

**U.S. Department of Commerce  
National Oceanic and  
Atmospheric  
Administration**



**Privacy Threshold Analysis for  
the  
NMFS Southeast Region Office Local Network  
NOAA4300**

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

### NOAA/NOAA4300

**Unique Project Identifier:** 006-48-01-14-02-3305-00

**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*

NOAA4300 is a general Support System. It supports all offices within the Southeast Region (SER) which include the Regional Administrator's Office; Operations, Management & Information Services Office; State/Federal Liaison Office; Sustainable Fisheries Division; Protected Resources Division; and, Habitat Conservation Division.

The system also supports non-SERO offices located in St. Petersburg including NOAA SE Office of General Counsel (GCSE), Damage Assessment Center (DAC), and NMFS SE Financial Services. The information for these Non-SERO offices is covered by the NOAA4020 Privacy Impact Assessment.

*b) System location*

NOAA4300 is physically housed in a leased portion of a three story building located within the city limits of Saint Petersburg, Florida. The building is 85% occupied by NOAA and NMFS offices. The network servers, web servers, and network management workstations are located in a secure room on the second floor.

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

NOAA4300 has an interconnection with NOAA4000 (NMFS WAN) for the following purposes:

- NMFS to NMFS network access
- Core backbone network services with Internet connectivity (TICAP)
- Enterprise Active Directory
- Tier 1,2, and 3 technical support
- Coordination of IP address (DNS)
- Real-time network monitoring
- VMS Data for purposes of Catch Shares (IFQ) program and Permits Management System (PIMS)

Upon verification of FIPS199 Moderate system compliance (or SP-171 equivalent), and the sharing of sensitive data has been authorized, a direct connection to ACCSP will be created, with a new Interconnection Agreement between NOAA4300 and ACCSP being created and signed. Starting September 1, 2020, in order to comply with modifications to both the Gulf of Mexico Charter Vessel and Headboat Reporting Requirement Rule (<https://www.fisheries.noaa.gov/action/gulf-mexico-modifications-charter-vessel-and-headboat-reporting-requirements>) and the South Atlantic Charter Vessel and Headboat Reporting Requirement Rule (<https://www.fisheries.noaa.gov/action/south-atlantic-modifications-charter-vessel-and-headboat-reporting-requirements>), NOAA4300 will be required to share permit holders' date of birth (DOB) and email addresses with ACCSP, **once ACCSP can provide documentation verifying a successful Assessment and Independent Validation and Verification of compliance with all applicable security policies, controls, and requirements of a FIPS199 Moderate (or equivalent) system.** The following timelines are based upon ACCSP's providing proof of compliance (third-party audit/SAR, control queries and artifacts, SSP, etc.) to NOAA4300, and are currently tentative at best. Once compliance is achieved, ACCSP will be required to provide annual verification of Continuous Monitoring methodology practices and current FIPS199 compliance through third party audit results prior to the renewal of any system interconnect or data sharing agreements.

- By June 1<sup>st</sup>, 2020, NOAA4300 plans to begin sharing permit holders' Date of Birth (DOB) with ACCSP.
- By June 30<sup>th</sup>, 2020, NOAA4300 plans to begin sharing electronic logbook and landing data with ACCSP.
- By September 30<sup>th</sup>, 2020, NOAA4300 plans to begin sharing Vessel Monitoring System (VMS) positional data with ACCSP in order to comply with pending regulations.
- By December 30<sup>th</sup>, 2020, in order to comply with pending regulations, NOAA4300 plans to share all for hire permit holder data with ACCSP.

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

As a General Support System, NOAA4300 functions as the overall office automation support system for the NOAA/NMFS offices in St. Petersburg, Florida. It provides access to automated systems typically found in administrative offices within the federal government. It supports all offices within the SER which include the Regional Administrator's Office; Operations, Management & Information Services Office; Economics Office; State/Federal Liaison Office; Sustainable Fisheries Division; Protected Resources Division; and, Habitat Conservation Division. The system also supports non-SERO offices located in St. Petersburg including NOAA SE Office of General Counsel (GCSE) and NMFS SE Financial Services.

NOAA4300 is also designed to serve the following purposes in terms of collecting, storing, processing and disseminating PII/BII:

- For administrative matters
- For litigation
- For civil enforcement activities
- For administering human resources programs
- To promote information sharing initiatives
- For criminal law enforcement activities

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

NOAA4300 collects and stores information that consists of basic identifying information about employees, contractors, volunteers, and partner agency staff who are facility occupants or system users. The information is maintained as a supplement to other records for purposes of human resource activities (including managing security clearances), Continuity of Operations (COOP) execution, and performing other related administrative tasks, e.g., travel, awards, facility management, and staff training requirements in support of individual job duties and requirements.

NOAA4300 also collects and stores permit-related data. In order to manage U.S. fisheries, the NMFS requires the use of permits or registrations by participants in the United States. The information collected by NMFS SERO includes the contents of permit applications and supporting artifacts. Typical transactions include initial or renewal permit applications. The permit holder or applicant completes a blank application downloaded from the applicable NMFS Web site, received in the mail, or obtained through visiting the Permits office, and submits it to the applicable office via online, or in person, including any required supporting documentation and proof of payment through pay.gov. Approved permits are mailed to applicants. For permit transfers within a family, marriage certificates, divorce decrees, and/or death certificates may be required. Tax Identification Numbers (TINs) allow positive identification and cost recovery billing of Individual Fishing Quota (IFQ) holders.

NOAA4300 employs contractors in a variety of roles in order to support its mission, primarily in the

Habitat/Sustainable Fisheries/Protected Resources branches. All contractors undergo the same security clearance process as Federal Government employees. Access to information collected and maintained within the system boundary of NOAA4300 is determined by the individual's job duties and role within the organization. Any request involving the sharing of sensitive data, whether internal or external, must be documented in a Memorandum of Understanding (MoU) or Interconnection Security Agreement (ISA), and approved by each system's Authorizing Official. Information is shared within the Southeast Region 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 (Such as the Office of General Counsel and the Southeast Division of the NMFS Office of Law Enforcement), the U.S. Coast Guard and the Department of Justice. Information will also be shared at the state or interstate level for the purpose of determining an applicant's eligibility when data collected by the state affects permit eligibility.

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

Information collected to manage security clearances may include: full name, home address, home phone number, e-mail address, educational background, Social Security Number (SSN), and employment history. Information maintained for COOP and other administrative processes includes: full name, grade level and/or position within the organization, role/responsibility, home address, home phone number, and mobile phone number.

In order to manage U.S. fisheries, the NMFS requires the use of permits or registrations by participants in the United States. The information collected by NMFS SERO includes the contents of permit applications and supporting artifacts. Typical transactions include initial or renewal permit applications. The permit holder or applicant completes a blank application downloaded from the applicable NMFS Web site, received in the mail, or obtained through visiting the Permits office, and submits it to the applicable office via online, or in person, including any required supporting documentation and proof of payment through pay.gov. Approved permits are mailed to applicants. For permit transfers within a family, marriage certificates, divorce decrees, and/or death certificates may be required. Tax Identification Numbers (TINs) allow positive identification and cost recovery billing of Individual Fishing Quota (IFQ) holders.

In addition, information is collected to facilitate public education, outreach, or collaboration with partners on research/conservation projects. For these activities, the name, address, e-mail address, telephone number, and other non-sensitive organizational information may be temporarily stored. These individuals, businesses or organizations may be workshop participants, business contacts, members of mailing lists, etc. In all cases the information is voluntarily submitted.

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

There is no public access to NOAA4300. Users are only allowed access to information that is required for them to fulfill their job duties. All portable computers are encrypted with McAfee Disk Encryption.

Access to PII is controlled through access control policies and access enforcement mechanisms. Separation of duties is strictly enforced for duties involving access to PII.

Least privilege is enforced for all NOAA4300 users, enforcing the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Access to information system media containing PII, including digital media, is restricted to authorized personnel. Users are uniquely identified and authenticated through either 2 factor authentication or USGCB compliant passwords before accessing PII.

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

Employees can contact the HR representative for NOAA4300 and review their information, or a personal contact information form can be completed and given to HR, who will then update the information accordingly.

Permits: Information may be reviewed/updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time.

Partners for public outreach and education may update their information at any time by contacting the appropriate staff member assigned as their coordinator.

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

Information is manually collected through mail, over the telephone, in person, email, fax, and online.

Information is currently transmitted to and from the system through a network connection internal to the NMFS WAN employing Virtual Private Network encryption (TCP/IP using TLS) to secure the data.

Once ACCSP has achieved FIPS199 (or equivalent) compliance, and direct data sharing has been approved and established, data will be sent via encrypted connection to ACCSP (using AES-256 Encryption over a dedicated connection). Once transferred, authorized SER staff can access the data through the SAFIS web interface, which uses HTTPS to secure the connection.

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): Pending connection/data sharing with ACCSP (upon 3rd party verification and validation of ACCSP obtaining FIPS199 moderate compliance). Video camera system at all facility entrance and exit points, and in parking lot for safety and security purposes.					

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	X
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.).”

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.

Tax Identification Numbers/Social Security Numbers are collected to allow positive identification for cost recovery billing of Individual Fishing Quota holders.

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.

FOIA-related authorities: 5 U.S.C. 552 and 552a, 15 CFR Part 4.

Permit and registration data are collected from individuals under the authority of the Magnuson- Stevens Fishery Conservation and Management Act, the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Atlantic Coastal Fisheries Cooperative Management Act, the Atlantic Tunas Convention Authorization Act, the Northern Pacific Halibut Act, international fisheries regulations regarding U.S. Vessels Fishing in Colombian Treaty Waters, the Marine Mammal Protection Act, the Endangered Species Act and the Fur Seal Act. The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.

From: COMMERCE/DEPT-13: Executive Orders 10450, 11478, 12065, [5 U.S.C. 301](#) and 7531-332; [15 U.S.C. 1501](#) *et seq.*; [28 U.S.C. 533-535](#); [44 U.S.C. 3101](#); Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.

From: COMMERCE/DEPT-14: 5 U.S.C. 301; 44 U.S.C. 31101; 42 U.S.C. 3211; 31 U.S.C. 240; 28 U.S.C. 533-535 and 1346(b); 15 U.S.C. 277 and 278e(b); E.O. 10450; E.O. 11478, as amended and all other authorities of the Department.

From: COMMERCE/DEPT-18: 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

From: COMMERCE/DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

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 NOAA4300, 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 NOAA4300, 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):

Eric Barton – ISSO, NOAA4300

Signature of ISSO or SO: 5837321 BARTON.ERIC.H.136 Digitally signed by BARTON.ERIC.H.1365837321 Date: 2020.08.26 08:17:35 -04'00' Date: \_\_\_\_\_

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

Signature of ITSO: OLEDAD.1541314390 AMORES.CATHERINE.S Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2020.08.31 08:23:33 -04'00' Date: \_\_\_\_\_

Name of Authorizing Official (AO):

Dr. Roy Crabtree – Regional Administrator, NMFS Southeast Region

Signature of AO: 365849559 CRABTREE.ROY.E.DR.1 Digitally signed by CRABTREE.ROY.E.DR.1365849559 Date: 2020.08.27 09:52:58 -04'00' Date: 8/27/2020

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: 5859600 THOMAS.ADRIENNE.M.136 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.09.01 09:39:32 -04'00' Date: 8/31/20

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

Signature of BCPO: 4447892 GRAFF.MARK.HYRUM.151 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2020.09.01 10:03:01 -04'00' Date: 9/1/20