Version Number: 01-2017

U.S. Department of Commerce
National Oceanic and Atmospheric Administration

Privacy Threshold Analysis
for the

Office of Response and Restoration Products System (ORRPS), NOAA6702

U.S. Department of Commerce Privacy Threshold Analysis

Office of Response and Restoration Products System (ORRPS), NOAA6702

Unique Project Identifier: NOAA6702

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 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).

NOAA6702 NOS OR&R operates the Office of Response and Restoration Products System (ORRPS). ORRPS is comprised of products developed and published by the Divisions within OR&R - Assessment and Restoration Division (ARD), the Emergency Response Division (ERD), Disaster Response Center (DRC) and Marine Debris Program (MDP). The ORRPS incorporates the product systems from these divisions. ORRPS is currently located in the Amazon Web Services (AWS) East/West FedRamp cloud. The applications currently include the Environmental Response Management Application (ERMA®) subsystem and the Data Integration, Visualization, Exploration, and Reporting (DIVER) subsystem application as part of the system boundary. The other websites currently hosted in ORRPS, include the Marine Debris, NOAA Response Asset Directory (NRAD), NOAA's Damage Assessment Remediation and Restoration Program (DARRP), and the OR&R Intranet. NOAA6702 has user identification requirements and applications that support assessment and restoration of natural resources, which 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.*

_X__ This is an existing information system that does not have an approved PIA, 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): NOAA6702 underwent initial Assessment and Authorization (A&A) in 2017 and after ISSO/ITSO review of the system data types and documentation it was determined that the system required a PIA.					

____ 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 later). *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.

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

NOAA6702 gathers information for user authentication which may have PII and information collected during the incidents that may be used for litigation which may include BII.

____

____ 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 about: *(Check all that apply.)*

___X_ Companies
___X_ 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.)*

__X__ DOC employees
__X__ Contractors working on behalf of DOC
___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 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.

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.

_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, 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 NOAA6702 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):

_____Nancy Wallace_____

Signature of ISSO or SO: WALLACE.NANCY.E.1382920305 Digitally signed by WALLACE.NANCY.E.1382920305 Date: 2018.03.13 11:50:52 -04'00' Date: _____

Name of Information Technology Security Officer (ITSO): __John D. Parker_____

Signature of ITSO: PARKER.JOHN.D.1365835914 Digitally signed by PARKER.JOHN.D.1365835914 Date: 2018.03.13 20:40:24 -04'00' Date: 3/13/18

Name of Authorizing Official (AO): ____Dave Westerholm_____

Signature of AO: _____ Date: 3/13/2018

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: 2018.03.20 15:59:56 -04'00' Date: _____

MARLIN.CHERYL.LEE.1380926292 Digitally signed by MARLIN.CHERYL.LEE.1380926292 Date: 2018.03.14 07:52:15 -04'00'