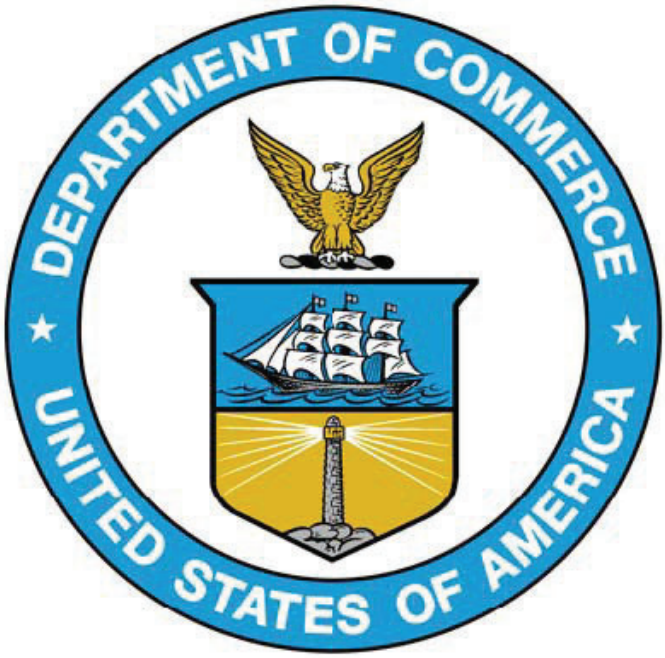
Version Number: 01-2021

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



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

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NMFS/NEFSC

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: *Provide a brief description of the information system.*

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).

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 fieldwork experience for a short period of time. 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, contact and procurement documentation and other administrative data that scientists, managers and administrators use to support the NMFS mission related research and management programmatic decision processes. The network also provides a mechanism to monitor and store facilities external camera systems that are required to maintain and observe the physical boundaries. The network also serves as a repository for data such as network access forms that contain information for center personnel that includes, but is not limited to signatures.

a) Whether it is a general support system, major application, or other type of system

NOAA4200 is classified as moderate General System Support (GSS) system.

b) System location

NOAA4200 supports local area network infrastructure in:

Woods Hole, MA
Narragansett, RI
Milford, CT
Highlands, NJ
Orono, ME

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

NOAA4200 has established inter-connect service agreements with:
NOAA4000 - NMFS Wide Area Network (WAN)
NOAA4011 - National Fishing Permit and Landing Reporting System (NFPLRS)
NOAA4100 - Greater Atlantic Regional Fisheries Office (GARFO)
NOAA4400 - Southeast Fisheries Science Center (SEFSC)
ACCSP – Atlantic Coastal Cooperative Statistics Program Interconnect Service Agreement

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

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 way the system operates to achieve the purpose*

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

The types of PII and BII that are collected and maintained are described below:
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 employees, contactors 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.

For civil and criminal enforcement activities:

Identifying numbers: on data collected from the fishing industry are shared (securely) with other interagency 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/websites. The posting of employee profiles is voluntary. Information is collected from federal and are available to all employees.

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

Only NOAA4200 personnel have access to the system.

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

Users access the data using NOAA4200 GSS. NOAA4200 personnel utilize Government Furnished Equipment (GFE) to access network resources. Two factor authentication is implemented for access to system resources. System access occurs from within the system boundary and via the NOAA4000 VPN appliance. Information can only be accessed by permitted NOAA personnel.

i) How information is transmitted to and from the system

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. Information is also shared via internal and external system interconnects. These connections occur through encrypted My SQL sessions or SSH sessions established between entities. These processes can be manual or automated through the use of scripting or chron jobs.

Questionnaire:

1. Status of the Information System

1a. 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 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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): WRD - procurement/contracting records are new; DFB - video recordings are a new collection.					

____ 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 *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

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. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	X
Video surveillance	X	Electronic purchase transactions	
Other (specify): 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 individuals that security cameras are in use.			

____ 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.

____ 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."

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

X DOC employees
X Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public
X Volunteers

____ 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?

X 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. NOAA4200 collects and maintains OF306 forms, as this is a requirement for Federal employment. SSNs are purged after being transmitted to Office of Security.
Provide the legal authority which permits the collection of SSNs, including truncated form. 5 U.S.C. 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance, and distribution of records.

____ 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?

_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.

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.

_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, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP 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 NOAA4200 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 NOAA4200 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Brian McGovern Office: NOAA/NMFS/NEFSC Phone: 202-964-1232 Email: Brian.McGovern@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: MCGOVERN.BRIAN.MICHAEL.1011403820 Digitally signed by MCGOVERN.BRIAN.MICHAEL.1011403820 Date: 2021.12.02 15:43:28 -05'00' Date signed: 12/2/2021	**Information Technology Security Officer** Name: Catherine Amores Office: NOAA/NMFS/OCIO Phone: 301-427-8871 Email: Catherine.Amores@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2021.12.07 16:58:52 -05'00' Date signed: 12/7/2021
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 240-577-2372 Email: Adrienne.Thomas@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.12.13 10:56:33 -06'00' Date signed: 12/13/21	**Authorizing Official** Name: Nicole Cabana Office: NOAA/NMFS/NEFSC Phone: 508-495-2279 Email: Nicole.Cabana@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: CABANA.NICOLE.MONIQUE.1237216586 Digitally signed by CABANA.NICOLE.MONIQUE.1237216586 Date: 2021.12.03 14:45:20 -05'00' Date signed: 12/3/21
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.12.16 17:10:00 -05'00' Date signed: 12/16/2021	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.