

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



Privacy Threshold Analysis for the
NOAA4100
Greater Atlantic Regional Office (GARFO) Network

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NMFS/Greater Atlantic Regional Office (GARFO) Network

Unique Project Identifier: NOAA4100

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: The Greater Atlantic Regional Fisheries Office Local Area Network (LAN) Infrastructure (System NOAA4100) is one of the National Oceanic & Atmospheric Administration's (NOAA) general support systems (GSS). A GSS is an interconnected information resource under the same direct management control that shares common functionality. The computer systems within GARFO provide service to our ultimate end beneficiaries, the habitat, the fish, and the environment; and to the biologists, scientists, statisticians, and economists within the region and nation; and all fishers who depend on our data.

The GARFO network operates using BII/PII for the purpose of administrative matters, litigation, civil enforcement activities, web measurement and customization technologies (single-session), administering human resource programs, promoting information sharing initiatives, criminal law enforcement activities and in support of GARFO business functions.

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).

Address the following elements:

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

The Greater Atlantic Regional Fisheries Office Local Area Network (LAN) Infrastructure (System NOAA4100) is one of the National Oceanic & Atmospheric Administration's (NOAA) general support systems (GSS). A GSS is an interconnected information resource under the same direct management control that shares common functionality. The computer systems within GARFO provide service to our ultimate end beneficiaries, the habitat, the fish, and the environment; and to the biologists, scientists, statisticians, and economists within the region and nation; and all fisheries who depend on our data.

b) System location

GARFO Primary location is in Gloucester, Ma with several satellite offices in: Hampton, VA; Northfield,

NJ; New Bedford, MA; Point Judith, RI; Portland, ME; Annapolis, MD; and Orono, ME.

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

The GARFO network maintains interconnection agreements with NMFS Headquarters in Silver Spring, MD (NOAA4000), NOAA Web Operations Center (NOAA0201) and the NMFS Northeast Fisheries Science Center (NOAA4200).

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

The GARFO network operates using BII/PII for the purpose of administrative matters, litigation, civil enforcement activities, web measurement and customization technologies (single-session), administering human resource programs, promoting information sharing initiatives, criminal law enforcement activities and in support of GARFO business functions.

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

Information on the GARFO network is retrieved through access controlled secure data applications and through secure database connections. All connections to the data have access control mechanisms in place and are encrypted.

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

NOAA4100 collects, maintains, and disseminates information used for identifying fisheries-related organizations and individuals, FOIA requests, fisheries specific data such as landing data from fish dealers, and catch based allocation data.

GARFO also collects and maintains PII for the following administrative support purposes:

1. For the employment onboarding process and HR administration: Employee ID, Financial Account (for setting up direct deposit, not kept in system after forwarding to U.S. Department of Agriculture (USDA)), Date of Birth, Driver's License, Passport, Alias, Gender, Age, Race, Home Address, Military Service, Occupation, Job title, Work History, Salary, Performance Plans, Fingerprints and Photographs (both forwarded to Defense Enrollment Eligibility Reporting System (DEERS) and not retained).
2. For establishing employee IT system user accounts: Name, Office, Government phone number, email address, and supervisor.

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

GARFO Employee PII is available only to the IT Staff and HR staff that is authorized to handle it, the IT Staff who are handle this data is made up of both federal employees and contract. HR Staff is only federal.

Permit information is shared within NMFS offices in order to coordinate monitoring and management of sustainability of fisheries and protected resources. Sources of information include the permit applicant/holder, other NMFS offices, the U.S. Coast Guard, the Northeast Fishery Management Council (NEFMC) and the Mid-Atlantic Fishery Management Council (MAFMC).

Permits BII is shared with State Fish and Game. The information (data for issuing fishing permits and permit histories, catch data collected from fishing vessels, landings data collected from fish dealers, and effort or catch based allocation data) shared within NMFS and State Fish and Game is to support both our mission and theirs. The State *Department of Fish & Game* works to preserve the state's natural resources and people's right to conservation of those resources, as protected by Article 97 of the Massachusetts Constitution. This includes civil and criminal law enforcement. The Department exercises responsibility over the Commonwealth's marine and freshwater fisheries, wildlife species, plants, and natural communities, as well as the habitats that support them.

The information listed above is also shared with:

The Northeast Fisheries Sciences Center (NEFSC), since we share some fisheries management responsibilities in the same regional area, much of our data collection, data analysis, and data dissemination roles either overlap or complement each other.

The Southeast Regional Office, as there is overlap in vessel activity with the Southeast Region, with vessels operating in both regions.

The Northeast Fishery Management Council (NEFMC) and the Mid-Atlantic Fishery Management Council (MAFMC) for the purpose of co-managing a fishery or for making determinations about eligibility for permits when state data are all or part of the basis for the permits. For purposes of data analysis. These Magnuson-Stevens Act (MSA) authorized fisheries management organizations have teams of analysts who use GARFO data to help drive fisheries management decision making.

The NEFMC and MAFMC and the North Atlantic Fisheries Organization for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures.

The Office of Law Enforcement for purposes of civil and criminal investigation and enforcement.

The Atlantic Coastal Cooperative Statistics Program (ACCSP). ACCSP is a critical data management partner to GARFO. Currently they are the data collection point for all federally permitted dealers, and the future vision is to make them the warehouse for all east coast federal fisheries data. Data exchanges between GARFO and ACCSP have been integral to fisheries management for many years.

State fishery managers of the Atlantic Coastal States of Maine, Massachusetts, and Rhode Island, because there is overlap between state management and some federal fish activity reporting requirements.

USCG Reciprocal information (data for issuing fishing permits and permit histories, catch data collected from fishing vessels, landings data collected from fish dealers, and effort or catch based allocation data). USCG access to GARFO Data requires NDA for each individual accessing the data. We do not access any confidential data from the USCG.

Army Corps of Engineers for support of environmental assessment.

The public: Vessel Owner Name, Name of Vessel and Permit Number are made publically available through our website. Notice of this is given on the permit application. We also allow other regions, centers and state organizations access to the publically available information directly from our database through a secure connection. This information is considered part of the public domain.

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

Information retrieval on NOAA4100 is done securely in a variety of ways. The majority of access is through the Greater Atlantic Region's website. The information that is shared and collaborated with other organizations is done securely through hardwired interconnections and through the NOAA4000 controlled non-permanent VPN.

i) How information is transmitted to and from the system

Information is transmitted to and from the system through secure encrypted channels

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	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): New Interconnection to NOAA0201 Web Operations Center					

_____ 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.

____ Yes. (*Check all that apply.*)

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

X 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
- X 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.

NMFS collects SSNs for employee onboarding and HR administration.

Provide the legal authority which permits the collection of SSNs, including truncated form.

Executive Orders: 9397 – Numbering System for Federal Accounts Relating to Individual Persons, as amended by 13478, 9830, and 12107; 10450 – Security Requirements for Government Employment; 12656 – Assignment of emergency preparedness responsibilities; 5 U.S.C. § 301 – 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?

☒ 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 SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

X The criteria implied by one or more of the questions above **apply** to the NOAA4100 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the NOAA4100 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>Information System Security Officer or System Owner</p> <p>Name: Peter Couture Office: NMFS GARFO TDMD Phone: 978-281-9115 Email: peter.couture@noaa.gov</p> <div style="text-align: right; margin-top: 20px;"> <small>Digitally signed by COUTURE.PETER.LAWRENCE. 1365711158 Date: 2023.05.01 15:33:09 -04'00'</small> </div> <p>Signature:  _____</p> <p>Date signed: <u>05/01/2023</u></p>	<p>Information Technology Security Officer</p> <p>Name: Catherine Amores Office: NMFS CIO Office Phone: 301-427-8871 Email: catherine.amores@noaa.gov</p> <div style="text-align: right; margin-top: 20px;"> <small>AMORES.CATHERINE.SOLEDA NE.SOLEDA.1541 D.1541314390 Date: 2023.05.04 17:23:11 -04'00'</small> </div> <p>Signature: <u>314390</u> _____</p> <p>Date signed: <u>05/04/2023</u></p>
<p>Privacy Act Officer</p> <p>Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov</p> <div style="text-align: right; margin-top: 20px;"> <small>BURRESS.ROBIN.SURRETT.1365847696 D.1365847696 Date: 2023.05.05 08:35:36 -04'00'</small> </div> <p>Signature: <u>696</u> _____</p> <p>Date signed: <u>05/05/2023</u></p>	<p>Authorizing Official</p> <p>Name: Sarah Bland Office: NMFS GARFO RO Phone: 978-281-9257 Email: Sarah.Bland@noaa.gov</p> <div style="text-align: right; margin-top: 20px;"> <small>BLAND.SARAH.ELIZABETH.1386899386 D.1386899386 Date: 2023.05.02 14:13:54 -04'00'</small> </div> <p>Signature: <u>86</u> _____</p> <p>Date signed: _____</p>
<p>Bureau Chief Privacy Officer</p> <p>Name: Robin Burress FOR Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov</p> <div style="text-align: right; margin-top: 20px;"> <small>BURRESS.ROBIN.SURRETT.1365847696 D.1365847696 Date: 2023.05.12 09:25:51 -04'00'</small> </div> <p>Signature: <u>ETT.1365847696</u> _____</p> <p>Date signed: _____</p>	Empty space for additional signature or date