA OCIO
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: NOAA4500

FISMA Name/ID (if different): NOAA4500

Name of IT System/ Program Owner: NMFS West Coast Region

Name of Information System Security Officer: Michael McCully

Name of Authorizing Official(s): Scott Rumsey

Date of Last PIA Compliance Review Board (CRB): 11/29/2016

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

Date of PIA Review: 12/6/2017

Name of Reviewer: Michael McCully

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 (SO or ISSO): Digitally signed by MCCULLY.MICHAEL.JAMAAL.1380349554
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=MCCULLY.MICHAEL.JAMAAL.1380349554
Date: 2017.12.06 16:49:22 -08'00'

Date of BCPO Review: 1/3/18

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 03 17 06 47 05'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
West Coast Region Local Area Network
NOAA4500

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

Version Number: 01-2015

U.S. Department of Commerce Privacy Impact Assessment
West Coast Region Local Area Network (LAN), NOAA4500

Unique Project Identifier: 006-48-01-14-02-3305-00

Introduction:

System Description

NOAA Fisheries is dedicated to protecting and preserving our nation's living marine resources through scientific research, fisheries management, enforcement, and habitat conservation. The West Coast Region of NOAA Fisheries administers fisheries programs along the coasts of Washington, Oregon and California; and in the vast inland habitats of Washington, Oregon, California and Idaho. We work to conserve, protect, and manage salmon and marine mammals under the Endangered Species Act and Marine Mammal Protection Act, and sustainably manage West Coast fisheries as guided by the Magnuson-Stevens Fisheries Conservation Act. To achieve this mission and advance sound stewardship of these resources, we work closely with tribes, local, state and federal agencies, our stakeholders, and partners to find science-based solutions to complex ecological issues.

The NOAA4500 (West Coast Region [WCR] LAN) functions as the overall office automation support system for WCR, National Marine Fisheries Service (NMFS), National Oceanic Atmospheric Administration (NOAA) in multiple physical locations throughout the western United States.

The purpose of the NOAA4500 Information System is to provide access to automated systems typically found in administrative offices within the federal government. The Information System supports all offices within the WCR.

Authorizations and Permits for Protected Species (APPS)
The web based system contains applications for permits required by the Marine Mammal Protection Act and the Endangered Species Act. Researchers use the system to submit an application for a scientific research permit.

NOAA4500 System Maintenance Information
PII and BII information contained within the NOAA4500 system boundary provide the System Owner, ISSO, and administrators with the identity and contact information of all authorized users of the system. This information is used to reset passwords, notify users of outages, and support NOAA4500 COOP operations.

Information Sharing:

Authorizations and Permits for Protected Species (APPS)
Researchers may include a curriculum vitae or resume with their application. Information collected is not shared outside of NOAA4500.

In the event that the agency initiates an enforcement action against a permit holder, PII/BII may be used by the Department of Justice (DOJ in litigation and/or criminal law enforcement actions. In the event that a civil enforcement case is brought against a permit holder, the agency may share PII/BII with DOJ.

NOAA4500 System Maintenance Information
NOAA4500 does not share any of the Federal or Contractor employee information provided outside of NOAA.

Authorities:

Authorizations and Permits for Protected Species (APPS)
The Endangered Species Act of 1973 and the Marine Mammal Protection Act of 1972, amended 1994, require us to validate the researcher's qualifications for conducting research on protected species. Fishing permits under the Magnuson-Stevens Act are handled through a separate permit process.

NOAA4500 System Maintenance Information
5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

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. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-		e. New Public Access		h. Internal Flow or	

Anonymous				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	X	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):					

*Researcher resumes

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):					

*IP Addresses are collected for anyone logging on to APPS with a user name and password. We do not collect this information if the person does not log in and is accessing only the publicly available sections of the application. IP addresses are collected for federal employees and staff when logging into NOAA4500 for administrative purposes.

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		Email	X		
Other (specify):					

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

Non-government Sources					
Public Organizations	X	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	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
		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).

Authorizations and Permits for Protected Species (APPS)
The PII/BII collected by the IT system is from federal and state employees, members of the public, and employees/members of Tribal Nations. The information is used to verify that the individual has the necessary qualifications to conduct research on protected species. Applicants provide a curriculum vitae or resume documenting their academic and/or work related experience with the methods and procedures they plan to use on protected species.

In the event that the agency initiates an enforcement action against a permit holder, PII/BII may be used by the Department of Justice (DOJ in litigation and/or criminal law enforcement actions. In the event that a civil enforcement case is brought against a permit holder, the agency may share PII/BII with DOJ.

NOAA4500 System Maintenance Information
Federal and Contractor Employee data:

- Names, addresses, and email addresses collected from employees and contractors are used to manage account information for access control to systems and web applications.
- Names and work email addresses of employees and contractors are used to direct the public to appropriate personnel within the organization.

For emergency, disaster recovery, and continuity of operations, employee and contractor names, work and home emails and work and home telephone numbers are collected.

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	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			

Other (specify):			

*DOJ if a criminal case resulting from research activity

	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://apps.nmfs.noaa.gov/docs_cfm/privacy_statement.cfm	
X	Yes, notice is provided by other means.	Specify how: NOAA4500 System Maintenance Information: Information collected for employee/contractor emergency contact, and disaster recovery/continuity of operations is requested in writing by the employee/contractor's supervisor. Information collected for account management is requested in writing or via email by the user's supervisor, at the time that the user requests an account on the information system.
	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: Authorizations and Permits for Protected Species (APPS): The Endangered Species Act and Marine Mammal Protection Act require the applicant provide evidence of their qualifications. The individual would decline to provide PII/BII by not submitting information on his/her qualifications, and thus the application would be denied.. NOAA4500 System Maintenance Information: Employees may decline to provide PII /BII for emergency contact and disaster recovery by not filling in the PII/BII information. However, they will not be included in the contacts in case of emergency. Employees may decline to provide account information by not applying for an account, but this may be required for their job duties.
	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: When the applicant signs the permit applicant, he/she is consenting to the use of the PII/BII for the sole purpose of processing the application. NOAA4500 System Maintenance Information: Where specified in NOAA WFMO forms (http://www.wfm.noaa.gov/forms/noaa forms.html), employees have the opportunity to consent to particular use of their PII/BII. Employee and contractor General Personal Data information is required for badging and emergency notifications but users may decline in writing to their supervisors to provide COOP info. Employees and contractors are informed of the use of their data, and these data are not used for any other purpose.
	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:

	them.	Authorizations and Permits for Protected Species (APPS): Applicant information (e.g. address, phone, CV or resume) is automatically updated when profile information is updated via website. NOAA4500 System Maintenance Information: Instructions for updating contact information fields are provided in the forms the customer fills out. NOAA Employees can update PII for COOP and Emergency contact information on an as needed basis, by a written update/ request to their supervisors.
	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: NOAA4500 locations where PII/BII is present are monitored for successful and failed logons. Database activity is audited, stored locally and reported to the NOAA Security Operations Center (SOC).
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): November 20, 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). The privacy controls assessment submitted with this PIA has been reviewed by the BCPO.
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.
X	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.

Authorizations and Permits for Protected Species (APPS): NOAA Fisheries protects PII stored in APPS by minimizing the use and collection of PII. NOAA Fisheries also protects PII stored in APPS by controlling access to the information. APPS requires users to authenticate their identity by entering a username and password. NOAA4500 System Maintenance Information: NOAA4500 utilizes Data Resource Accounts and Group Memberships allow authorized staff to access NOAA4500 Data which may contain PII or BII. Computer account types include, but, are not limited to, Domain Accounts, Email/LDAP Accounts, Unix Accounts, Intranet Accounts, and Local System Accounts. Group memberships are used to assign Security Access Levels to authorized Data Resource Accounts. NOAA4500 applies Least Privilege and Least Functionality principles when providing security clearance. Access Enforcement Mechanisms (Encryption-at-Rest, Encryption-in-Transit, Distributed Directory Services) are implemented to prevent malicious or accidental access by unauthorized persons.

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)*: Authorizations and Permits for Protected Species (APPS): Commerce/NOAA-12 - COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Exempted Applicants http://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/noaa-12.html NOAA4500 System Maintenance Information: - Commerce/Department 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: Authorizations and Permits for Protected Species (APPS): - NOAA Records Schedule Chapter 1500 - Marine Fisheries, Section 1514-01. Available at http://www.corporateservices.noaa.gov/audit/records_management/schedules/ NOAA4500 System Maintenance Information: - GRS 1: Civilian Personnel Records, - GRS 3.1 General Technology Management Records, Item 040: Information technology oversight and compliance records, - GRS 3.2 Information Systems Security Record, Items 030, 031: System access records, - NOAA Records Schedules 1406-01: In Situ and Remotely Sensed Environmental Data; 1406-02, Order Processing Information Systems, 1406-03, Metadata Management Database
	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.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: The PII we collect does not include Sensitive

		Identifying Numbers or Distinguishing Features/Biometrics – or any other sensitive PII or BII.
X	Data Field Sensitivity	Provide explanation: Much of the information we collect (e.g. name, address, phone number) is available through business and phone directories.
X	Context of Use	Provide explanation: The information is used by NMFS to verify that the individual has the necessary qualifications to conduct research on protected species.
X	Obligation to Protect Confidentiality	Provide explanation: The Endangered Species Act of 1973 and the Marine Mammal Protection Act of 1972
	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: Michael McCully
Office: NOAA Fisheries, West Coast Region
Phone: 206-518-2347
Email: Mike.McCully@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: MCCULLY.MICHAEL.JAMAAL.1380349554 Digitally signed by MCCULLY.MICHAEL.JAMAAL.1380349554 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=MCCULLY.MICHAEL.JAMAAL.1380349554 Date: 2017.12.13 01:26:27 -08'00'

Date signed: 12/12/2017

Information Technology Security Officer

Name: Catherine Amores
Office: NOAA, 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: 2018.01.02 11:15:53 05'00'

Date signed: 1/2/2017

Authorizing Official

Name:
Office:
Phone:
Email:

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: Scott Rummy

Date signed: 12/15/2017

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: 2018.01.03 17:06:00 -05'00'

Date signed: 447892

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
West Coast Region
NOAA4500

U.S. Department of Commerce Privacy Threshold Analysis

West Coast Region / NOAA4500

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:

NOAA Fisheries is dedicated to protecting and preserving our nation's living marine resources through scientific research, fisheries management, enforcement, and habitat conservation. The West Coast Region of NOAA Fisheries administers fisheries programs along the coasts of Washington, Oregon and California; and in the vast inland habitats of Washington, Oregon, California and Idaho. We work to conserve, protect, and manage salmon and marine mammals under the Endangered Species Act and Marine Mammal Protection Act, and sustainably manage West Coast fisheries as guided by the Magnuson-Stevens Fisheries Conservation Act. To achieve this mission and advance sound stewardship of these resources, we work closely with tribes, local, state and federal agencies, our stakeholders, and partners to find science-based solutions to complex ecological issues.

The NOAA4500 (West Coast Region [WCR] LAN) functions as the overall office automation support system for WCR, National Marine Fisheries Service (NMFS), National Oceanic Atmospheric Administration (NOAA) in multiple physical locations throughout the western United States.

The purpose of the NOAA4500 Information System is to provide access to automated systems typically found in administrative offices within the federal government. The Information System supports all offices within the WCR.

Authorizations and Permits for Protected Species (APPS)
The web based system contains applications for permits required by the Marine Mammal Protection Act (MMPA)and the Endangered Species Act (ESA). Researchers use the system to submit applications which contain PII (Employment and Education Information) prior to receiving research permit.

NOAA4500 System Maintenance Information

PII and BII information contained within the NOAA4500 system boundary provide the System Owner, ISSO, and administrators with the identity and contact information of all authorized users of the system. This information is used to reset passwords, notify users of outages, and support NOAA4500 COOP operations.

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.

____ 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.) Endangered Species Research Application Information.*

__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 NOAA4500 IT System.

- NOAA4500 will conduct a PIA.

_____ I certify the criteria implied by the questions above **do not apply** to the NOAA4500 IT 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): Michael McCully

Signature of ISSO or SO: Digitally signed by MCCULLY.MICHAEL.JAMAAL.1380349554 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=MCCULLY.MICHAEL.JAMAAL.1380349554 Date: 2017.09.12 09:33:00 -07'00' Date: 09/12/2017

Name of Information Technology Security Officer (ITSO): Richard Miner

Signature of ITSO: Digitally signed by MINER RICHARD SCOTT 13986 04519 Date: 2017 09 21 08:08:03 04'00' Date: 9/21/2017

Name of Authorizing Official (AO): Scott Rumsey

Signature of AO: Digitally signed by RUMSEY SCOTT M 1365888341 Date: 2017 09 20 10:27:40 07'00' Date: 09/20/2017

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 2017 09 21 10 10 10 04'00' Date: 9.21.17

Mark Graff - NOAA Federal

From:	Mark Graff NOAA Federal
Sent:	Thursday, January 4, 2018 3:13 PM
To:	Robert Swisher NOAA Federal; Ed Kearns NOAA Federal; Sarah Brabson NOAA Federal; Robert Hembrook NOAA Federal
Cc:	Eric Williams NOAA Affiliate
Subject:	December Monthly Privacy Report
Attachments:	Group Communication Security Policy.docx; PTA PIA Management Report (17).xlsx; DOC SORN Status Sheet_NOAA.xlsx

Hey Everyone,

(Adding Robert H. due to the Group Communications Security Policy reference).

Let me know if you guys are ok with this report as is or if anyone has any changes they see that could improve it:

> Good Afternoon,
>
> This is a report regarding the activities of the NOAA Privacy Program from December 1-December 31, 2017. Attached are two spreadsheets outlining the status of SORNs, PIAs, and PTAs within NOAA.
>
> Some of highlights of the Program's activities for the month include:
>
> - NOAA Privacy has begun the briefing process for the NOAA Group Communications Security Policy. The Policy would require NOAA users to add additional security measures, such as participant registry or conference call locking, when discussing Sensitive PII or other matters considered to fall within the NARA guidance on Controlled Unclassified Information. A draft of the Policy is attached for your reference.
> - NOAA has begun its first round of re-Certifications for FISMA Systems that already have a DOC-approved PIA in place and have not undergone changes that impact privacy since the last PIA approval. The process has been significantly more streamlined and does not require a DOC Compliance Review Board. NOAA still has 2 systems that collect PII that are operating without a DOC-approved PIA.
>
> NOAA Privacy has agreed to help lead the DOC tabletop exercise for Privacy Incidents planned to take place in early 2018. The exercise is intended to examine problematic areas in coordinating a well-structured response to Moderate or High Privacy incident under the DOC Breach Response and Notification Plan. DOC's commencement of tabletop exercise activities is consistent with the new requirements imposed by the revisions to OMB Circular A-130.

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

STATUS OF NOAA SYSTEMS OF RECORD NOTICES (SORN)

SORN	Title/Purpose	Date SORN Previously Published	Date Sent to DOC
NOAA 1	Applications for NOAA Corps	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 3	Commissioned Officer Official Personnel Folders	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 5	Fisheries Law Enforcement Cases (Address Update)	8/10/2007 (72 FR 45009)	5/30/2013

NOAA 6	Fishermen's Statistical Data	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 10	NOAA Diving Program	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 11, NOAA Mailing Lists	Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.	NA	5/30/2013
NOAA 12	Marine Mammals, Endangered and Threatened Species, Permits and Exemptions (Amendment)	8/10/2007 (72 FR 45009)	2008
NOAA 13	Records of the Regional Fishery Management Councils	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 14	Dr. Nancy Foster Scholarship Program	2005	8/22/2014
NOAA 15	Observation Privacy Act System of Records Notice 2	10/17/2002 (67 FR 64086)	5/30/2013
NOAA 16	Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska (first published as Crab Economic Data Report for Bering Sea/Aleutian Islands Management Area (BSAI) off the coast of Alaska, now including two newer economic data report collections)	3 3 2005 (70 FR 10360)	5/30/2013

NOAA 19	Permits and Registrations for United States Federally Regulated Fisheries	4 17 2008/73 FR 20914	5/30/2013
NOAA 20	SARSAT	4 17 2008/73 FR 20914	5/5/2016
NEW NOAA 21	Fisheries Finance Program	NA	2008
NEW NOAA 22	NOAA Health Service Questionnaire	NA	2008
NEW NOAA 23	West Coast Region Economic Data Reports	NA	12/23/2014
		NA	3/9/2017

NEW DEPT 29	UAS	

2015-16 status at DOC
Published 11/25/15; effective 1/19/16
Published 5/5/16; effective 6/14/16
Added missing info and returned to DOC 3 8 16. 4 13 16, DOC decided that it should be a complete update. OLE completed updates 6 16 16; I cleaned up and sent 2 outstanding minor questions, 6 17 16. At one time it had been thought to separate out GC files into another SORN, but it was decided not to. To DOC 6 20 16. Responded to edits and comments rec'd 6 29 16, on 6 30 16, and added the new volunteer routine use. 6 30 17: now at Assistant General Counsel for Legislation, Regulation, and Oversight

MHG completed review 5 22 17; few edits, added volunteer routine use and put in new template, 5 25 17; sent to DOC same day. In new template to DOC 10 14 17
To DOC 12 13 16
Published 10/9/15; effective 11/23/15. Second amended version published 1-12-17. Another amended version to OPOG 6 26 17
Published July 8, 2016. Became effective August 17, 2016.
Published 9/17/15; effective 10/28/15
Published 7/31/2014; effective 09/02/2014
Published 10/9/15;effective 11/23/15

Published 8/7/2015. effective 9/15/15
Amended SORN published 1-12-17
Published July 8, 2016. Became effective August 17, 2016.
Published 1/19/16; effective 3/1/2016
Published 8-7-15; effective 9/15/15

Pending; Expedited Review Memorandum under consideration

(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)

(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, January 5, 2018 10:15 AM
To:	Robert Swisher NOAA Federal
Cc:	Ed Kearns NOAA Federal; Sarah Brabson NOAA Federal; Robert Hembrook NOAA Federal; Eric Williams NOAA Affiliate
Subject:	Re: December Monthly Privacy Report
Attachments:	NOAA8860_PTA_2017 03 08_v02_FOR_CPO mhg.pdf

Will do

(b)(5) [redacted]

Sarah, my suggestio (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 Fri, Jan 5, 2018 at 9:46 AM, Robert Swisher NOAA Federal <robert.swisher@noaa.gov> wrote:

> Looks good to me Mark....let me know if we need to do any escalation on the 3 REDS on the PTA/PIA Management Report.

On Thu, Jan 4, 2018 at 3:12 PM, Mark Graff NOAA Federal <mark.graff@noaa.gov> wrote:

> Hey Everyone,
>
> (Adding Robert H. due to the Group Communications Security Policy reference).
>
> Let me know if you guys are ok with this report as is or if anyone has any changes they see that could improve it:
>
> Good Afternoon,
>
> This is a report regarding the activities of the NOAA Privacy Program from December 1-December 31, 2017. Attached are two spreadsheets outlining the status of SORNs, PIAs, and PTAs within NOAA.
>
> Some of highlights of the Program's activities for the month include:
>
> - NOAA Privacy has begun the briefing process for the NOAA Group Communications Security Policy. The Policy would require NOAA users to add additional security measures, such as participant registry or conference call locking, when discussing Sensitive PII or other matters considered to fall within the NARA guidance on

Controlled Unclassified Information. A draft of the Policy is attached for your reference.

- NOAA has begun its first round of re-Certifications for FISMA Systems that already have a DOC-approved PIA in place and have not undergone changes that impact privacy since the last PIA approval. The process has been significantly more streamlined and does not require a DOC Compliance Review Board. NOAA still has 2 systems that collect PII that are operating without a DOC-approved PIA.

NOAA Privacy has agreed to help lead the DOC tabletop exercise for Privacy Incidents planned to take place in early 2018. The exercise is intended to examine problematic areas in coordinating a well-structured response to Moderate or High Privacy incident under the DOC Breach Response and Notification Plan. DOC's commencement of tabletop exercise activities is consistent with the new requirements imposed by the revisions to OMB Circular A-130.

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

Rob Swisher
Director, Governance and Portfolio Division
NOAA OCIO
W 301 628 5755
(b)(6)

Version Number: 01-2015

U.S. Department of Commerce
NOAA – National Weather Service

Privacy Threshold Analysis
for the
Weather and Climate Computing Infrastructure Services (WCCIS)
(NOAA8860)

Prepared: 03/2017

U.S. Department of Commerce Privacy Threshold Analysis

NOAA Weather and Climate Computing Infrastructure Services (WCCIS)

Unique Project Identifier: NOAA8860

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: NOAA8860 is comprised of seven critical sub-systems which are NCEP Central Operations (NCO), Weather and Climate Operational Supercomputing System (WCOSS), Weather Prediction Center (WPC), Ocean Prediction Center (OPC), Environmental Modeling Center (EMC), Climate Prediction Center (CPC) and the National Hurricane Center (NHC). All of the sub systems are located in College Park Maryland except NHC, which is located in Miami Florida.

NCO
Provides the means for project managers, program managers, administrators, Meteorologist, Mathematician, Hydrologists, Oceanographers, Support Physical Scientist and administrative support personnel to process and analyze data in a systematic comprehensive, accurate, clear and manageable manner.

WCOSS
The Weather and Climate Operational Supercomputing System (WCOSS), located: in Reston, VA; Orlando, FL - provides an advanced numerical modeling platform to the organizational elements of NWS to satisfy their operational requirements and to support their transitional development activities in the areas of meteorology, hydrology, and oceanography. Daily operational requirements consist of executing large-scale numerical weather models, processing data from weather satellites, radiosondes and commercial aircraft, and generating numerous graphical output products. The products generated by these activities provide public weather services to general users, warning of severe weather threatening life and property, and specialized services to other agencies and commercial users.

WPC

Provides forecast, guidance, and analysis products and services to support the daily public forecasting activities of the National Weather Service (NWS) and its customers, as well as tailoring support to other government agencies in emergency and special situations.

OPC
Originates and issues marine warnings and forecasts and continually monitors and analyzes maritime data. Guidance on marine atmospheric variables is provided to National Weather Forecast Offices with offshore and coastal responsibilities and other marine related programs, including direct support for all national and international marine users.

EMC
Develops numerical models to provide model-based forecast guidance for weather, marine, and climate forecasts at NCEP and the National Weather Service. In support of this mission, EMC a) improves the NWS numerical models through a broad program of research in data assimilation and modeling, b) develops, improves, and monitors operational data assimilation systems and models of the atmosphere, ocean, and land and c) pursues its research and development program internally as well as cooperatively with scientists from Universities, NOAA Laboratories and other government agencies, and the international scientific community

CPC
Provides climate services to the users in federal state, and local governments and the research community. Services include prediction of climate variability, monitoring of the climate system, development of databases for determining current state of climate, and analysis and assessment of origins of climate anomalies and their linkages to the rest of the climate system. CPC activities and interests cover time scales ranging from weeks to seasons and include land, ocean, and atmosphere extending from surface into the stratosphere.

NHC
Issues forecast advisories, watches, warnings for tropical cyclones over the Atlantic (including the Gulf of Mexico and Caribbean) basin and the eastern Pacific basin east of 140 degrees west longitude. NHC backs up the Central Pacific Hurricane Center for tropical cyclones forecasts, watches and warnings from 140 degrees west longitude to the dateline. The Tropical Analysis and Forecast Branch of the NHC operate 24 hours/day every day. NHC conducts tropical weather analysis, weather discussions, issue marine forecasts and warnings for the Atlantic, the eastern north Pacific and portions of the eastern South Pacific Ocean.

NIDS
The development environment is a virtual environment to allow development of new applications and updates to existing applications. Staging is a testing area for applications prior

to being put on Production. It is here in which the applications are tested to meet the CIA requirements of the Production NIDS.

IDP

The Integrated Dissemination Program (IDP) is a web application hosting environment located at the NCWCP in College Park, MD and Boulder CO. All applications hosted in IDP must be compliant with the security policy documented in the IDP Software Onboarding Process. IDP-hosted applications inherit security controls that are system-specific to the IDP web-hosting environment. IDP-hosted applications are also individually documented with the security controls that are implemented to secure each web application.

VoIP

The NCO Voice-Over-IP (VoIP) system supports voice telephony services - including voice mail - for the entire NCEP College Park facility. The VoIP system is housed in a government-owned building located at 5830 University Research Center, College Park MD, 20740. This building is occupied by government, contractor, and authorized security and facilities management personnel.

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..."

__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 [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):
_____

Signature of ISSO or SO: KYGER.BEN.K.1365887310 Digitally signed by KYGER.BEN.K.1365887310 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=KYGER.BEN.K.1365887310 Date: 2017.03.09 07:53:34 05'00' Date: 3/9/17

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE ANDREW PATRICK 1472149349 DN: c=US, o=U S Government, ou=DoD, ou=PKI, ou=OTHER, cn=BROWNE ANDREW PATRICK 1472149349 Date: 2017 03 10 08:58:38 05'00' Date: _____

Name of Authorizing Official (AO): _____

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: 2017.05.10 10:22:56 -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: 2017.05.10 10:54:59 -04'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Monday, January 8, 2018 12:28 PM
To:	Mark Graff NOAA Federal
Subject:	NOAA0200 PTA for your signature
Attachments:	NOAA0200 Privacy Threshold Analysis V.03 2017_08032017 AO signed.pdf

Doug signed this quite some time ago but I obviously lost track. OCIO PTAs and PIAs, I need to focus harder on.

Anyway, the attached appears correct.

thx Sarah

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

NOAA OCIO
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:	Tuesday, January 9, 2018 9:46 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA0200 PTA for your signature
Attachments:	NOAA0200 Privacy Threshold Analysis V.03 2017_08032017 AO signed mhg.pdf

Looks good here it is signed.

I can't tell you how many of these kinds of "geez, I forgot about this one" issues are cropping up on the FOIA taskings side. Totally understand.

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

On Tue, Jan 9, 2018 at 9:37 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> I don't believe I received this after Doug signed, but I still lost track that it needed to be renewed. thx
>
> Forwarded message
> From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
> Date: Mon, Jan 8, 2018 at 12:28 PM
> Subject: NOAA0200 PTA for your signature
> To: Mark Graff NOAA Federal <mark.graff@noaa.gov>
>
> Doug signed this quite some time ago but I obviously lost track. OCIO PTAs and PIAs, I need to focus harder on.
>
> Anyway, the attached appears correct.
>
> thx Sarah
>
> Sarah D. Brabson
> IT Infrastructure Investment Program Manager
> PRA Clearance Officer
>
> NOAA OCIO
> Governance and Portfolio Division

Office 301 628 5751
Ce (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)

U.S. Department of Commerce (DOC)
National Oceanic and Atmospheric Administration (NOAA)
Office of the Chief Information Officer (OCIO)
Information Technology Security Program (ITSP)

Privacy Threshold Analysis
For the
NOAA Network Operations Center (NOC)
(NOAA0200)

Prepared by

Office of the Chief Information Officer (OCIO)

Version 03-2017

August 3, 2017

U.S. Department of Commerce Privacy Threshold Analysis

NOAA0200 NETWORK OPERATIONS CENTER (NOC)

Unique Project Identifier: NOAA0200

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 NOAA Network Operations Center (NOC) is housed at the Silver Spring Metro Center (SSMC) campus in SSMC Building 3, located at 1315 East West Highway, Silver Spring Maryland. The NOC is staffed Monday through Friday from 6:30 AM through 6:30 PM ET. Emergency support is provided via mobile phone and pager, 24 hours a day, 7 days a week.

The NOAA NOC provides an interconnection between NOAA0200 and other NOAA IT systems and facilitates standardization of data transport and network services. The benefit to NOAA organizations is streamlined operations resulting in cost reduction. Additionally, this allows NOAA organizations to utilize the Intrusion Detection Systems services and Incident Response Capability of the NOAA Computer Incident Response Team (N-CIRT, NOAA0100).

- Provide management of the campus backbone routers and monitor the devices directly connected to these routers.
- Resolve network-related issues through fault management and provides a single point of contact by phone or email, and help desk/trouble ticketing system to manage call placement and problem resolution.
- Interoperate with SSMC LAN administrators, MAN/WAN groups, and remote sites.
- Recover from disasters, prevent unauthorized access, and alert LAN administrators of security-related issues through security management.
- Manage network assets, cable utilization, and IP address use through IP and configuration management.
- Produce and manage real-time performance statistics to address performance-related issues, and make recommendations for performance improvements.

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. *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.

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 NOAA NETWORK OPERATIONS CENTER (NOC) 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 NOAA NETWORK OPERATIONS CENTER (NOC) 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): Kevin Mitchell

Signature of ISSO or SO: MITCHELL.KEVIN.A.1398622886 Digitally signed by MITCHELL.KEVIN.A.1398622886 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=CONTRACTOR, cn=MITCHELL.KEVIN.A.1398622886 Date: 2017.08.01 13:41:25 04'00' Date: _____

Name of Information Technology Security Officer (ITSO): Jean Apedo

Signature of ITSO: JONES.JAMES.IV.1049453465 Digitally signed by JONES.JAMES.IV.1049453465 Date: 2017.08.10 10:35:47 -04'00' Date: _____

Name of Authorizing Official (AO): Doug Perry

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=PERRY.DOUGLAS.A.1365847270 Date: 2017.08.24 08:13:56 04'00' Date: _____

Name of Privacy Officer: Mark Graff

Signature of 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: 2018.01.09 09:41:29 05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Tuesday, January 9, 2018 9:38 AM
To:	Mark Graff NOAA Federal
Subject:	Fwd: NOAA0200 PTA for your signature
Attachments:	NOAA0200 Privacy Threshold Analysis V.03 2017_08032017 AO signed.pdf

I don't believe I received this after Doug signed, but I still lost track that it needed to be renewed. thx

Forwarded message
From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Mon, Jan 8, 2018 at 12:28 PM
Subject: NOAA0200 PTA for your signature
To: Mark Graff NOAA Federal <mark.graff@noaa.gov>

Doug signed this quite some time ago but I obviously lost track. OCIO PTAs and PIAs, I need to focus harder on.

Anyway, the attached appears correct.

thx Sarah

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

NOAA OCIO
Governance and Portfolio Division
Office 301 628 5751
Ce (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)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Mark Graff - NOAA Federal

From: Mark Graff NOAA Federal

Sent: Tuesday, January 9, 2018 1:47 PM

To: Catherine Amores NOAA Federal; Mary Wohlgemuth NOAA Federal; Wendy Holmes NOAA Affiliate; Anthony Hammond NOAA Affiliate; Scott Leonard NOAA Federal; Albert McMath NOAA Federal; Joe Maniscalco NOAA Federal; Thomas Heinrichs NOAA Federal; Juanita Sandidge NOAA Federal; Joe Brust; Thomas Renkevens NOAA Federal; Ron Mahmot NOAA Federal; John Clark NOAA Federal; Alan Hall NOAA Federal; Ajay Mehta NOAA Federal; Andre Hammond NOAA Federal; Chris Sisko NOAA Federal; Marc Moser NOAA Federal; Larry Ledlow NOAA Federal; Marge Ripley NOAA Federal; James Valenti NOAA Federal; Victor Kalu NOAA Federal; Thomas Narow NOAA Affiliate; David Garcia NOAA Affiliate; Shawnn Shears NOAA Federal; James Schreiber NOAA Federal; Charles Obenschain NOAA Federal; Brian Little NOAA Federal; Scott Koger NOAA Affiliate; Isaac Sanvee NOAA Affiliate; Jeffrey VanDam NOAA Affiliate; John Sanns NOAA Federal; Mark Hall NOAA Federal; Kenneth Haywood NOAA Federal; Kris Tai NOAA Affiliate; Matthew Jochum NOAA Federal; Marcus Ertle NOAA Federal; William Wooten Janney NOAA Affiliate; Sherry Goynes NOAA Affiliate; Jason Symonds NOAA Federal; Ericka EvansSterling NOAA Affiliate; Mark Paese NOAA Federal; Vanessa Griffin NOAA Federal; Steven Cooper NOAA Federal; Juliana Blackwell NOAA Federal; Larry Tyminski NOAA Federal; Bill Lapenta NOAA Federal; Richard Varn NOAA Federal; Mark Strom; Christopher Strager; Christopher Cartwright NOAA Federal; Grant Cooper NOAA Federal; Carven Scott NOAA Federal; Daniel Morris NOAA Federal; Kristen Koch NOAA Federal; David Michaud NOAA Federal; Margarita Gregg NOAA Federal; Thomas Graziano NOAA Federal; Deborah Lee NOAA Federal; Chris Sabine NOAA Federal; Dave Westerholm NOAA Federal; Richard Ullman NOAA Federal; Scott Rumsey NOAA Federal; Harry Cikanek NOAA Federal; _NOAA ITSOs; Ken Van Langen NOAA Federal; Steven Freeman NOAA Federal; Wilbert Francis NOAA Affiliate; Michael McCully NOAA Federal; Cynthia Bridgett NOAA Federal; Tina Williams NOAA Affiliate; Mark Deforest NOAA Federal; Brian McGovern NOAA Federal; Eric Barton NOAA Federal; Barry Harrell NOAA Federal; Nick Tenney NOAA Federal; Rick Miner NOAA Federal; Rich Cosgrove NOAA Federal; Rossyn Tasaka NOAA Federal; Barbara Von mettenheim NOAA Affiliate; Chuck Baxley NOAA Federal; Maurice Mcleod NOAA Federal; Linda Matthews NOAA Federal; Giovanni Sella NOAA Federal; MaryLouise Kurchock NOAA Federal; James Cooperman NOAA Affiliate; Dana Larson NOAA Federal; Russell Worman NOAA Federal; Christina Horvat NOAA Federal; Arthur Yo NOAA Federal; Joseph Devost NOAA Federal; Patrick Quigley NOAA Federal; Jennifer Dover NOAA Federal; Julie Raugh NOAA Federal; Blanche Marshall NOAA Federal; Timothy Wugofski NOAA Federal; Steve Michnick NOAA Federal; Mark Dorosh NOAA Affiliate; Chris Ortiz NOAA Federal; Joy Baker NOAA Federal; Sallie Ahlert NOAA Federal; Phil Mieczynski NOAA Federal; Adam Van Meter NOAA Federal; Nicholas Rappold NOAA Federal; Peter Thoenen NOAA Federal; Gary Petroski NOAA Federal; Chris Hornbrook NOAA Federal; James Brown NOAA Federal; John McKeever NOAA Federal; Rene Rodriguez NOAA Federal; Rick Jiang NOAA Federal; Jeff Flick NOAA Federal; Jeff Horn NOAA Federal; Russell Richards NOAA Federal; John Parker NOAA Federal; Timothy O'Brien NOAA Affiliate; Ali Darab NOAA Affiliate; David Skiffington NOAA

	Affiliate; Robert Lai NOAA Affiliate; John Shore NOAA Affiliate; Frank Hughes NOAA Affiliate; James Jones NOAA Federal; John Hill NOAA Federal; _NOAA Assistant CIOs; Zachary Goldstein NOAA Federal; Michelle Reed NOAA Federal; Douglas Perry NOAA Federal; Benjamin Friedman NOAA Federal; Karl Mueller NOAA Federal; John D. Parker NOAA Federal
Cc:	Robert Swisher NOAA Federal; Dennis Morgan NOAA Federal; Sarah Brabson NOAA Federal; John Almeida NOAA Federal; Cc: OCIO/OPPA; Bogomolny, Michael (Federal); Eric Williams NOAA Affiliate; Robert Hogan; Ed Kearns NOAA Federal; _OCIO GPD
Subject:	December Monthly Privacy Report
Attachments:	PTA PIA Management Report (17).xlsx; DOC SORN Status Sheet_NOAA.xlsx; DRAFT Group Communication Security Policy.docx

Good Afternoon,

This is a report regarding the activities of the NOAA Privacy Program from December 1-December 31, 2017. Attached are two spreadsheets outlining the status of SORNs, PIAs, and PTAs within NOAA.

Some of highlights of the Program's activities for the month include:

- NOAA Privacy has begun the briefing process for the NOAA Group Communications Security Policy. The Policy would require NOAA users to add additional security measures, such as participant registry or conference call locking, when discussing Sensitive PII or other matters considered to fall within the NARA guidance on Controlled Unclassified Information (CUI). A copy of the draft Policy is attached for your reference.
- NOAA has begun its first round of re-Certifications for FISMA Systems that already have a DOC-approved PIA in place and have not undergone changes that impact privacy since the last PIA approval. The process has been significantly more streamlined and does not require a DOC Compliance Review Board. NOAA still has 2 systems that collect PII that are operating without a DOC-approved PIA.

NOAA Privacy has agreed to help lead the DOC tabletop exercise for Privacy Incidents planned to take place in early 2018. The exercise is intended to examine problematic areas in coordinating a well-structured response to Moderate or High Privacy incidents under the DOC Breach Response and Notification Plan. DOC's commencement of tabletop exercise activities is consistent with the new requirements imposed by the revisions to OMB Circular A-130.

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

STATUS OF NOAA SYSTEMS OF RECORD NOTICES (SORN)

SORN	Title/Purpose	Date SORN Previously Published	Date Sent to DOC
NOAA 1	Applications for NOAA Corps	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 3	Commissioned Officer Official Personnel Folders	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 5	Fisheries Law Enforcement Cases (Address Update)	8/10/2007 (72 FR 45009)	5/30/2013

NOAA 6	Fishermen's Statistical Data	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 10	NOAA Diving Program	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 11, NOAA Mailing Lists	Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.	NA	5/30/2013
NOAA 12	Marine Mammals, Endangered and Threatened Species, Permits and Exemptions (Amendment)	8/10/2007 (72 FR 45009)	2008
NOAA 13	Records of the Regional Fishery Management Councils	8/10/2007 (72 FR 45009)	5/30/2013
NOAA 14	Dr. Nancy Foster Scholarship Program	2005	8/22/2014
NOAA 15	Observation Privacy Act System of Records Notice 2	10/17/2002 (67 FR 64086)	5/30/2013
NOAA 16	Economic Data Reports for Alaska Federally Regulated Fisheries off the coast of Alaska (first published as Crab Economic Data Report for Bering Sea/Aleutian Islands Management Area (BSAI) off the coast of Alaska, now including two newer economic data report collections)	3 3 2005 (70 FR 10360)	5/30/2013

NOAA 19	Permits and Registrations for United States Federally Regulated Fisheries	4 17 2008/73 FR 20914	5/30/2013
NOAA 20	SARSAT	4 17 2008/73 FR 20914	5/5/2016
NEW NOAA 21	Fisheries Finance Program	NA	2008
NEW NOAA 22	NOAA Health Service Questionnaire	NA	2008
NEW NOAA 23	West Coast Region Economic Data Reports	NA	12/23/2014
		NA	3/9/2017

NEW DEPT 29	UAS	

2015-16 status at DOC
Published 11/25/15; effective 1/19/16
Published 5/5/16; effective 6/14/16
Added missing info and returned to DOC 3 8 16. 4 13 16, DOC decided that it should be a complete update. OLE completed updates 6 16 16; I cleaned up and sent 2 outstanding minor questions, 6 17 16. At one time it had been thought to separate out GC files into another SORN, but it was decided not to. To DOC 6 20 16. Responded to edits and comments rec'd 6 29 16, on 6 30 16, and added the new volunteer routine use. 6 30 17: now at Assistant General Counsel for Legislation, Regulation, and Oversight

MHG completed review 5 22 17; few edits, added volunteer routine use and put in new template, 5 25 17; sent to DOC same day. In new template to DOC 10 14 17
To DOC 12 13 16
Published 10/9/15; effective 11/23/15. Second amended version published 1-12-17. Another amended version to OPOG 6 26 17
Published July 8, 2016. Became effective August 17, 2016.
Published 9/17/15; effective 10/28/15
Published 7/31/2014; effective 09/02/2014
Published 10/9/15;effective 11/23/15

Published 8/7/2015. effective 9/15/15
Amended SORN published 1-12-17
Published July 8, 2016. Became effective August 17, 2016.
Published 1/19/16; effective 3/1/2016
Published 8-7-15; effective 9/15/15

Pending; Expedited Review Memorandum under consideration

(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)

(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:	Wednesday, January 10, 2018 8:08 AM
To:	CPO
Cc:	Gioffre, Kathy (Federal); Graff, Mark (Federal); Toland, Michael (Federal)
Subject:	Re: NOAA Systems on Q2 calendar for which we've submitted certifications
Attachments:	NOAA8877 FY18 PTA 20171206 (1) mhg.pdf; NOAA8877 FY18 certification and PIA 20171206 mhg.pdf

Sure, here you go: certification, re signed PIA (in this case they are in one document) and recently signed PTA. The only change to the PIA was to update the most recent ATO date.

thx Sarah

On Tue, Jan 9, 2018 at 5:17 PM, CPO <CPO@doc.gov> wrote:

> Sarah, can you resend the NOAA8877 certification?
>
> ***Warm Regards,***
>
> *Dorrie Ferguson,*
>
> *Management and Program Analyst*
>
> *Office of Privacy & Open Government*
>
> *dferguson@doc.gov*
>
> *Office: (202) 482-8157*
>
> **From:** Sarah Brabson - NOAA Federal [mailto:sarah.brabson@noaa.gov]
> **Sent:** Tuesday, January 09, 2018 2:46 PM
> **To:** CPO <CPO@doc.gov>
> **Cc:** Gioffre, Kathy (Federal) <KGioffre@doc.gov>; Graff, Mark (Federal) <Mark.Graff@noaa.gov>; Toland, Michael (Federal) <MToland@doc.gov>
> **Subject:** NOAA Systems on Q2 calendar for which we've submitted certifications
>
> For 2 1 18: NOAA6205 certification submitted.

For 2 15 18: NOAA8877 certification submitted.

On Tue, Jan 9, 2018 at 10:27 AM, CPO <CPO@doc.gov> wrote:

> Good morning, Sarah,
>
> It's attached.
>
> ***Warm Regards,***
>
> *Dorrie Ferguson,*
>
> *Management and Program Analyst*
>
> *Office of Privacy & Open Government*
>
> *dferguson@doc.gov*
>
> *Office: (202) 482-8157*
>
> **From:** Sarah Brabson - NOAA Federal [mailto:sarah.brabson@noaa.gov]
> **Sent:** Tuesday, January 09, 2018 9:34 AM
> **To:** Gioffre, Kathy (Federal) <KGioffre@doc.gov>; CPO <CPO@doc.gov>
> **Cc:** Graff, Mark (Federal) <Mark.Graff@noaa.gov>
> **Subject:** Do we have a reasonably final Q2 CRB schedule?
>
> I know we have items for Jan 25 and Feb 8, but need to know if other dates!
>
> thx Sarah
>
> Sarah D. Brabson

IT Infrastructure Investment Program Manager

PRA Clearance Officer

NOAA OCIO

Governance and Portfolio Division

Office 301 628 5751

Ce (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)

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

NOAA OCIO
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: NOAA8877 FY18 PIA 20171206.pdf

FISMA Name/ID (if different): Radar Operations Cener Local Area Network (ROC LAN)/NOAA8877

Name of IT System/ Program Owner: Michael W. Miller

Name of Information System Security Officer: Sallie M. Ahlert

Name of Authorizing Official(s): Joseph A. Pica (NWS OBS) and Richard Varn (NWS ACIO)

Date of Last PIA Compliance Review Board (CRB): May 5, 2017

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

Date of PIA Review: December 6, 2017

Name of Reviewer: Sallie M. Ahlert, 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 (SO or ISSO):  Digitally signed by AHLERT.SALLIE.M.1365877706
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=AHLERT.SALLIE.M.1365877706
Date: 2017.12.07 13:12:37 -06'00'

Date of BCPO Review: 12.27.17

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: 2017.12.27 09:55:12 -05'00'

Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA8877
Radar Operations Center Local Area Network (ROC LAN)

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
NOAA8877 ROC LAN

Unique Project Identifier: 006-48-01-12-3103-00

Introduction: System Description

(a) General Description - NOAA8877 is a moderate impact General Support System (GSS), which provides a small to medium enterprise LAN for the National Oceanic and Atmospheric Administration (NOAA)/National Weather Service (NWS) Radar Operations Center (ROC) and its tri-agency personnel. The ROC's primary mission is to support operations, maintenance, and sustainment of the tri-federal agency (Department of Commerce (DOC), Department of Defense (DOD), and Department of Transportation (DOT)) Next Generation Weather Radar (NEXRAD) weather radar fleet. NOAA8877 provides general office collaboration software and tools together with highly specialized software and hardware systems, which enable ROC's personnel in four branches (Operations, Engineering, Program Support, and Applications) to perform their respective System Development Life Cycle (SDLC) functional roles. Operations Branch runs a 24x7 radar hotline, performs independent testing of modifications and software, and provides on-site technical field support for specialized and particularly difficult radar modifications. Engineering Branch does multi-year planning, project management, development, unit and integration testing, security design, and implementation for all the hardware and software modifications to the radar systems. Program Support Branch provides logistics support, contract maintenance, configuration management, and documentation. Applications Branch leads data quality analysis and improvement initiatives. In addition, this branch leads the scientific groups that make determination on readiness of new science for integration into the radar.

Information in the NOAA8877 ROC LAN general support system primarily consists of programmatic and technical documentation for the NOAA8104 NEXRAD, NOAA8212 Terminal Doppler Weather Radar Supplemental Product Generator (TDWR SPG), and NOAA3065 weather radar data major application programs. If any of the data is sensitive or For Official Use Only (FOUO) programmatic or technical data, then the data is restricted by drives and folders to only ROC personnel authorized to access the information.

(b) Typical Transaction - A typical transaction might be the initiation of a DOC or DOD performance evaluation. The appropriate forms are completed on the ROC team leader's P: drive. It will then be printed, hand-carried for signature, and then transferred as described via UPS. Alternately, the agency-specific secure electronic transfer procedure is followed.

Another transaction example might be the collection of an individual's or other entity's (member of the public, public organization, or private sector) name and email address (work or home, whichever is applicable), who visits the ROC website and voluntarily wishes to have a question answered. In addition, there are work-related secure ROC website databases that store radar system specific data, which may be accessed by tri-agency civilian and military personnel about the radar they are responsible to maintain and/or operate. Further, the field radar maintenance and/or operations personnel may voluntarily provide comments or corrections on technical

documentation. The information is collected only to the extent needed to answer the question(s) posed or to request clarifications, if necessary.

(c) Information Sharing\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 ROC LAN contains personally assigned network shares (P:\), which are accessible only by the person assigned the shared drive. Per ROC directives, DOC and DOD team leaders are required to use only their P: drive to initiate and prepare forms data necessary for awards and performance.

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.

DOD civilian and military performance and awards data initiated at the ROC is required per Air Force Directive-Instructions (AFIs) 36-2406, 36-2502, and 36-2606 to document the individual job performance. The transfer of the information is then submitted to the appropriate Air Force HR personnel via encrypted email or via UPS tracked package as per the applicable AFI.

In addition, the system collects PII of ROC personnel for purposes of emergency recall and ROC Continuity of Operations Planning (COOP). The emergency recall and COOP data is stored on a LAN shared drive only accessible by authorized personnel and on Federal Information Processing Standards (FIPS) 140-2 encrypted iron keys provided by the ROC LAN Information System Security Officer (ISSO) to the ROC director and branch chiefs for emergency recall.

The system collects information necessary to sponsor foreign visitors. The DOC International Affairs Office coordinates or provides oversight for these visits. The information collected includes the foreign visitor's name, date of birth, city and country of birth, and passport number. This information is stored, if required, on the P: drive only of the Program Branch Chief, who is the sponsor of foreign visitors. Foreign National visitors who have "Green Cards" are not required to submit this data. The information on foreign visitors is necessary to sponsor visitors to the ROC from foreign countries. The information on foreign visitors is required for obtaining approval from the Bureau Western Region Security Office (WRSO) in Seattle, Washington to ensure that the foreign visitor is authorized to enter the United States. This foreign visitor information is not disseminated or shared external to ROC.

(d) Authority - Statutory or regulatory authorities for collection and maintenance of the information include:

- 15 USC 1151(Dissemination of Technological, Scientific, and Engineering Information)
- 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)
- DAO 207-12 Foreign Visitor and Guest Access Program

(e) Categorization - NOAA8877 ROC LAN 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):					

☒ 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		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 and credit card information, including truncated form: * Government only issued travel and purchase cards. ** DOD performance and award forms require the individual's SSN; DOC does not require it.					

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		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		f. Business Associates	x		
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	x	Online	
Telephone		Email	x		
Other (specify):					

Government Sources					
Within the Bureau	x	Other DOC Bureaus	x	Other Federal Agencies	x
State, Local, Tribal		Foreign (visitors)*	x		
Other (specify): * Foreign Visitors are foreign government representatives.					

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	
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):			

	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): For emergency recall and COOP			

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 information collected on DOD military and civilian personnel is used to complete military performance and promotion evaluation forms for Air Force personnel. The performance evaluations are required by Air Force Directive-Instruction (AFI) 36-2406 to document the individual's job performance. The performance or promotion evaluation is completed by the NWS or DOD supervisor, discussed with the military member, and securely emailed to Offutt Air Force Base (AFB) using the Common Access Card (CAC) Public Key Infrastructure (PKI) credentials or alternately via tracked UPS package. Once processed at Offutt, the form is returned to the ROC for final signatures and then emailed securely or hand-carried to Tinker Air Force Base (AFB), which has administrative responsibility for the DOD personnel at the ROC (*outside the ROC LAN boundary*). Tinker AFB electronically files a copy in the individual's personnel file and then sends the form to Randolph AFB for final disposition. Per Air Force direction, all forms are transmitted and signed electronically. This information is not shared with anyone beyond those that are required to process it within the respective agency.

Electronic personnel related forms of NOAA employees only are transferred to NOAA HR in bulk or on a case-by-case basis via DOC Accellion (for NOAA records only) or via tracked United Parcel Service (UPS) package. This information is not shared with anyone beyond those that are required to process it within the respective bureau.

The information on foreign visitors is required for obtaining approval from the Western Region Security Office (WRSO) in Seattle, Washington to ensure that the foreign visitor is authorized to enter the United States. This information is not shared outside of the system, by ROC.

NEXRAD technical documentation and telecommunications information is FOUO. The tri-agency (DoD, FAA, and DOC) maintenance or operations field personnel must request access and be authorized to access site specific data, which is maintained at the ROC. Their identifying information (name, work email, and work telephone number) are used to create an account.

Name and email (work or home, whichever is applicable) contact information is collected on a voluntary basis from anyone who makes a web query about the NEXRAD system on the ROC website feedback form. The information is requested in order to provide a response directly to the requestor or make clarifications, when necessary (members of the public, public organizations, private sector).

ROC collects PII of ROC personnel on a voluntary basis for purposes of emergency recall. Employees may decline. ROC collects PII of ROC personnel assigned by the director to the ROC COOP team for COOP recall purposes. COOP employees must provide their PII recall information to be assigned a COOP team role. The employee recall and employee COOP data is stored on a LAN shared drive only accessible by authorized personnel and on FIPS 140-2 encrypted iron keys provided by the ROC LAN ISSO to the ROC director and branch chiefs for emergency recall.

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			
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 WMFO Recruitment Analysis Data System (RADS). NOAA8877 uploads data in specified formats to RADS. Locally, data is segregated on the ROC LAN in specified LAN data stores. ROC LAN shared stores have media protection controls and user procedures in place to keep the data on the ROC LAN.
	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): DoD Military personnel for DoD Personnel Data.			

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.roc.noaa.gov/WSR88D/PAStatement_NOAA8877.aspx .	
x	Yes, notice is provided by other means.	Specify how: a. Web Inquiries –Notice is provided by a privacy statement on the Web site. b. Written notice is included on all personnel forms that employees complete. 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 ROC emergency recall and COOP, employees are asked permission in person when collecting the applicable information. All ROC personnel are informed of the intended purpose. d. Notice is provided verbally to a foreign visitor, by the U.S. sponsor or the DOC person staffing the DOC International Affairs Office, at the time of his/her appearance at the office, that completion of the information on the Foreign National Visitor and Guest Access request form is required for obtaining authorization for a visit.
	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. For web queries, providing PII/BII is voluntary to those wishing to receive a response. Feedback only to the ROC Webmaster may be provided anonymously. c. For the emergency recall roster, ROC personnel can inform their supervisor or administrative officer in person or in writing that they decline to provide PII/BII. COOP team employees must provide their recall information. If a COOP team member declines, they would not be able to perform the duties of this function for the ROC, and they would be removed from this

		role. b. For DOD personnel data, employees may opt not to provide PII/BII – at the time of the request, and 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 can be added without contacting employees. The performance record/information is required in order to conduct performance evaluations. d. Foreign visitors may, at the time of appearance at the DOC International Affairs Office, verbally decline to provide the information requested of them, either to their U.S. sponsor who completes the form, or to the DOC personnel staffing the office. However, refusal to supply the required data will result in being denied access to the Department or any of its bureaus.
	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. ROC web queries (requests for data or for access to site specific radar data): a Privacy Policy statement, stating that provision of the information implies consent to its use, is provided on the Web site. b. Employees may opt not to consent to use of PII/BII – at the time of the request to the personnel administration representative who is assisting them - but this information is needed for processing awards. c. For ROC employees' emergency recall and COOP, the information is used for only one the stated emergency recall purpose. d. Foreign visitors may, at the time of appearance at the DOC International Affairs Office, verbally decline consent to provide the information requested of them, either to their U.S. sponsor who completes the form, or to the DOC personnel staffing the office, but this information is needed for sponsoring them in the Department or any of its bureaus.
	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. Web queries: An individual can review a query before sending, but cannot review or update after submitting. b. Personnel records are obtained/reviewed through the respective DOD and DOC electronic official personnel folder secured repositories but updates must be provided to the servicing HR office.

		c. For Emergency and COOP information, the employee may not review the information, because it contains other staff's PII, but may provide updates to the assigned administrative staff. d. Foreign visitors may submit requests to review and update to the DOC International Affairs Office.
	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: Windows file system auditing monitors, tracks, and records changes to the files containing PII/BII. This does not track content changes.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): **5/26/2017 with DOC PO approved PIA 5/12/2017.** ☐ 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.
	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): As stated in the ROC 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 ROC Rules of Behavior (ROB) indicating that they have read and understand the ROB. In addition, as of September 2015, ROC LAN users review and acknowledge the current ROC ROB annually in concurrence with the release of the NOAA annual IT security awareness training. The Feb 2016 ROB update includes a section for PII definition, storage, sharing, and how to report PII incidents. To protect mobile information, all ROC 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.

Segregation of data with granularity of control on data shares to the user or group level, as appropriate. Controlled access for servers and data storage areas limited to only ROC LAN system administrators. FIPS 140-2 encryption for all mobile laptop devices. Rules of Behavior annual supplemental training on where to store PII and how to handle transfers locally and via DOC Accellion. Two specific scanner locations for PII that are not network connected and to ensure PII data is not emailed with multi-function scanner/copier.

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)*: For employee information, the applicable SORN is COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies. This covers all ROC employees. NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission. Specifically, the SORN covering the Foreign Visitor/Guest Information: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons--COMMERCE/DEPT-9.
	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 Specific Records Schedule 100-24 IT Operations and Management Records, General Record Schedule GRS-20 for general IT related data, NOAA 302-03 Personnel Actions, NOAA 600-07 Foreign Visitors, NOAA 1301-05 Sensors and Equipment Project Case Files, NOAA 1301-07 Radar Project Case Files
	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	
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: NOAA8877 ROC LAN does not have an aggregation of individual PII data, as would NOAA or DoD personnel systems and DOC financial and travel systems. There are no ROC personnel specific datasets on the ROC LAN that would expose all employees or make all employees easily identifiable. NOAA8877 does not have aggregations of PII on members of the public to support identifiability.
x	Quantity of PII	Provide explanation: NOAA8877 ROC LAN has fewer than 160 users total. Breakdown of ROC personnel is < 42% DOC and < 10% DoD. The impact as a result of loss of employee PII at the ROC is estimated to be minor and is anticipated to have limited adverse effect on continued performance of primary mission function.

x	Data Field Sensitivity	Provide explanation: Examples of the most sensitive situation examples would be ROC employee names and phone numbers on an emergency call roster, a list of the few ROC employee names and government purchase card numbers, or foreign government visitor information that is required to be kept by the ROC employee host. Release of employee or foreign visitors names and contact information would not likely cause harm to the individuals.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: End users do not access data (PII or otherwise) on NOAA8877, except with NOAA secured and encrypted assets approved for the specific purpose. Per rules of behavior, PII is accessed or used for its intended purpose on the system via directly connected nodes, and is not transferred to or transported on NOAA mobile devices. PII is established in designated/protected shared access folders and is made accessible only to those with a need to know.
x	Other:	Provide explanation: All end of life cycle NOAA8877 disks servers, multi-function copier/printers/faxes, and end user desktop/laptop components are wiped and shredded per policy and not reused in any manner.

Section 12: Analysis

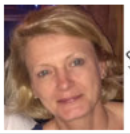
12.1 Indicate whether the conduct of this PIA results in any required business process changes.

x	Yes, the conduct of this PIA results in required business process changes. Explanation: More stringent privacy data related procedures were put in place to address gaps identified in NOAA8877 processes and technologies. Summary of adjustments is given below: • Administrative personnel were trained on use of two local PC/non-networked scanners to control transfer of personnel related PII into ROC LAN for eventual upload to NOAA WMFO or other appropriate HR systems. This avoids problems with PII on paper copies being scanned via multi-function copier, which can only send as email attachments to recipient. • Primary users of PII are administrative personnel, branch chiefs, and team leaders. They occasionally have need to share data in folders with others to continue processing of the paperwork, for submission, and/or for peer review purposes. These folders are designated on the ROC LAN as PII-Secured and locked down to specific users.
	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: USB connected scanners were added in two specific building locations to facilitate the transfer of potentially sensitive personnel data (awards, ratings, hiring, etc.) from paper copies to the system for processing in NOAA WMFO systems.
	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: Sallie M. Ahlert Office: DOC\NOAA\NWS\OBS1 (ROC) Phone: (405) 573-8870 Email: Sallie.M.Ahlert@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.  Sallie M. Ahlert Digitally signed by AHLERT.SALLIE.M.1365877706 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=AHLERT.SALLIE.M.1365877706 Date: 2017.12.07 13:12:06 -06'00'	**Information Technology Security Officer** Name: Joy Baker Office: DOC\NOAA\NWS\ACIO Phone: (228) 688-2801 Email: Joy.Baker@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. BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER.JOY.ALLISON.1269758577 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=BAKER.JOY.ALLISON.1269758577 Date: 2017.12.07 13:30:44 -06'00'
Authorizing Official Name: Joseph A. Pica Office: DOC\NOAA\NWS\OBS Phone: (301) 427-9778 Email: Joseph.A.Pica@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. PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.12.21 08:49:58 05'00'	**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. 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: 2017.12.27 09:55:57 -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: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
Radar Operations Center Local Area Network (ROC LAN)
NOAA8877
December 06, 2017

U.S. Department of Commerce Privacy Threshold Analysis

NOAA ROC LAN

Unique Project Identifier: NOAA8877

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: NOAA8877 is a General Support System (GSS), which provides a small to medium enterprise LAN for the NOAA\NWS ROC and its tri-agency personnel. The ROC's primary mission is to support operations, maintenance, and sustainment of the tri-federal agency (DOC, DOD, and DOT) NEXRAD weather radar fleet. NOAA8877 provides general office collaboration software and tools together with highly specialized software and hardware systems, which enable ROC's personnel in four branches (Operations, Engineering, Program Support, and Applications) to perform their respective System Development Life Cycle (SDLC) functional roles. Operations Branch runs a 24x7 radar hotline, performs independent testing of modifications and software, and provides on-site technical field support for specialized and particularly difficult radar modifications. Engineering Branch does multi-year planning, project management, development, unit and integration testing, security design, and implementation for all the hardware and software modifications to the radar systems. Program Support Branch provides logistics support, contract maintenance, configuration management, and documentation. Applications Branch leads data quality analysis and improvement initiatives. In addition, this branch leads the scientific groups that make determination on readiness of new science for integration into the radar. 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. *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 ROC LAN 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 ROC LAN 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): Michael W. Miller

Signature of ISSO or SO: MILLER.MICHAEL.W.1180644136 Digitally signed by MILLER MICHAEL W 1180644136 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn MILLER MICHAEL W 1180644136 Date 2017 12 06 16 35 34 06'00' Date: 12/6/2017

Name of Information Technology Security Officer (ITSO): Joy Baker

Signature of ITSO: BAKER.JOY.ALLISON.1269758577 Digitally signed by BAKER JOY ALLISON 1269758577 DN c US, o U S Government, ou DoD, ou PKI, ou OTHER, cn BAKER JOY ALLISON 1269758577 Date 2017 12 07 07 39 04 06'00' Date: 12/7/2017

Name of Authorizing Official (AO): Joseph A. Pica

Signature of AO: PICA.JOSEPH.A.1086500961 Digitally signed by PICA.JOSEPH.A.1086500961 Date: 2017.12.21 08:48:20 05'00' Date: 12/21/2017

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 2017 12 27 10 06 54 05'00' Date: 12.27.17

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, January 10, 2018 8:35 AM
To:	Jason MacMaster NOAA Federal; Bill McMullen NOAA Federal
Cc:	Mark Graff NOAA Federal; John D. Parker NOAA Federal
Subject:	Re: NOAA6001: certification needed, or CRB 2 8 18
Attachments:	NOAA6001 FY17 PIA _revised 032017.docx; PIA Annual Review Certification Form with PA Officer Final_20171101.pdf; NOAA6001 PTA 2017 2 8 17 signed jp cc mhg.pdf

Jason and Bill: If there are no changes to NOAA6001 since last March, that would create privacy risks, we can submit a certification attesting to that, in place of a new PIA.

1. Here is the last PIA in Word. If no changes that create new privacy risks, you can pdf and then you need to obtain new NOS signatures and send to me for Mark's signature.

2. For the attached certification (fillable pdf), one of you would complete and sign, and send to me for Mark's signature. Please also make sure the most recent SAR, including or addition to a privacy control assessment, is available in CSAM.

3. We will also need a new PTA, since the last one was signed 2/17. It needs to state that there are no new privacy risks. Attached is the last one in pdf. Let me know if you need the Word template. Once you've obtained NOS signatures, please also send to me for Mark's signature.

IF there are changes that create new privacy risks, please update the PIA to reflect that, and also state it on the new PTA.

The DOC compliance review board (CRB) conference call will take place on 2 8 18 (to obtain approval for an updated PIA). If we do the certification, we'll just send that, the PIA and PTA to DOC, and no need for a call. Otherwise, we need to get the final PIA and PTA to them, hopefully by the end of Jan, so they can review before the CRB.

Please call me at 717 548 4077 with any questions. Next Tuesday and Wed I'll be in the office (see signature block) and then back at the above number.

On Wed, Jan 10, 2018 at 8:21 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Thanks, John. Will do.
>
> On Wed, Jan 10, 2018 at 8:11 AM, John D. Parker NOAA Federal <john.d.parker@noaa.gov> wrote:
>
> > Hi Sarah,
> >
> > Jason MacMaster is the ISSO and Bill McMullen is the CTO/IT Manager.
> >
> > Please include both on email communications as well as me.
> >
> > Thanks,

> John
>
> – –

(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: 01-2015

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the
NOS Enterprise Information System
(NOAA6001)

U.S. Department of Commerce Privacy Threshold Analysis

NOS Enterprise Information System (NOAA6001)

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 Ocean Service (NOS) Enterprise Information System (EIS) is an integrated collection of components designed to provide general office automation, infrastructure and connectivity services to NOS Headquarters and component program and staff offices either resident in Silver Spring, MD, or logically connected to the system through WAN links.

NOAA6001 groups elements of the system into three areas, each of which serves a distinct and specific function:

Network Devices -- NOS SSMC (Silver Spring Metro Center) campus backbone and NOS Wide Area Network (WAN)

NOS Domain Servers -- The NOS domain infrastructure components and Headquarters Local Area Network (File, Print, Application) services

Web Application Servers -- NOS application and database hosting services

In addition to the general purpose office automation support (file/printer sharing, application hosting, collaboration, etc.) provided by NOAA6001, the system provides help desk services and supports a number of internal web sites and a minor application which collects, stores and/or disseminates PII.

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.)."

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

__X__ **Companies** - the names of the companies interested in information developed by NOS, which is provided by the users

__X__ **Other business entities** - AAMB 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 this is financial information 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.

The Constituents' database collects limited PII from stakeholders involved with or interested in information provided by the National Ocean Service.
NOAA6001 collects and stores information related to the Office of the Assistant Administrator, Management and Budget (AAMB), which includes limited PII, specifically, names, telephone numbers and email addresses (voluntarily submitted by data providers and customers) to facilitate external coordination with data providers.

NOAA6001 stores PII on an ad-hoc basis 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 stores COOP information, travel authorization and vouchers, passports and international travel forms, information for the security badging process, and performance appraisal ranking.

In NOS, the Local Registration Authority (LRA) is responsible for identity verification of NOS administrators that need to request public key infrastructure (PKI) certificates from DOD. This verification process uses form DD-2841 that requires the LRA to enter PII. This form is stored on the NOS network in a password protected zip file. The PII collected consists of the unique identification number from a federal government-issued identification credential with a picture, for example Military ID card or Passport card; the unique identification number from a non-federal government-issued identification card, for example Driver License card. The form also contains common access card (CAC) card electronic data interchange personal identifier (EDIP), full name, work email, work phone number. Only the numbers are collected from the artifacts and stored

in the system. The LRA returns the artifacts to the user and does not store images of them on NOAA6001 systems.

____ 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 NOS Enterprise Information System 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) or System Owner (SO):

_____

Signature of ISSO or SO: VON METTENHEIM.BARBARA.GALL.1464040290 Digitally signed by VON METTENHE M BARBARA GALL 1464040290 DN: c US o U S Government ou DoD ou PKI ou CONTRACTOR cn VON METTENHEIM BARBARA GALL 1464040290 Date: 2017 02 13 11:19:58 05'00' _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn PARKER.JOHN.D.1365835914 Date: 2017.02.13 11:33:57 -05'00' _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: CARTWRIGHT.CHRISTOPHER.1365832702 Digitally signed by CARTWRIGHT.CHRISTOPHER.1365832702 DN: c US, o U.S. Government, ou DoD, ou PKI, ou OTHER, cn CARTWRIGHT.CHRISTOPHER.1365832702 Date: 2017.02.15 11:12:01 -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: 2017.02.15 13:27:33 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: _____

FISMA Name/ID (if different): _____

Name of IT System/ Program Owner: _____

Name of Information System Security Officer: _____

Name of Authorizing Official(s):_____

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

Date of PIA Review: _____

Name of Reviewer: _____

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: _____

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

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: _____

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: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Wednesday, January 10, 2018 10:20 AM
To:	Sean Mcmillan NOAA Federal
Cc:	James Jones NOAA Affiliate; Mark Graff NOAA Federal
Subject:	RE NOAA2220 PIA new privacy risks? please see below
Attachments:	NOAA2220_PIA_20170331_final.docx; PIA Annual Review Certification Form with PA Officer Final_20171101.pdf; NOAA2220 PTA_20170331 for signature Signed RS.pdf

Hi, Sean, did NOAA2220 have any changes that would create new privacy risks, since April 2017? If not, we do not need to do a new PIA this year, just complete a certification that there are no new privacy risks.

1. Here is last year's PIA either for update if needed (new privacy risk(s)) and sending to me for review, OR if no changes, simply pdf'ing and obtaining current signatures, and sending to me for Mark Graff's signature.

2. If a new PIA is not needed, please complete and sign the attached fillable pdf certification, and send to me for Mark's signature. Please also ensure that recent SAR is in CSAM for Mark's review.

3. A new PTA IS needed, since the last one was signed 3/17. If you are making no changes to the PIA, the question in the PTA about privacy risks should be answered "no new privacy risks". Here is the last signed PTA, let me know if you need the Word template for a new one.

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

NOAA OCIO
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
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: The NOAA2220 System consists of ships, aircraft and land based ground support systems. Many of these systems have similar general functions and operating characteristics, security needs, and operating environments, and shore-based applications that support the ship missions. Common shipboard IT infrastructure functions include network connectivity, domain authentication, internet connectivity, and general business support services, such as file and print services. Ships are configured with satellite communication systems, such as Inmarsat and VSAT, and connect to NOAA networks and the internet via contract satellite service providers. While each ship has common (or class similar) configurations, mission requirements require each to have a unique configuration. To facilitate their inclusion in a consolidated System Security Plan (SSP), each ship and subsystem is described in the System Security Plan.

The NOAA fleet of ships are managed, operated and maintained by NOAA's Office of Marine and Aviation Operations (OMAO), Marine operations centers (MOCs), located in Norfolk, Virginia; Honolulu, Hawaii; and Newport, Oregon. Additional ship-specific support is provided through port office facilities in Woods Hole, Massachusetts; Davisville, Rhode Island; Charleston, South Carolina; Pascagoula, Mississippi; San Diego, California; and Ford Island, Hawaii. Limited pier-side support is also provided to ships in Newport, Rhode Island 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.*

_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	X	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. *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.

_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 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: Sean T McMillan Date: 31 Mar 17

Name of Information Technology Security Officer (ITSO): LCDR James Jones

Signature of ITSO: James Jones III Date: 31 MAR 17

Name of Authorizing Official (AO): CDR Joseph Baczkowski

Signature of AO: Date: 31 MAR 17

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF

Signature of BCPO: SWISHER.DONALD.ROBERT.1376511460 Digitally signed by SWISHER.DONALD.ROBERT.1376511460 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SWISHER.DONALD.ROBERT.1376511460 Date: 2017.03.31 15:34:51 -04'00' Date:

(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)

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

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

Name of PIA: _____

FISMA Name/ID (if different): _____

Name of IT System/ Program Owner: _____

Name of Information System Security Officer: _____

Name of Authorizing Official(s):_____

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

Date of PIA Review: _____

Name of Reviewer: _____

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: _____

Date of Privacy Act (PA) Review: _____

Name of Reviewer: _____

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: _____

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: _____

Jean Apedo - NOAA Federal

From:	Jean Apedo NOAA Federal
Sent:	Thursday, January 11, 2018 8:23 AM
To:	Sarah Brabson NOAA Federal; Mark.Graff@noaa.gov
Cc:	David Skiffington NOAA Affiliate
Subject:	RE: 0201 PIA and PTA signatures?
Attachments:	NOAA0201 PTA_122717 v2.pdf

Hi Sarah and Mark,
Please find attached the signed PTA.
Thank you.

From: David Skiffington NOAA Affiliate [mailto:david.j.skiffington@noaa.gov]
Sent: Thursday, January 11, 2018 8:20 AM
To: Sarah Brabson NOAA Federal; Jean Apedo NOAA Federal
Subject: Re: 0201 PIA and PTA signatures?

Sarah,
Doug asked for a tiny change. He has signed it and sent it to me yesterday, but the ITSO (Jean) signature needs to be added.

David

On Thu, Jan 11, 2018 at 8:15 AM, Sarah Brabson - NOAA Federal <sarah.brabson@noaa.gov> wrote:
Honestly, if Doug signed the PIA, what would prevent him from signing the PTA? Did you send them together? thx

On Wed, Jan 10, 2018 at 2:35 PM, Sarah Brabson - NOAA Federal <sarah.brabson@noaa.gov> wrote:
Thanks!!

On Wed, Jan 10, 2018 at 2:32 PM, Jean Apedo - NOAA Federal <jean.apedo@noaa.gov> wrote:
I sent both documents to Doug this morning. I am following up on the PTA and will update you.

On Jan 10, 2018, at 2:23 PM, Sarah Brabson - NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Thanks, Jean, where is the PTA? It was circulating for signatures as of 12-12-17.
>
> Sarah
>
> On Wed, Jan 10, 2018 at 2:07 PM, Jean Apedo - NOAA Federal <jean.apedo@noaa.gov> wrote:
> Hello Sarah and Mark,
> Please find attached NOAA0201 PIA for your signature.
> Thank you.

From: Douglas Perry NOAA Federal [mailto:douglas.a.perry@noaa.gov]
Sent: Wednesday, January 10, 2018 12:21 PM
To: Jean Apedo NOAA Federal
Cc: Ann Madden NOAA Federal; David Skiffington NOAA Affiliate
Subject: Re: FW: 0201 PIA and PTA signatures?

See attached, signed PIA.

On Wed, Jan 10, 2018 at 10:17 AM, Jean Apedo - NOAA Federal <jean.apedo@noaa.gov> wrote:

Doug,
Please find attached NOAA0201 PTA and PIA for your review.
Thank you.

From: David Skiffington NOAA Affiliate [mailto:david.j.skiffington@noaa.gov]
Sent: Monday, January 08, 2018 11:04 AM
To: Jean Apedo NOAA Federal
Subject: Fwd: 0201 PIA and PTA signatures?

---------- Forwarded message ----------
From: **Sarah Brabson - NOAA Federal** <sarah.brabson@noaa.gov>
Date: Mon, Jan 8, 2018 at 10:57 AM
Subject: 0201 PIA and PTA signatures?
To: David Skiffington - NOAA Affiliate <david.j.skiffington@noaa.gov>

Still need ITSO and AO signatures on these, so I can get Mark's signatures. . thx

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

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

--
David J. Skiffington (Actionet Contractor)
NOAA Web Operations Center - NOAA0201 ISSO
Phone: 301.628.5662
Cell: (b)(6)

--
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)

--
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)

--

David J. Skiffington (Actionet Contractor)
NOAA Web Operations Center - NOAA0201 ISSO
Phone: 301.628.5662
Cell: (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, January 11, 2018 8:48 AM
To:	Sarah Brabson NOAA Federal
Subject:	Re: NOAA0201 re signed PIA and new PTA for signature
Attachments:	NOAA0201 PTA_122717 v2 mhg.pdf

Here is the PTA

PIA to come.

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

On Thu, Jan 11, 2018 at 8:35 AM, Sarah Brabson NOAA Federal <sarah.brabson@noaa.gov> wrote:

> Mark, you signed the certification a few weeks ago.
>
> I sent you the PIA yesterday but here it is again, now with the PTA, for signature.
>
> Kathy G. says DOC has decided to ask for the ATO date to be updated, in the re signed PIA so after you sign, I'll fix that one . .
>
> I've re attached the certification that you already signed on December 4, for your reference.
>
> 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 Threshold Analysis
for the
Web Operations Center (NOAA0201)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Web Operations Center

Unique Project Identifier: 006-000351100 00-48-03-17-01-00

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 Web Operations Center (WOC) is a diverse information technology services provider to Line and Staff Offices within NOAA. The WOC provide a wide range of information technology services and functions which include high availability, scalability, redundancy, clustering, and high performance computing to replicate and distributed general information as well as critical time sensitive life and property information to the general public and meteorology community.

The services and functions of the information system technology have been broken down into five (5) core services and functions: WOC Domain Name System Services (WOCDNSS), WOC Information Sharing Services (WOCISS), WOC Adoptive System Framework (WOCASF), WOC NOAA Enterprise Message System (WOCNEMS) and WOC Collaboration Services (WOCCS). These services and functions make up the subsystems within NOAA0201. Each subsystem has a different FIPS 199 security categorization as described in the NOAA0201 FIPS 199 Security Categorization document. NIST SP 300-37 rev1 describes how various independent subsystems could be grouped together for purpose of risk management into more comprehensive system (system of systems).

The WOC systems are physically located at 8 NOAA datacenters (W1: Silver Spring, Maryland W2: Largo, Maryland W3: Norman, Oklahoma W4: Boulder, Colorado W5: Fort Worth, Texas and W6: Seattle, Washington, W7: Ashville, NC and W8: Fairmont, WVA).

Note: NOAA0201 has been assessed on 1/12/2017 using NIST 800-53 Rev 4.

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.*

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

2. 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.

3. Personally Identifiable Information

3a. 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 3a, please respond to the following questions.

3b. 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.

3c. 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, 3b, and/or 3c 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 NOAA0201 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 NOAA0201 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):

David J. Skiffington

Signature of ISSO or SO: SKIFFINGTON.DAVID.JEROME.1374262730 Digitally signed by SKIFFINGTON.DAVID.JEROME.1374262730 DN: c US, o U.S. Government, ou DoD, ou PKI, ou CONTRACTOR, cn SKIFFINGTON.DAVID.JEROME.1374262730 Date: 2018.01.10 13:45:29 05'00' Date: _____

Name of Information Technology Security Officer (ITSO): Jean Apedo

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 2018.01.11 08 22 08 05'00' Date: _____

Name of Authorizing Official (AO): Douglas Perry

Signature of AO: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2018.01.10 17:12:41 -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: 2018.01.11 08:47:32 -05'00' Date: _____

Sarah Brabson - NOAA Federal

From:	Sarah Brabson NOAA Federal
Sent:	Thursday, January 11, 2018 8:36 AM
To:	Mark Graff NOAA Federal
Subject:	NOAA0201 re signed PIA and new PTA for signature
Attachments:	NOAA0201 PTA_122717 v2.pdf; NOAA0201 Web Operations Center WOC_122717 PIA.pdf; NOAA0201_PIA Annual Review Certification Form 20171204 mhg.pdf

Mark, you signed the certification a few weeks ago.

I sent you the PIA yesterday but here it is again, now with the PTA, for signature.

Kathy G. says DOC has decided to ask for the ATO date to be updated, in the re signed PIA so after you sign, I'll fix that one . .

I've re attached the certification that you already signed on December 4, for your reference.

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)