

# U.S. Department of Commerce

## NOAA



### Privacy Threshold Analysis for the NOAA4500 - West Coast Region (WCR) Network

## U.S. Department of Commerce Privacy Threshold Analysis NOAA4500 - West Coast Region (WCR) Network

**Unique Project Identifier:** 006-48-01-14-02-3305-00

**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 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 West Coast Region (WCR) of NOAA Fisheries is a General support system.

*b) System location*

Seattle, WA  
Portland, OR  
Santa Rosa, CA  
Sacramento, CA  
Arcata, CA  
Long Beach, CA

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

The Information System is interconnected with the NMFS Enterprise Wide Area Network (NOAA4000)

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

The purpose of the NOAA4500 Information System is to provide access to automated systems typically found in administrative offices within the federal government.

We work to conserve, protect, and manage salmon and marine mammals under the Endangered Species Act and Marine Mammal Protection Act, and sustainably manage West Coast fisheries as guided by the Magnuson-Stevens Fisheries Conservation Act.

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

To achieve this mission and advance sound stewardship of these resources, we work closely with tribes, local, state and federal agencies, our stakeholders, and partners to find science-based solutions to complex ecological issues.

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

Authorizations and Permits for Protected Species (APPS)

The PII/BII collected by the IT system is from federal and state employees, members of the public, and employees/members of Tribal Nations. The information is used to verify that the individual has the necessary qualifications to conduct research on protected species. Applicants provide a curriculum vitae or resume documenting their academic and/or work related experience with the methods and procedures they plan to use on protected species.

NOAA4500 System Maintenance Information

Federal and Contractor Employee data:

Names, addresses, and email addresses collected from employees and contractors are used to manage account information for access control to systems and web applications.

Names and work email addresses of employees and contractors are used to direct the public to appropriate personnel within the organization.

For emergency, disaster recovery, and continuity of operations, employee and contractor names, work and home emails and work and home telephone numbers are collected.

eDiscovery Application

The information is used in the review process, in which approved users redact the scanned documents before it is released to the requestor. The application does not actually save the data; it only saves the metadata or pointers to the scanned document.

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

Authorizations and Permits for Protected Species (APPS): Authorized Federal Employees and contractors that access the system with username and password.

---

NOAA4500 System Maintenance Information: WCR IT Staff only

---

eDiscovery Application: Authorized Federal Employees and contractors that access the system with username and password

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

**Authorizations and Permits for Protected Species (APPS)**

The web based system contains applications for permits required by the Marine Mammal Protection Act (MMPA) and the Endangered Species Act (ESA). Researchers use the system to submit an application which contain PII (employment and education information) prior to receiving a scientific research permit. Information collected is not shared outside of NOAA4500. NOAA Fisheries protects PII stored in APPS by minimizing the use and collection of PII. NOAA Fisheries also protects PII stored in APPS by controlling access to the information. APPS requires users to authenticate their identity by entering a username and password.

**eDiscovery Application**

The eDiscovery Platform system is a web-based application used to simplify agency response to Freedom of Information Act (FOIA) requests, aid in the processing Administrative Records (AR), and to a lesser extent, Congressional Inquiries and Legal Holds. The system serves as a single point for the collection, review, tagging, redaction and export of responsive records. The Information System protects PII stored in the eDiscovery Application by minimizing the use and collection of PII. The Information System also protects PII stored in APPS by controlling access to the information. The eDiscovery Application requires users to authenticate their identity by entering a username and password.

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

**NOAA4500 System Maintenance Information:**

NOAA4500 utilizes Data Resource Accounts and Group Memberships to allow authorized staff to access NOAA4500 Data which may contain PII or BII. Computer account types include, but are not limited to, Domain Accounts, Email/LDAP Accounts, Unix Accounts, Intranet Accounts, and Local System Accounts. Group memberships are used to assign Security Access Levels to authorized Data Resource Accounts. NOAA4500 applies Least Privilege and Least Functionality principles when providing security clearance. Access Enforcement Mechanisms (Encryption-at-Rest, Encryption-in-Transit, Distributed Directory Services) are implemented to prevent malicious or accidental access by unauthorized persons.

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.)

Activities			
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 PIA 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 NOAA4500 - WCR Network 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):

Brett W. Amedick

Signature of ISSO or SO: AMEDICK.BRETT.WILLIAM.1259412729 Digitally signed by AMEDICK.BRETT.WILLIAM.1259412729 Date: 2020.08.04 14:06:31 -07'00' Date: \_\_\_\_\_

Name of Information Technology Security Officer (ITSO): Catherine Amores

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2020.08.18 15:54:00 -04'00' Date: \_\_\_\_\_

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.08.19 14:16:48 -04'00' Date: \_\_\_\_\_

Name of Authorizing Official (AO): Scott M. Rumsey

Signature of AO: Scott Rumsey Digitally signed by RUMSEY.SCOTT.M.1365888341 Date: 2020.08.19 09:36:07 -07'00' Date: \_\_\_\_\_

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

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.08.20 07:40:24 -04'00' Date: \_\_\_\_\_