Version Number: 01-2019

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: 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

for Dr. Catrina D. Purvis LISA MARTIN Digitally signed by LISA MARTIN Date: 2020.04.14 21:33:47 -04'00' 03/05/2020

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.

(a) Whether it is a general support system, major application, or other type of system

The National Ocean Service (NOS) Center for Operational Oceanographic Products and Services (CO-OPS) is a Major application.

(b) System location

Located primarily in Silver Spring MD, but with field offices in Seattle Washington, Chesapeake Virginia, and Gulf Breeze Florida that collects and distributes observations and predictions of water levels and currents to ensure safe, efficient and environmentally sound maritime commerce. CO-OPS also has a presence in both the Microsoft Azure cloud and Amazon Web Services (AWS) cloud.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

To accomplish this mission, NOAA6205 relies on the below Systems for services:

System Interconnections/Information Sharing

System Information
NOAA0100 Organization: N-CIRT Network
NOAA0200

Organization: NOAA Network Operations Center (NOC)
NOAA3100 Organization: OAR Pacific Marine Environmental Laboratory (PMEL)
NOAA5004 Organization: Data Collection System Automatic Processing System
NOAA6001 Organization: NOS Enterprise Information System
NOAA8870 Organization: National Weather Service Telecommunication Gateway

(d) The way the system operates to achieve the purpose(s) identified in Section 4

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 on either 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 that provide limited external information to the public. This information has been reviewed and approved by CO-OPS.

(e) How information in the system is retrieved by the user

The information is retrieved through an application user interface, except for the data that is kept on the shared drives.

(f) How information is transmitted to and from the system

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. Although the CO-OPS' Chesapeake surveillance system has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII

captured is immediately deleted. This system also only operates at our Chesapeake field office to further reduce the potential of inadvertently capturing PII.

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.

(g) Any information sharing conducted by the system

None of the applications share PII outside of NOAA except that NOS employee information may be shared with Commerce and other federal agencies in case of a breach.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

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

• NOAA-11: 5 U.S.C. 301, Departmental Regulations
• 15 U.S.C. 1512, Powers and duties of Department
• DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C.
• 3101 Equal Employment Act of 1972
• 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. 1265
• Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110
• Executive Order 12564; Public Law 100-71, dated July 11, 1987
• 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
• GSA/GOVT-7: 5 U.S.C. 301
• Federal Information Security Management Act of 2002 (44 U.S.C. 3554)

• E-Government Act of 2002 (Pub. L. 107–347, Sec. 203) • Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504 note) • Homeland Security Presidential Directive 12 (HSPD–12) • Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004 • OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

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):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

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

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. 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	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. 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): User ID, IP Address, and Date/Time of Access is automatically collected by the System for auditing purposes only.					

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

Other Information (specify)

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

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

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

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

2.3 Describe how the accuracy of the information in the system is ensured.

Information 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 user inputting the data as is required to ensure the accuracy of this information.

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. The contracting officer reviews users' data prior to inputting into the system and the user reviews their data at various points in the process.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

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

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)

Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

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

Section 3: System Supported Activities

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

Activities			
Audio recordings		Building entry readers	X
Video surveillance	X	Electronic purchase transactions	
Other (specify): The Chesapeake Field Office utilizes a video surveillance system that is managed by the FOD staff. Signs indicating that the facility is being monitored by video are posted. This is a stand-alone system that records onto disks, which are overwritten every 60 days (or when full). Only the FOD manager and the one IT staff have access to the disks. Although the CO-OPS' Chesapeake surveillance system has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. This system also only operates at our Chesapeake field office to further reduce the potential of inadvertently capturing PII. 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			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	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 order to determine a potential contractor's ability to fulfil contract a request for proposal (RFP) proprietary information (BII) may be collected to review proposals.			

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 aids in managing administrative programs related to an employee or contractor's employment status, travel, and other human capital resources activities. PII is collected from employees as well for emergency purposes. The Division Chiefs and Deputies within CO-OPS also use this information 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, Gulf Breeze, 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.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the

bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

If users print information from the system with privacy data placed in it, there is a chance that this data could be viewed if the document is left in plain sight. Non-sensitive PII could be exposed if unauthorized access to the system is somehow achieved. To combat the potential of users accidentally causing privacy incidents, users are required to take privacy training at least annually as a part of our annual security awareness course. Users must a sign rules of behavior to ensure they understand their responsibilities to the system and that data which resides on it.

Section 6: Information Sharing and Access

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

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

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

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

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA6205 is connected to the NOS Line Office information system NOAA6001 and the other NOAA information systems, mentioned above in this document, for VPN, security, and network operations. NOAA6205 does not share or receive PII or BII through these technical infrastructure connections. NOAA6205 has established security permissions based on NOS Active Directory network account (enforced with 2FA for all accounts), 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: The Privacy Act statement and/or 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 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 that 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 employees and contractors 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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 3/30/19 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. MODERATE

X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

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 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

____ Yes, the PII/BII is searchable by a personal identifier.

_X_ No, the PII/BII is not searchable by a personal identifier.

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: 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. DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons, GSA-GOVT-9, System for Award Management, GSAGOVT-10, FAR Data Collection System.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: 1603 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 Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

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

X	Identifiability	Provide explanation: 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.
X	Obligation to Protect Confidentiality	Provide explanation: Users are required to log into the application with a user name and password. The database fields that contain PII are encrypted.
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 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Potential threats that exist for information collected include data exfiltration and improper handling, retention, sanitization and/or disposal of data. To mitigate these threats CO-OPS has enacted the following:

CO-OPS utilizes the NOAA Office of Human Capital Services, which collects, stores and maintains employee data for internal COOP, Human Resources, and workforce planning purposes only.
CO-OPS follows and implements principle of least privilege and separation of duties (RBAC) in combination with rule-based access control. Only authorized individuals with a need to know will have access to data.

All CO-OPS components are, configured following secure baselines, continuously monitored through weekly/monthly vulnerability scans, and log reviews. All CO-OPS staff are required to complete the mandatory IT security awareness training every year.

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

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

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

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

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