Version Number: 01-2019

U.S. Department of Commerce
NOAA

Privacy Threshold Analysis
for the

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

U.S. Department of Commerce Privacy Threshold Analysis

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

Unique Project Identifier: 006-48-01-15-01-3402-00

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

Description of the information system and its purpose: The National Ocean Service (NOS) 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.

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

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

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

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

System Interconnections/Information Sharing

System Information
NOAA0100 Organization: N-CIRT Network
NOAA0200 Organization: NOAA Network Operations Center (NOC)
NOAA3100 Organization: OAR Pacific Marine Environmental Laboratory (PMEL)
NOAA5004 Organization: Data Collection System Automatic Processing System
NOAA6001 Organization: NOS Enterprise Information System
NOAA8870 Organization: National Weather Service Telecommunication Gateway

d) The purpose that the system is designed to serve

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.

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.

f) A general description of the type of information collected, maintained, use, 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.

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

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.

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.

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.

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. 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.*

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

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

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

_X_ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	X*
Video surveillance	X	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.

____ 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
- ____ National Institute of Standards and Technology Associates
- _X_ Contractors working on behalf of DOC
- ____ Other Federal Government personnel
- _X_ Members of the public

____ No, this IT system does not collect any PII.

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

4b. Does the IT system collect, maintain, or disseminate 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.

_X_ 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?

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

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

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.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

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

CERTIFICATION

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

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

Name of Information System Security Officer (ISSO) or System Owner (SO): Marian Westley

Signature of ISSO or SO: WESTLEY.MARIAN.B.1365896638 Digitally signed by WESTLEY.MARIAN.B.1365896638 Date: 2019.12.05 15:01:48 -05'00' Date: 12/5/2019

Name of Information Technology Security Officer (ITSO): John Parker

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2019.12.09 09:40:51 -05'00' Date: _____

Name of Authorizing Official (AO): Richard Edwing

Signature of AO: EDWING.RICHARD.F.1365829620 Digitally signed by EDWING.RICHARD.F.1365829620 Date: 2019.12.05 15:18:14 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2019.12.17 08:54:21 -05'00' Date: _____