

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



**Privacy Threshold Analysis
for the**

**Center for Operational Oceanographic Products and Services PORTS®
and NWLON IT System (NOAA6205)**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/ Center for Operational Oceanographic Products and Services

PORTS® and NWLON IT System

Unique Project Identifier: NOAA6205

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

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.

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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

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

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

b) *System location*

The headquarters for NOAA6205 is located in Silver Spring MD, 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

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)*

The system resides on the NOAA NOS network as a standalone system and does not share privacy data with other NOAA systems via interconnection.

- d) *The purpose that the system is designed to serve*

The NOS CO-OPS collects and distributes observations and predictions of water levels and currents to ensure safe, efficient, and environmentally sound maritime commerce. It performs data processing capabilities and operational data analysis/quality control. It produces and disseminates oceanographic products, such as the products required by the National Weather Service to meet flood and tsunami warning responsibilities, and the products required by FEMA for response to maritime events.

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 and include federal employees and contractors.

The CO-OPS PORTS® and NWLON System (NOAA6205) and the infrastructure components that store, process, and transmit 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, 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 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. NOAA6205 also has servers within the Microsoft Azure Cloud system. These are identified in the NOAA6205 Hardware Inventory.

e) The way the system operates to achieve the purpose

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 IaaS and PaaS within both Azure and AWS. These cloud based services do not host, process, or transmit any PII. 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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

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.

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.

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) Identify individuals who have access to information on the system

NOAA6205 users are uniquely identified and authenticated before accessing NOAA6205 IT resources. NOAA6205 users can be employees, contractors, guest researchers, and individuals from allied nations that have been granted system access. Identification and authentication to NOAA6205 is done via NOAA LDAP, NOAA6205 LDAP, or Access Manager. These three identification and authentication types are detailed below:

1. **Active Directory:** Applications using this authentication type connect to a NOAA-operated LDAP server for the purposes of unique user identification and authorization. Connections of this type are made via SSL/TLS. The NOAA LDAP servers are operated at the NOAA level, and account and access requests are handled via requests entered via NOAA6205's Jira ticketing system, and are assigned to a system administrator with privileges to provision or remove NOAA LDAP accounts.
2. **NOAA6205 LDAP:** The NOAA6205 LDAP is a clustered instance of OpenLDAP for the purposes of unique user identification and authorization for NOAA6205 Linux servers and applications. Applications utilizing this connection type connect to either the primary or secondary NOAA6205 LDAP servers, connecting via SSL/TLS. Account requests for this type are handled via NOAA6205's Jira ticketing system and are assigned to a system administrator with privileges to provision or remove NOAA6205 LDAP accounts.

3. Access Manager: Applications utilizing this connection type connect via SSL to a database-driven authentication application used to uniquely identify users of various applications. Requests for new accounts or closures of existing accounts are handled via NOAA6205's Jira ticketing system.

NOAA6205 maintains web servers that have publicly accessible information. This information is accessible anonymously using the HTTP and FTP protocols. However, individuals are uniquely identified and authenticated in order to change information on the web servers.

h) 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 HTTP and FTP protocols. However, individuals are uniquely identified and authenticated in order to change information on the web servers.

i) 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. 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 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

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

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

- This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

- Yes. This is a new information system.
- Yes. This is an existing information system for which an amended contract is needed.
- No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

X No. This is not a new information system.

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

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

X Yes. (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.			

___ No.

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

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

X Yes, the IT system collects, maintains, or disseminates BII.

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

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

X DOC employees

- Contractors working on behalf of DOC
- Other Federal Government personnel
- Members of the public

No, this IT system does not collect any PII.

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

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

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

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

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

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

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

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

No, the context of use will not cause the assignment of a higher PII confidentiality

impact level.

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

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the NOAA6205 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 I certify the criteria implied by the questions above **do not apply** to the NOAA6205 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>Information System Security Officer or System Owner Name: Marian Westley Office: NOAA/NOS/CO-OPS Phone: 240-533-0481 Email: Marian.westley@noaa.gov</p> <p>Signature: <u>WESTLEY.MARIA</u> <small>Digitally signed by WESTLEY.MARIAN.B.1365896638</small> Date signed: <u>N.B.1365896638</u> <small>Date: 2020.12.11 14:15:22 -05'00'</small></p>	<p>Information Technology Security Officer Name: John Parker Office: NOAA/NOS Phone: 240-533-0832 Email: John.d.parker@noaa.gov</p> <p>Signature: <u>PARKER.JOHN.D.1365835914</u> <small>Digitally signed by PARKER.JOHN.D.1365835914</small> Date signed: <u>914</u> <small>Date: 2020.12.14 15:31:21 -05'00'</small></p>
<p>Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 828-257-3148 Email: Adrienne.Thomas@noaa.gov</p> <p>Signature: <u>THOMAS.ADRIENNE.M.1365859600</u> <small>Digitally signed by THOMAS.ADRIENNE.M.1365859600</small> Date signed: <u>M.1365859600</u> <small>Date: 2020.12.14 16:19:25 -05'00'</small></p>	<p>Authorizing Official Name: Richard Edwing Office: NOAA/NOS/CO-OPS Phone: 240-533-0482 Email: Richard.edwing@noaa.gov</p> <p>Signature: <u>EDWING.RICHARD.F.1365829620</u> <small>Digitally signed by EDWING.RICHARD.F.1365829620</small> Date signed: <u>D.F.1365829620</u> <small>Date: 2020.12.11 13:36:27 -05'00'</small></p>
<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov</p> <p>Signature: <u>GRAFF.MARK.HYRUM.151447892</u> <small>Digitally signed by GRAFF.MARK.HYRUM.151447892</small> Date signed: <u>47892</u> <small>Date: 2021.01.05 12:54:07 -05'00'</small></p>	