

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration
(NOAA)
National Ocean Service (NOS)
Office of Response and Restoration**



**Privacy Threshold Analysis
for the
NOAA6701, Office of Response and Restoration Local Area
Network**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOS/OR&R LAN

NOAA6701

Unique Project Identifier: NOAA6701

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: *Provide a general description of the information system and its purpose in a way that a non-technical person can understand.*

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).

NOAA6701 provides services to the Assessment Restoration Division (ARD), Emergency Response Division (ERD), Marine Debris Program (MDP) and the General Counsel for Natural Resources (GCNR) office. Services include help desk support, file sharing, data storage, and print services for the organizational units. NOAA6701 enables use of other external enterprise services on the campus networks, as well as provides Internet connectivity. NOAA6701 provides an operational environment supporting the mission and staff of the program offices located on the Silver Spring Metro Center Campus, Western Regional Center campus, Mobile Disaster Response Center, and all regional staff. NOAA6701 supports user identification, human resources, travel, passport, and cost recovery, which in some instances may require the collection of PII or BII.

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	X	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	X
j. Other changes that create new privacy risks (specify): NOAA6703 that included the Disaster Response Center (DRC) was merged into NOAA6701. During the review of data collected in the NOAA6703 boundary it was discovered that there was additional PII. We will also be including data from public surveys.					

☐ This is an existing information system in which changes do not create new privacy risks. *Continue to answer 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. See Item 1J.*

☐ 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 [IT SYSTEM NAME] 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):

Russell Worman

Signature of ISSO or SO: WORMAN.RUSSELL.8 LOWELL.1153249918 Digitally signed by WORMAN.RUSSELL.LOWELL.115324991
Date: 2017.11.02 09:41:30 -07'00' Date: 11/02/2017

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

Signature of ITSO: PARKER.JOHN.D.13658 35914 Digitally signed by PARKER.JOHN.D.1365835914
Date: 2017.11.02 13:02:58 -04'00' Date: 11/2/2017

Name of Authorizing Official (AO): Dave Westerholm

Signature of AO: WESTERHOLM.DAVID.G.1083783156 Digitally signed by WESTERHOLM.DAVID.G.1083783156
Date: 2017.11.06 15:32:44 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): MARK GRAFF

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 514447892 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: 2017.11.07 08:28:32 -05'00' Date: _____