

**U.S. Department of Commerce  
NOAA**



**Privacy Threshold Analysis  
for the  
West Coast Region  
NOAA4500**

# U.S. Department of Commerce Privacy Threshold Analysis

## West Coast Region / NOAA4500

**Unique Project Identifier:** [Number]

**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:**

NOAA Fisheries is dedicated to protecting and preserving our nation's living marine resources through scientific research, fisheries management, enforcement, and habitat conservation. The West Coast Region of NOAA Fisheries administers fisheries programs along the coasts of Washington, Oregon and California; and in the vast inland habitats of Washington, Oregon, California and Idaho. 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. 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.

The NOAA4500 (West Coast Region [WCR] LAN) functions as the overall office automation support system for WCR, National Marine Fisheries Service (NMFS), National Oceanic Atmospheric Administration (NOAA) in multiple physical locations throughout the western United States.

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

**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 applications which contain PII (Employment and Education Information) prior to receiving research permit.

-----  
**NOAA4500 System Maintenance Information**

PII and BII information contained within the NOAA4500 system boundary provide the System Owner, ISSO, and administrators with the identity and contact information of all authorized users of the system. This information is used to reset passwords, notify users of outages, and support NOAA4500 COOP operations.

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):			

- 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.*

- 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.) Endangered Species Research Application Information.*

- 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 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 IT System.

- NOAA4500 will conduct a PIA.

       I certify the criteria implied by the questions above **do not apply** to the NOAA4500 IT System 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): \_\_\_\_\_

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

Name of Information Technology Security Officer (ITSO): \_\_\_\_\_

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

Name of Authorizing Official (AO): \_\_\_\_\_

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

Name of Bureau Chief Privacy Officer (BCPO): \_\_\_\_\_

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