

U.S. Department of Commerce
NOAA



Privacy Threshold Analysis
for the
NOAA4200 - Northeast Fisheries Science Center (NEFSC) Network

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOAA4200 – Northeast Fisheries Science Center (NEFSC) Network

Unique Project Identifier: NOAA4200

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).

- a) NOAA4200 is classified as moderate General System Support (GSS) system.
- b) The NOAA4200 consists of 4 local area networks (LAN) used to support the staff at the Northeast Fisheries Science Center (NEFSC). The NEFSC has scientific and administrative staff located in private, State and Federal Office buildings in Orono Maine, Woods Hole Massachusetts, Narragansett Rhode Island, Milford Connecticut, and Highlands New Jersey.
- c) NOAA4200 interconnects with Fisheries systems NOAA4000, NOAA4011, NOAA4100 and NOAA4400.
- d) The Northeast Fisheries Science Center Network is used to provide information technology support to all federal employees, contractors and volunteers. A volunteer is subject to the same security clearance requirements as an employee or contractor. Volunteers would assist with rudimentary tasks, such as stuffing envelopes for fish age structure collection or serving as an unpaid student intern for field work experience for a short period of time.
- e) The network provides access to essential NOAA services such as email, the Internet, shared printer, copiers, plotters, software applications and files. Information and data that are processed, analyzed and summarized include environmental, biological, chemical, technical, and other administrative data that scientists, managers and administrators use to support the NMFS mission related research and management programmatic decision processes.
- f) **For administrative matters:**
Work-Related Data: is required to determine eligibility for access to federal buildings and information technology (IT) resources. Resumes, which contain work history, may be included on employee profile websites. The posting of employee profiles is voluntary. Information is collected from federal employees, contractors and volunteers.

Identifying Numbers: Vehicle identifiers are used to match to parking decals which are placed on the vehicle of each person to authorize parking at the federal facility. The parking decal may be a sticker or a temporary parking pass. The license plate number is collected so the parking pass or decal can be linked to the proper vehicle. This information is required all persons parking at the federal facility, i.e. federal employees, contractors, volunteers, and all visitors.

General Personal Data: Name, Home Address, Home telephone number, and Personal Email Address are required for telework agreements, emergency contact forms, and emergency notification systems. Medical data is required to determine eligibility to participate on research cruises as a member of the scientific party. General personal data is required for employees if they have a telework agreement. Personal data for emergency notification systems are required for federal employees, contractors, and volunteers. System Administration/Audit Data (SAAD) is required to monitor, maintain and report IT security related activities on NOAA4200. This information is collected from federal employees and contractors.

Technologies Used Containing PII/BII not Previously Deployed: Building entry readers are required to maintain secure physical access to federal facilities and video surveillance is required to record activities, for security reasons, occurring on the grounds of federal facilities. Notices are posted on all buildings which notify that security cameras are in use. For civil and criminal enforcement activities: Identifying numbers on data collected from the fishing industry are shared (securely) with other intra-agency users such as the Greater Atlantic Regional Fisheries Office and the NMFS Office of Law Enforcement (OLE) who are required to use the data to regulate the fishing activities. The vessel and dealer ID numbers allow these data to be matched to each other and to other data sets collected by observers and OLE, such as VMS data. The interconnect agreements for the NOAA4200 provide the details on information sharing with other offices in NMFS. This information is collected from members of the public.

To aid the fishing industry to meet federal regulatory requirements for reporting:

Identifying numbers: Vessel federal and/or state fishing permit number; Dealer federal and/or state permit number; Fishing trip identifier; vessel registration numbers: The identifiers are required to be on commercial fisheries statistics data collected or reported by the fishing industry so these data can be associated with the proper entity. This information is collected from members of the public.

Access to legal guidance and regulations are provided on or through the NEFSC public web servers. Members of the public and employees, contractors, and volunteers are provided the laws and regulations under which these data are required or needed; i.e. 50 CFR 648 and 697. NOAA regulations for work related data and employee rights are posted on <https://www.csp.noaa.gov/policies/> and are available to all employees.

- g) Only NOAA4200 personnel has access to the system.
- h) User access the data using NOAA4200 GSS.
- i) Information is transfer on NOAA4200 GSS.

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, 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.

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.*)

Companies

Other business entities ((Fishing industry members to include dealers/processors and fishing vessels)

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.

