

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



**Privacy Threshold Analysis**  
**for the**  
**NOAA4400**

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

NOAA4400

**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:** *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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 Southeast Fisheries Science Center (SEFSC) is a general support system that conducts multi-disciplinary research programs to provide management information to support national and regional programs of NOAA's National Marine Fisheries Service (NMFS) and to respond to the needs of Regional Fishery Management Councils, Interstate and International Fishery Commission, Fishery Development Foundations, government agencies, and the general public.

The Science

In general, SEFSC develops the scientific information required for:

- Fishery resource and conservation
- Fishery development and utilization
- Habitat conservation
- Protection of marine mammals and endangered marine Species

Impact analyses and environmental assessments for management plans and international negotiations are also prepared, and research is pursued to address specific needs in:

- Population Dynamics
- Fishery Biology Fishery
- Economics
- Engineering and Gear Development Protected
- Species Biology

*b) System location*

The Southeast Fisheries Science Center (SEFSC) is headquartered in Miami, FL.

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

The Southeast Fisheries Science Center (SEFSC) is headquartered in Miami, FL. and interconnects with NOAA4000; NOAA4020; NOAA4200, and NOAA4300. These NMFS interconnections all connect via the NMFS WAN and are primarily used for database connections to provide data to NMFS science centers and regional offices.

The data being shared amongst these systems consists of aggregated fishery and marine life data and does not include PII or BII. Authorized personnel use this data for research purposes, and they access this data following access controls put in place by each system following the guidelines of the current NIST IT Security standard.

The SEFSC is responsible for scientific research on living marine resources that occupy marine and estuarine habits of the continental southeastern United States, as well as Puerto Rico and the U.S. Virgin Islands. The SEFSC is one of the six national marine fishery science centers' responsible for federal marine fishery research programs

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

The SEFSC is responsible for scientific research on living marine resources that occupy marine and estuarine habits of the continental southeastern United States, as well as Puerto Rico and the U.S. Virgin Islands. The SEFSC is one of the six national marine fishery science centers' responsible for federal marine fishery research programs.

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

PII/BII in the IT system is being collected, maintained, or disseminated for (a) administrative matters; (b) civil enforcement activities; and (c) criminal law enforcement activities if needed.

NOAA4400 does not collect SSNs or EINs; however, the organization gathers some minimum PII as, captain's names, addresses, and phone numbers, and this information is used for processes such as (d) compliance - ensuring logbooks are submitted as required; (e) mailing (logbooks, permits, etc.); (f) uses mailing address of record; (g) providing HMS regulations and species guides to Atlantic Tournaments; and (h) for online no-fish electronic reporting - account creation and mailing.

NOAA4400 has a Fisheries Logbook System (FLS) which collects vessel and captain's names, numbers of each species caught, the numbers of animals retained or discarded alive or discarded dead, the location of the set, the types and size of gear, the duration of the set, port of departure and return, unloading dealer and location, number of sets, number of crew, date of departure and landing, and an estimate of the fishing time. NOAA4400 collect the job title of individual completing the logbook, and their telephone numbers as well.

Information in the system is retrieved by the user after following multiple conditions that have been implemented, system wide, to restrict user from selecting incorrect options, including database field and values, and in addition, after the data is collected and validated, numerous QAQC reports are ran to confirm the data accuracy.

The specific ways in which a user can retrieve the information is through SQL, SAS, R, Oracle, and APEX queries. Access to the systems requires the specific permissions, and the data is encrypted at rest.

Access to the system is granted base on specific roles and very few users have the ability to access the whole system.

Logs for every single operation, (no exceptions), are generated, collected, and kept indefinitely, which allows the reconstruction and analysis of any event that might happen at a particular point.

Operation logs are generated with time and location.

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

NOAA4400 collect Vessel ID/Documentation # in order to trace information back to the required permit.

Please see section 2.1 on the PIA. Multiple conditions have been implemented, system wide, to restrict user from selecting incorrect options, including database field and values, and in addition, after the data is collected and validated, numerous QAQC reports are ran to confirm the data accuracy.

Access to the system is granted base on specific roles and very few users have the ability to access the whole system.

Logs for every single operation, (no exceptions), are generated, collected, and kept indefinitely, which allows the reconstruction and analysis of any event that might happen at a particular point. Operation logs are generated with time and location.

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

Access to the system is granted base on specific roles and very few users have the ability to access the whole system.

Logs for every single operation, (no exceptions), are generated, collected, and kept indefinitely, which allows the reconstruction and analysis of any event that might happen at a particular point.

Operation logs are generated with time and location.

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

NOAA4400 has a Fisheries Logbook System (FLS) which collects vessel and captain's names, numbers of each species caught, the numbers of animals retained or discarded alive or discarded dead, the location of the set, the types and size of gear, the duration of the set, port of departure and return, unloading dealer and location, number of sets, number of crew, date of departure and landing, and an estimate of the fishing time. NOAA4400 collect the job title of individual completing the logbook, and their telephone numbers as well.

Information in the system is retrieved by the user after following multiple conditions that have been implemented, system wide, to restrict user from selecting incorrect options, including database field and values, and in addition, after the data is collected and validated, numerous QAQC reports are ran to confirm the data accuracy.

The specific ways in which a user can retrieve the information is through SQL, SAS, R, Oracle, and APEX queries. Access to the systems requires the specific permissions, and the data is encrypted at rest.

Access to the system is granted base on specific roles and very few users have the ability to access the whole system.

Logs for every single operation, (no exceptions), are generated, collected, and kept indefinitely, which allows the reconstruction and analysis of any event that might happen at a particular point.

Operation logs are generated with time and location.

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

All data is encrypted at rest, and during transit and is handled by the Database Administrator in an Oracle System. The information is secured via both administrative and technological controls. BII is stored on shared drives that require CAC for access. The principle of least privilege and separation of duties is implemented by SEFSC to ensure that only personnel with the need to know have access to this information.

Logbook data, when entered, is stored on our Oracle Database server. This system uses the native database authentication for user access. The only way to read data on the Oracle Database is to have access by authenticating with a username and password.

Computerized database is password protected, and access is limited. Paper records are maintained in secured file cabinets in areas that are accessible only to authorized personnel of NOAA4400.

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). *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.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

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

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 NOAA4400 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 SEFSC 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): Luis O. Noguero

Signature of ISSO or SO: 9 NOGUEROL.LUIS.O.150558943 Digitally signed by NOGUEROL.LUIS.O.150558943 Date: 2020.08.26 09:14:53 -04'00' Date: \_\_\_\_\_

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

Signature of ITSO: AD.1541314390 AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2020.09.08 16:20:46 -04'00' Date: \_\_\_\_\_

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: 9600 THOMAS.ADRIENNE.M.136585 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.09.08 17:05:24 -04'00' Date: \_\_\_\_\_

Name of Authorizing Official (AO): Braydon Mikesell

Signature of AO: 13648 MIKESELL.BRAYDON.GLENN.12615 Digitally signed by MIKESELL.BRAYDON.GLENN.1261513648 Date: 2020.08.26 11:14:28 -04'00' Date: \_\_\_\_\_

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

Signature of BCPO: 14447892 GRAFF.MARK.HYRUM.15 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.09.10 14:24:51 -04'00' Date: \_\_\_\_\_