

**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

NOAA6205

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).

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. 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.

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).

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):					

- X This is an existing information system in which changes do not create new privacy risks. *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.

- _____ Yes. *Please describe the activities which may raise privacy concerns.*

- X 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.)."

☒ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

☒ Companies

☒ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

☒ DOC employees

☒ Contractors working on behalf of DOC

☒ 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 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.

4c. 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, and/or 4c 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 NOAA6205 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): Maurice McLeod

Signature of ISSO or SO: MCLEOD.MAURICE.ST
GEORGE.1267033699  Digitally signed by MCLEOD.MAURICE.ST
GEORGE.1267033699
Date: 2017.11.30 08:15:28 -05'00' Date: _____


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

Signature of ITSO: PARKER.JOHN.D.1365835914  Digitally signed by PARKER.JOHN.D.1365835914
Date: 2017.12.06 02:12:37 -05'00' Date: _____

Name of Authorizing Official (AO): Richard Edwing

Signature of AO: EDWING.RICHARD.F.1
365829620  Digitally signed by
EDWING.RICHARD.F.1365829620
Date: 2017.11.30 08:41:51 -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
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892
Date: 2017.12.27 10:16:35 -05'00' Date: _____