

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



**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 006-000351103 00-48-02-00-02-00**

**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 Oceanic and Atmospheric Administration (NOAA), National Ocean Service (NOS), Office of Response and Restoration (OR&R) is the focal point in NOAA for preventing, planning for, and responding to oil spills, releases of hazardous substances, and hazardous waste sites in coastal environments and restoring affected resources. OR&R protects and restores coastal resources through the application of science and technology. On behalf of the public, OR&R addresses environmental threats from catastrophic emergencies such as the oil spills of the ship, Exxon Valdez or the oil drilling rig of the Deep Water Horizon; chronic releases from contaminated sediments such as the Hudson River Superfund site; and vessel groundings in sanctuaries such as coral reefs in the Florida Keys. By working in partnerships, OR&R empowers communities and decision makers to be coastal stewards by transferring the results of its experience through training, guidance, and decision-making tools that emphasize actions to take to improve coastal health.

NOS OR&R operates the Office of Response and Restoration Products System (ORRPS), NOAA6702. 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 system is a cloud based solution operating the Environmental Response Management Application (ERMA®) subsystem, the Data Integration, Visualization, Exploration, and Reporting (DIVER) subsystem, the Marine Debris website, NOAA Response Asset Directory (NRAD) website, NOAA's Damage Assessment Remediation and Restoration Program (DARRP) website, Response and Restoration website, and the OR&R Intranet website. NOAA6702 has user identification requirements and applications that support assessment and restoration of natural resources, which may require the collection of PII or BII.

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*

NOAA6702 is a general support system. 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), Business Services Group (BSG), Marine Debris Program (MDP), and the Disaster Preparedness Program (DPP). NOAA6702 hosts public and non-public web sites and applications. NOAA6702 does host websites and applications that collect and/or disseminate PII in the form of images, photographs, video and/or audio may recordings No social media sites are operated for OR&R from NOAA6702.

*b) System location*

NOAA6702 is located in the Amazon Web Services (AWS) East/West FedRamp cloud.

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

NOAA6702 interconnects with NOAA6701, the Office of Response and Restoration Local Area Network LAN (LAN). This connection provides secure connection for management for NOAA6702 and NOAA6701 provides the logistics, support, development, etc. for NOAA6702.

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

NOAA6702 hosts the applications including Environmental Response Management Application (ERMA<sup>®</sup>) 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 Program web site and Blog, NOAA Response Asset Directory (NRAD), NOAA's Damage Assessment Remediation and Restoration Program (DARRP), Office of Response and Restoration public web page and Blog, and the OR&R Intranet. These applications allow OR&R to

fulfill its mission responding to disasters that affect our nation's coasts and water ways and restore the environment to its pre-disaster state.

*e) The way the system operates to achieve the purpose*

NOAA6702 is an Internet connected system that is in a virtual environment in the AWS cloud. The cloud allows OR&R to utilize the "Elastic" capabilities of the cloud to rapidly ramp up response tools such as ERMA and DIVER for large responses and downsize when the disaster is over. NOAA6702 hosts the applications including Environmental Response Management Application (ERMA<sup>®</sup>) 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 Program web site and Blog, NOAA Response Asset Directory (NRAD), NOAA's Damage Assessment Remediation and Restoration Program (DARRP), Office of Response and Restoration public web page and Blog, and the OR&R Intranet. These applications allow OR&R to fulfill its mission responding to disasters that affect our nation's coasts and water ways and restore the environment to its pre-disaster state.

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

The PII collected in NOAA6702 may include information needed to establish accounts for non-NOAA and public users who subscribe to ORR newsletters, take training classes offered by ORR (Name, address, email address and organization/affiliation and for those who take surveys in order that we may mail follow-up surveys to those who consent (including age, level of education, numbers of adults and children in family, name and home address). Information for audit logging of IT systems such as User ID, IP Address, and Date/Time of Access may be collected. The NOAA6702 system enables OR&R in providing public outreach, communication, and employee/partner recognition on our public web sites which may include photos, biographies, and award recognition. BII collected is data related to oil/chemical spills that maybe traced to a business entity with some liability in a case. The case data, when a case is active, may contain BII (oil spill evidence identifying the source of the spill) This data may be used in settlement negotiations and litigation.

*g) Identify individuals who have access to information on the system*

OR&R has dedicated staff assigned by duties such as system administrators and managers whose access to the files are managed through role based access controls. Non-NOAA users and members of the public have access to the publically available web sites and applications in NOAA6702.

*h) How information in the system is retrieved by the user*

Data is retrieved using Government Furnished Equipment (GFE) to open, review, verify, and securely delete the information for NOAA personnel updating and maintaining the applications in NOAA6702. General public users do not require accounts to access public sites including public outreach, communication, employee/partner recognition which may include photographs, video and/or audio recordings, and biographies. Non-NOAA partners who require access to applications that are not publicly available use username and passwords. All the sites which are hosted utilize SSL/TLS certificates for enhanced security through the user's browser.

*i) How information is transmitted to and from the system.*

Information in NOAA6702 is mostly collected through online web applications, forms. Any information that is collected through an e-mail link is then collected and maintained by NOAA6701 in its support role for NOAA6702. Applications such as ERMA in NOAA6702 share data with other federal agencies such as the Coast Guard, DOI, and DHS. Homeland Security Infrastructure Program (HSIP) data comes from a Department of Homeland Security (DHS) mapped server (mapping system similar to ERMA). ERMA Receives ship location information from Nationwide Automatic Identification System (NAIS) from the Coast Guard's secure server. Encryption of data in transit is used for system connections.

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.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>			
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). *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.

Yes. *(Check all that apply.)*

<b>Activities</b>	
Audio recordings	Building entry readers
Video surveillance	Electronic purchase transactions
Other (specify):	

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.

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."

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

DOC employees

National Institute of Standards and Technology Associates

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

Dana Larson

Signature of ISSO or SO: \_\_\_\_\_ Date: \_\_\_\_\_

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

Signature of ITSO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Authorizing Official (AO): Scott Lundgren

Signature of AO: \_\_\_\_\_ Date: \_\_\_\_\_

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

Signature of BCPO: \_\_\_\_\_ Date: \_\_\_\_\_