

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



Privacy Impact Assessment
for the
NOAA6205
Physical Oceanographic Real-Time System and National Water Level
Observation Network (PORTS-NWLON)

Reviewed by: Mark H. 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

TAHIRA MURPHY Digitally signed by TAHIRA MURPHY
Date: 2024.11.29 22:18:36 -05'00' 10/31/2024

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

Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NOS/CO-OPS/Physical Oceanographic Real-Time System and National
Water Level Observation Network

Unique Project Identifier: NOAA6205

Introduction: System Description

Provide a brief description of the information system.

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.

Address the following elements:

(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 system.

(b) System location

The headquarters for NOAA6205 is located in Silver Spring, Maryland, with field offices in Seattle, Washington; Chesapeake, Virginia, and Gulf Breeze, Florida that collect and distribute observations and predictions of water levels and currents to ensure safe, efficient and environmentally sound maritime commerce. NOAA6205 also has a majority of our servers in the 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)

NOAA6205 interconnects with the following systems:

- NOAA0100 (NOAA Cyber Security Center) for IT security services– no shared Personally Identifiable Information/Business Identifiable Information (PII/BII)
- NOAA0550 (NOAA N-Wave is the name of network service provider for NOAA) for network connectivity – no shared PII/BII
- NOAA8870 (National Weather Service Telecommunication Gateway). NOAA6205 sending data to National Weather Service (NWS) via NOAA internal network– no shared PII/BII
- NOAA6001 (NOS Enterprise Information System) The interconnection with NOAA6001 is utilized for connections to NOS hosted applications and NOAA campus

backbone – no shared PII/BII

NOAA6205 also utilizes NOAA virtual private network (VPN) for remote connectivity and NOAA N-Wave for connection to AWS East-West Federal Risk and Authorization Management Program (FedRamp) Cloud hosting protected by secure sockets layer (SSL)– no shared PII/BII

(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. NOAA6205 also utilizes Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) within AWS. These cloud-based services do not host, process, or transmit any PII/BII. The only personal information stored are in relation to account information such as user logins, with fields such as username, password, and NOAA e-mail address.

(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. Web servers that have publicly accessible information is accessible anonymously using the Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) protocols. However, privileged users are uniquely identified and authenticated in order to change information on the web servers.

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

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. NOAA6205 transmits data within NOAA organization using NOS/N-Wave network that secured by N-Wave infrastructure. All data is encrypted during transit with no PII/BII information shared.

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' Continuity of Operations Plan (COOP) and other administrative processes. The information being collected is shared within the Bureau on a case-by-case basis.

This employee identifying information is collected to be able to manage administrative programs related to an employee or contractor's employment status, travel, and other human resources activities. Employee's emergency contact information to be used in the COOP event only. None of the administrative processes listed require social security number (SSN)s.

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

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. The Chesapeake surveillance system is a standalone, low image quality video system provided by the facilities managers at Chesapeake to their CO-OPS tenants. The video quality of the system renders it unable to gather PII which may be displayed on an individual. It is also not the purpose of the device to capture or store any PII and any potential PII captured is immediately deleted. This system also only operates at our Chesapeake field office to further reduce the potential of inadvertently capturing PII. CO-OPS does not capture photographs for badging since that is performed (and stored) by the NOAA Office of Security. CO-OPS does utilize staff pictures (with written permission) as part of either internal or external website as part of CO-OPS program, possible profile narrative, and/or presentation of CO-OPS mission activities.

Vendor provided Business Identifiable Information (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.

Internal data security is provided by defense-in-depth (NOS/N-Wave network) with layered security for internal data (physical access, firewalls, Active Directory, Access Controls, etc.). Public data is hosted on publicly accessible websites which are all hosted with SSL/TLS certificates for enhance security. All data is encrypted during transit and at rest.

(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. Information is shared periodically within the bureau on a case-by-case basis. Additionally, non-sensitive POC information on certain subjects are made available via the NOAA6205 web presence. Though the utilization of Google drive/docs/sheet is taking place within NOAA6205, users are prohibited by policy to store any PII information within these services. NOAA6205 provides water levels and currents predictions to NOAA8870 (National Weather Service Telecommunication Gateway) via NOAA internal network– no shared PII/BII.

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

Type of Information Collected	Applicable SORNS	Programmatic Authorities
Breach Investigation	COMMERCE/DEPT-13	Privacy Act of 1974, 5 U.S.C. 552a(e)(10)
		Federal Information Security Modernization Act of 2014 (FISMA 2014)
		OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
Security Investigations	COMMERCE/DEPT-13	Executive Orders 10450, 11478
		5 U.S.C. 7531-332
		28 U.S.C. 533-535
Building Entry/Access & Surveillance	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
	COMMERCE/DEPT-6	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
Acquisition Sensitive	GSA-GOVT-9	
	GSA-GOVT-10	
	COMMERCE/DEPT-2	
Personnel Records, Collection & Use of SSN	COMMERCE/DEPT-18	44 U.S.C. 3101
		Executive Order 12107
	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
	GSA/GOVT-7:	Federal Personal Identity Verification Identity Management System (PIV IDMS)
Information for Members of the Public, Travel, Health Emergency Info & Reasonable Accommodation (includes medical and religion accommodation requests)	COMMERCE/DEPT-9	
	COMMERCE/DEPT-18	Executive Order 13164
	COMMERCE/DEPT-31	Rehabilitation Act, 29 U.S.C. 701 et. seq
		Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d)
		29 CFR parts 1602, 1630, 1904, 1910, and 1960
		29 USC chapter 15 (e.g., 29 U.S.C. 668)
		Executive Order 12196
		5 U.S.C. 7902
	COMMERCE/NOAA-11	Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission

(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): NOAA6205 does not utilize unmanned aircraft system (UAS) therefore there is no Privacy Risks from UAS.					

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.

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		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	X
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	X	s. Marital Status	
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 collection 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	X
c. Work Address	X	g. Work History		k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. 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		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): NOAA6205 does not utilize unmanned aircraft system (UAS), therefore there are no Photographs collected. The X has been removed from box e. Photographs.					

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	X
Telephone		Email			

Other (specify):

Government Sources					
Within the Bureau		Other DOC Bureaus	X	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 Describe how the accuracy of the information in the system is ensured.

Mission data

CO-OPS mission data is posted after completing quality assurance validation. All incoming mission data undergoes complete quality assurance prior to being incorporated into the mission business process. All of our observational, oceanographic data acquired in the field undergoes a rigorous multi-tier Quality assurance/Quality control (QA/QC) process in Real-Time, Near-Real-Time, Monthly Data Processing.

Real-Time:

Data acquired in real-time are automatically undergo a basic quality control process during data ingestion prior to being inserted into our database. Any raw data disseminated at this stage are filtered based on these preliminary QC flags.

Near-Real-Time:

Within a short period of time, data is additionally QC at a more detailed level via an QC software automated process.

CO-OPS 24x7 monitors the data and use information from QC results and other tools to QA/QC the data and stop dissemination to the public of bad data that still passed basic QC.

Monthly Data Processing:

CO-OPS Data Processing Team, on a monthly basis, generates quality controlled verified data products. CO-OPS uses this data for longer term water level records.

Acquisitions data

CO-OPS acquisition data is reviewed by the contracting officer. Data is verified by the contracting officer contacts via Email and phone calls; this process is used to verify information provided by the vendor.

HR Data

CO-OPS Human resources (HR) data is validated at the time of receipt by the HR representative. The HR representative compares picture Identification (ID) and other information to validate the applicant's identity. For travel, the HR representative also validates the information at the time of collection. This includes comparison of Driver's License and Passport. HR data for travel is only used to assist the employee in making travel arrangements and is not stored. Applicant data is only maintained during the hiring process. This information aids in managing administrative programs related to an employee or contractor's employment status, travel, and other human capital resources activities. Emergency contact information is collected for each employee.

The Division Chiefs and Deputies within CO-OPS also use this information in communicating with employees during emergencies and contingent events. Ensuring the accuracy of information provided by employees, contractors, volunteers and partner agency staff who use the system is the responsibility of the division chief, team lead, or contracting officer.

None of the administrative processes listed (mission, acquisitions, or HR data) require Social Security numbers (SSNs). SSNs have been deliberately removed from CO-OPS' administrative processes for some time now. 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 is required to ensure the accuracy of this information.

Vendor provided BII is also collected in the form of contract 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

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB control Number: 0648-0342, NOAA Website Satisfaction Survey (webpage: Survey) OMB control number: 0648-0762, 3D Nation Elevation Data Requirements and Benefits Study
	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 owned by the facilities management at Chesapeake and accessed by the Field Operations Division (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. The Chesapeake surveillance system is a standalone, low image quality video system provided by the facilities managers at Chesapeake to their CO-OPS tenants. The video quality of the system renders it unable to gather PII which may be displayed on an individual. It is also not the purpose of the device to capture or store any PII and any potential 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 separate PIV cards, containing only the users name, are used to gain entry, but do not store any of the data embedded on the card.			
	There is 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 fulfill the 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).

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 and human resource 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. This information aids in determining web measurement and customization needs as well as to help improve the overall service that CO-OPS provides online. 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 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 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.

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 sign rules of behavior to ensure they understand their responsibilities to the system and that data which resides on it.

NOAA6205 utilizes the National Ocean Service (NOS) Microsoft Active Directory to enforce user identification and authorization to access the information system. NOAA6205 uses NOAA0100 ArcSight (a security appliance used by NOAA0100 to monitoring and tracking logs) audit logging. NOAA uses Common Access Card (CAC)/Identity, credentialing, and access management (ICAM)/Multifactor authentication (MFA) to authenticate user access. NOAA6205 uses data encryption at rest and in transit. Public facing systems authenticate through NOAA ICAM where required. All users are vetted and background investigations are performed before access to the information system is granted. The Least privilege access method is employed in the system and only allows authorized users to access the data. Data in the information system is encrypted and all PII or BII data is encrypted with a Federal Information Processing Standards (FIPS)140-2 encryption method while at rest with the NOS enterprise Trellix Endpoint encryption solution. The DOC KiteWorks secure email system is used to transmit PII/BII data.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

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

X	<p>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:</p> <ul style="list-style-type: none"> • NOAA0100 (NOAA Cyber Security Center) for IT security services– no shared Personally Identifiable Information/Business Identifiable Information (PII/BII) • NOAA0550 (NOAA N-Wave is the name of network service provider for NOAA) for network connectivity – no shared PII/BII • NOAA8870 (National Weather Service Telecommunication Gateway). NOAA6205 sending data to National Weather Service (NWS) via NOAA internal network– no shared PII/BII • NOAA6001 (NOS Enterprise Information System) The interconnection with NOAA6001 is utilized for connections to NOS hosted applications and NOAA campus backbone – no shared PII/BII NOAA6205 also utilizes NOAA virtual private network (VPN) for remote connectivity and NOAA N-Wave for connection to AWS East-West Federal Risk and Authorization Management Program (FedRamp) Cloud hosting protected by secure sockets layer (SSL)– no shared PII/BII <p>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 pushes Standard Hydrometeorological Exchange Format (SHEF)/Character Form for the Representation and EXchange of data (CREX) bulletin data to NWS, these are regular station observation data ((water level (WL), meteorological (met)) and does not contain any PII.</p> <p>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 two factor authentication (2FA) for all accounts), restrictions in firewall access-control list (ACL) and security permissions on specific network folders where documentation is stored.</p> <p>NOAA6205 also connects to NOAA0100, NOAA0550, and NOAA8870.</p>
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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): Guest researchers and individuals from allied nations may have access to the system, but will not have access to PII/BII.			

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://tidesandcurrents.noaa.gov/privacy.html	
X	Yes, notice is provided by other means.	<p>Specify how:</p> <p>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 does not capture photographs for badging since that is performed (and stored) by the NOAA Office of Security. CO-OPS does utilize staff pictures (with written permission) as part of either internal or external website as part of CO-OPS program, possible profile narrative, and/or presentation of CO-OPS mission activities.</p> <p>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.</p> <p>CO-OPS staff members (employees) are provided notice of information to be collected from them upon hire as well as via CO-OPS 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.</p> <p>Vendor provided BII is collected in the form of contract 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.</p>

	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.	<p>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.</p> <p>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.</p> <p>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.</p>
	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.	<p>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.</p> <p>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.</p> <p>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.</p> <p>Vendor provided BII is collected in the form of contract 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.</p>
	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.	<p>Specify how: Visitors to the CO-OPS site provide current information when contacting us.</p> <p>CO-OPS employees and contractors are queried on a quarterly basis, during which they can provide updates.</p> <p>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.</p> <p>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.</p>
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>04/08/2024</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the 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).

NOAA6205 utilizes the National Ocean Service (NOS) Microsoft Active Directory to enforce user identification and authorization to access the information system. NOAA6205 uses ArcSight audit logging, CAC/ICAM/MFA. Data encryption at rest and in transit. Public facing systems authenticate through NOAA ICAM where required. All users are vetted and background investigations are performed before access to the information system is granted. Least privilege is employed in the system and only those users authorized access to information are allowed access to the data. Data in the information system is encrypted and all PII or BII data is encrypted with a FIPS140-2 encryption method while at rest. CO-OPS utilizes laptop computers for end users and we encrypt all laptops with the NOS enterprise Trellix Endpoint encryption solution. The DOC KiteWorks secure email system is used to transmit PII/BII data.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?
 X Yes, the PII/BII is searchable by a personal identifier.
 _____ 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	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i></p> <ul style="list-style-type: none"> • COMMERCE/DEPT-31: Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations. • COMMERCE/DEPT-25: Access Control and Identity Management System • GSA/GOVT-7: Federal Personal Identity Verification Identity Management System (PIV IDMS) • OPM/GOVT-1: General Personnel Records • COMMERCE-NOAA-11 Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission; • COMMERCE/DEPT-18, Employees Information Not Covered by Notices of Other Agencies; • COMMERCE/DEPT-2, Accounts Receivable; • COMMERCE/DEPT-6, Visitor Logs and Permits for Facilities under Department Control; • COMMERCE/DEPT-13, Investigative and Security Records. • COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other • Persons, • GSA-GOVT-9, System for Award Management, GSA-GOVT-10, FAR Data Collection System.
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	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	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p> <p>Chapter 100 - General (Updated 9/2020) Chapter 200 - Administrative and Housekeeping Records (Updated 9/2020) Chapter 300 - Personnel (Updated 7/2020) Chapter 700 - Procurement Supply and Equipment Maintenance (Updated 6/2020) Chapter 900 - Facilities Security and Safety (Updated 6/2020) Chapter 1000 - Motor Vehicle Management and Transportation Service (Updated 7/2020) Chapter 1100 - Printing Binding Duplication and Distribution Records (Updated 5/2017) Chapter 1200 - Scientific Research (Updated 10/2017) Chapter 1300 - Weather (Updated 1/2020) Chapter 1400 - Satellites and Data Centers (Updated 10/2017) Chapter 1500 - Marine Fisheries (Updated 2/2018) Chapter 1600 - Ocean Programs (Updated 8/2020) Chapter 1700 - NOAA Corps (Updated 8/2020) Chapter 1800 - Marine and Aviation Technology (Updated 6/2016) Chapter 2100 - Sea Grants (Updated 5/2018) Chapter 2200 - Records of the Chief Information Officer (Updated 5/2018) Chapter 2300 - General Information Technology Management Records (Updated 5/2018) Chapter 2400 - Information System Security Records (Updated 5/2018)</p>
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.

	No, retention is not monitored for compliance to the schedule. Provide explanation:
--	---

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

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

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, 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 level.
(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 non-sensitive information. No sensitive information is collected.
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. CO-OPS does not capture photographs for badging since that is performed (and stored) by the NOAA Office of Security. CO-OPS does utilize staff pictures (with written permission) as part of either internal or external website as part of CO-OPS program, possible profile narrative, and/or presentation of CO-OPS mission activities.
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. The storage of PII is primarily temporary and the data is kept only in access control restricted locations to minimize the number of authorized users. Documents are also stored to restricted shared networks, restricted based on single individual or CO-OPS division based on need to know. Any requested changes or additions of individuals to restricted folders must be approved by the supervisor along with security team representative as part of the change management process. All Travel documents and Acquisition documents are kept in accordance with the record retention schedule for auditing requirements.
	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 role-based access control (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.