

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

Catrina D. Purvis Digitally signed by Katrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.12.01 15:51:41 -05'00'

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):					

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

System Administration/Audit Data (SAAD)			
a. User ID	X	c. Date/Time of Access	X
b. IP Address	X	d. Queries Run	
		e. ID Files Accessed	
		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
Telephone		Email	X
Other (specify):			

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

<input type="checkbox"/>	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.

<input type="checkbox"/>	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): 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: <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.</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 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.</p> <p>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.</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. Specify how: <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.</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</p>
---	--

		<p>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:</p> <p>For visitors to the CO-OPS site, the one purpose of collecting the information is described in the Privacy Act Statement. CO-OPS 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 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.</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:</p> <p>Visitors to the CO-OPS site provide current information when contacting us.</p> <p>CO-OPS staff members are queried on a quarterly basis, during</p>
---	---	---

		<p>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	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p>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.</p>
X	<p>The information is secured in accordance with FISMA requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&A): <u>November 4, 2014</u></p> <p><input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.</p>
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 <i>(list all that apply)</i> : 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 <u>(date)</u> .
	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.