

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



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

## U.S. Department of Commerce Privacy Threshold Analysis

### NMFS / NOAA4100 – Greater Atlantic Regional Office (GARFO) Network

**Unique Project Identifier: 006-03-02-00-01-0511-00**

**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 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).

*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, Cape May, NJ, East Hampton, NY, New Bedford, MA, Point Judith, RI, Narragansett, 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), the NMFS Northeast Fisheries Science Center (NOAA4200), and the Atlantic Coastal Cooperative Statistics Program (ACCSP).

*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, use, 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*

<p>Due to the varying sensitivity of NOAA4100’s data, the individuals that have access to our data range from the public to only those who have been authorized by the data owner. NOAA4100 data is shared with a variety of organizations. This includes other federal agencies, state and local agencies, fisheries management organizations, fish dealers, educational entities, vessel owners and the public.</p>
---

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

<p>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.</p>
--

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

<p>Information is transmitted to and from the system through secure encrypted channels</p>
--

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.

For employee onboarding and HR administration.  
SORN DEPT – 18 Employees Information not covered by Records of other Agencies;

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 PTA 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 NOAA4100 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 NOAA4100 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): Peter Couture

Signature of ISSO or SO:  Digitally signed by COUTURE.PETER.L.1365711158  
Date: 2020.07.16 06:50:35 -04'00' Date: 07/16/2020

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

Signature of ITSO: AMORES.CATHERINE.S  
OLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390  
Date: 2020.07.22 17:20:43 -04'00' Date: 07/22/2020

\_\_\_\_\_  
Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: THOMAS.ADRIENNE.M.13  
65859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600  
Date: 2020.07.23 10:14:08 -04'00' Date: 07/23/2020

\_\_\_\_\_  
Name of Authorizing Official (AO): Kim Damon-Randall

Signature of AO: DAMON  
RANDALL.KIMBERLY.B.1365821093 Digitally signed by DAMON  
RANDALL.KIMBERLY.B.1365821093  
Date: 2020.07.16 09:05:50 -04'00' Date: 07/16/2020

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

Signature of BCPO: GRAFF.MARK.HYRUM.1  
514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892  
Date: 2020.07.23 12:28:00 -04'00' Date: 07/23/2020