Version Number: 01-2021

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

Privacy Threshold Analysis for the
NOAA4400 (SEFSC)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NMFS/SEFC

Unique Project Identifier: NOAA4400

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 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 SEFSC provides the scientific advice and data needed to effectively manage the living marine resources of the Southeast region and Atlantic high seas. We work closely with NOAA Fisheries Southeast Regional Office to provide independent, objective science.

Our multidisciplinary research informs natural resource management. Fisheries management councils, fisheries commissions, and federal, state and local agencies depend on our science to make decisions that protect and conserve the region's living marine resources.

In general, SEFSC develops the scientific information required for:

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

The Research is based on the impact analyses and environmental assessments for management plans and international negotiations, and is pursued to address specific needs in the following fields:

Population dynamics
Fishery biology

Fishery economics
Engineering and gear development
Protected species biology

NOAA4400 has an interconnection with the Atlantic Coastal Cooperative Statistics Program(ACCSP). Through its interconnection with ACCSP, individual fishermen trip data, dealer report data, and permit data are shared between SEFSC and ACCSP. The permit data does not include Personal Identifiable Information (PII).

Also, NOAA4400 still collecting fisherman trip and landing statistics to meet a federal mandate under the Magnuson-Stevens Act to collect and report recreational and commercial fisheries data. There are no other ways to operate without this collection. The collected data is accessed by ACCSP Staff, SEFSC Staff,and ACCSP partners with individual user confidential access approved by SEFSC staff. Confidential named user access is for a set period and is automatically revoked at the expiration date.

Address the following elements:

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

The Southeast Fisheries Science Center (SEFSC – FISMA NOAA4400) is a general support system

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 ACCSP; NOAA0550; NOAA4000; NOAA4020; NOAA4200, and NOAA4300. The 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; and as per the connection with ACCSP, all data is encrypted usingthe oracle native encryption (sqlnet.ora), and TLS. If the VPN works, we have an encrypted connection plus a VPN, and in case the VPN does not work, we are still protected byusing our existing encrypted connection.

The data being shared amongst these systems consists of aggregated fishery and marine life data; and minimum PII and BII needed to maintain the system operation. 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 fisheries 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, 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

Personal Identifiable Information (PII) and Business Identifiable Information (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.

The integration of drones (UAS) into SEFSC Protected Resources and Biodiversity Division operations allow for additional information to be gathered during operations, including aerial photo-identification and dorsal photography that allow for assessments of individual organism growth, health, body condition, and reproductive status and provide more accurate estimates of group sizes and group membership.

NOAA4400 could also utilize UAS to locate and assess stranded animals in areas difficult to access. Outside of the protected resources applications, regular or opportunistic UAS deployments could also be used to identify and, if coupled with acoustic data, determine the three-dimensional extent and density of schooling pelagic fishes (e.g., menhadens, tunas), which could ultimately be utilized to estimate the biomass. UAS could also be utilized to support additional projects yielding data on the marine environment, including on critical habitats and seawater chemistry, to name a few.

UAS: As outlined in DEPT-29, the use of UAS has the potential for inadvertent collection of PII, such as images of individuals along the coastlines that are within the area of study by the UAS vehicle. However, no information retrieval using any unique identifier within Survey datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. NOAA4400 does not use any application capable of facial recognition within any captured images. It is anticipated that the UAS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to identify any individuals uniquely.

If the drone goes down during flight, the retrieval of the unit would be at the operator's discretion based on safety and technical factors. Inadvertently obtained PII captured during the flight could be retrieved by others if technically possible from the damaged drone. NOAA4400 closely collaborate with OCS, and OCS is compliant with all policies and procedures posted on the UAS.noaa.gov site along with the NOAA Unmanned Aircraft System Privacy Policy.

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

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.

The integration of drones (UAS) into SEFSC Protected Resources and Biodiversity Division operations allow for additional information to be gathered during operations, including aerial photo-identification and dorsal photography that allow for assessments of individual organism growth, health, body condition, and reproductive status and provide more accurate estimates of group sizes and group membership.

NOAA4400 could also utilize UAS to locate and assess stranded animals in areas difficult to access. Outside of the protected resources applications, regular or opportunistic UAS deployments could also be used to identify and, if coupled with acoustic data, determine the three-dimensional extent and density of schooling pelagic fishes (e.g., menhadens, tunas), which could ultimately be utilized to estimate the biomass. UAS could also be utilized to support additional projects yielding data on the marine environment, including on critical habitats and seawater chemistry, to name a few.

UAS: As outlined in DEPT-29, the use of UAS has the potential for inadvertent collection of PII, such as images of individuals along the coastlines that are within the area of study by the UAS vehicle. However, no information retrieval using any unique identifier within Survey datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. NOAA4400 does not use any application capable of facial recognition within any captured images. It is anticipated that the UAS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to identify any individuals uniquely.

If the drone goes down during flight, the retrieval of the unit would be at the operator's discretion based on safety and technical factors. Inadvertently obtained PII captured during the flight could be retrieved by others if technically possible from the damaged drone. NOAA4400 closely collaborate with OCS, and OCS is compliant with all policies and procedures posted on the UAS.noaa.gov site along with the NOAA Unmanned Aircraft System Privacy Policy.

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

Access to the system is granted based on specific roles and very few users can access the whole system.

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

Operation logs are generated with time and location.

NOAA4400 has a relatively new interconnection with the Atlantic Coastal Cooperative Statistics Program (ACCSP). Through this association, commercial dealer, as well as permit-based commercial and for-hire fishermen, data is collected by ACCSP and exchanged with NOAA4400. Individual fishermen trip data, dealer report data, and permit data are shared between SEFSC and ACCSP. The permit data does not include PII.

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.

The user retrieves information in the system after following multiple conditions that have been implemented, system-wide, to restrict the user from selecting incorrect options, including database fields and values. In addition, after the data is collected and validated, numerous QAQC reports are run to confirm the data's accuracy.

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

Access to the system is granted based on specific roles and very few users can access the whole system.

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

Operation logs are generated with time and location. ACCSP pulls data using an encrypted sqlnet connection over a dynamic VPN to NOAA HQ (4000). Data are retrieved by the authenticated end-users and state fisheries administrators through the ACCSP Warehouse. Federal agencies who have an Interconnect Security Agreement may retrieve the data from the ACCSP Warehouse or SAFIS databases, follow agreed-upon secure data transfer protocols, and provide access to their users through their localdata delivery processes

appropriate.

All internal data and resources are retrieved using Government Furnished Equipment (GFE) through approved applications to open, review, verify, and securely delete information. Internal resources are secured through defense-in-depth with layered security such as physical access, firewalls, active directory, access controls, permission, etc.

Internal CAC authenticated users can utilize (based on permissions) data stored in PDF, Files, and databases through networked client's devices and NOAA VPN service for remote access. NOAA4400 uses Google services for email and collaboration services.

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. SEFSC implements the principle of least privilege and separation of duties to ensure that only personnel with the need to know to have access to this information.

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

A 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.

ACCSP pulls data using an encrypted sqlnet connection over a dynamic VPN to NOAA HQ (4000). Data is passed through FIPS 140-2 approved encryption mechanisms (SQLNET AES256 encrypted sessions) if networks are interconnected. When the information is transmitted to and from the ACCSP, ACCSP pulls data using an encrypted sqlnet connection over a dynamic VPN to NOAA HQ (4000). The connections at each end must be located within controlled access facilities and protected 24 hours a day. Individual users will not have access to the data except through their system's security software inherent to the operating system.

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.*

_____ 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.*

__X__ 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		Building entry readers	
Video surveillance	X	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.)."

__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.)*

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

_X_ 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 Package9)

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to the NOAA4400 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 [IT SYSTEM NAME] 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: Luis O. Noguerol Office: SEFSC Phone: 305-361-4464 Email: luis.noguerol@noaa.gov Signature: NOGUEROL.LUIS.O.(IO).1505589439 Digitally signed by NOGUEROL.LUIS.O.(IO).1505589439 Date: 2022.10.26 16:32:39 -04'00' Date signed:	**Information Technology Security Officer** Name: Catherine Amores Office: NOAA Fisheries HQ Phone: 301-427-8871 Email: Catherine.amores@noaa.gov Signature: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2022.11.15 13:30:21 -05'00' Date signed:
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: robin.burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2022.11.21 11:18:08 -05'00' Date signed:	**Authorizing Official** Name: Braydon Mikesell Office: SEFSC Phone: 305-361-4260 Email: braydon.mikesell@noaa.gov Signature: MIKESELL.BRAYDON.GLENN.1261513648 Digitally signed by MIKESELL.BRAYDON.GLENN.1261513648 Date: 2022.10.31 14:24:58 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.12.08 09:15:28 -05'00' Date signed:	

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.