

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



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

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NMFS/Southeast Regional Office

Unique Project Identifier: NOAA4300

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).

NOAA4300 supports all offices within the Southeast Region (SER), which includes 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.

Address the following elements:

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

NOAA4300 is a General Support System.

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.

While there are field offices for NOAA4300 located in Charleston, SC, Beaufort, SC, Galveston, TX,

Baton Rouge, LA, Miami, FL, and Fernandina Beach, FL, these users and endpoints are located outside the system boundary of NOAA4300 and connect to the system using VPN. These offices are either hosted within other system boundaries, or on an independent ISP and completely remote.

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
- Coordination of IP address (DNS)
- Real-time network monitoring
- VMS and Permits Data for purposes of Catch Shares (IFQ) program and Permits Management System (PIMS)*

*Data exchange over the existing interconnection due to the PIMS application being migrated to the cloud instance hosted by NOAA4000. PIMS data is now exchanged over the existing secure interconnection shared with NOAA4000. Even though it's hosted by NOAA4000, the application is considered to be within NOAA4300's system boundary due to the supposed architecture of the instance.

NOAA4300 uses the interconnection with NOAA4000 to share permit related data with NOAA4400 (SEFSC) in Miami.

NOAA4300 has an interconnection with NOAA4011 for purposes of fishery management in conjunction with NFPLRS, and the hosting of the Catch Shares Online System.

NOAA4300 is currently preparing to migrate the Catch Shares Online System from NOAA4011 to a cloud instance hosted by the NOAA WOC as part of the Amazon Government Web Services Cloud (a FedRAMP certified cloud vendor). The instance containing the migrated Catch Shares Online System is managed by NOAA4300, and the instance and application will fall within the NOAA4300 System Boundary. The contractor currently managing the application (Tesa) within NOAA4011 will be performing the migration to the new instance, and ensuring all functionality and data remain intact.

The function of the application and data it contains will be unchanged. There is no change to the type of data stored or processed by NOAA4300.

Upon completion of the migration to the new instance, both NOAA4011 and NOAA4300 staff will verify functionality and data integrity/minimization prior to the migrated application going into production.

NOAA4300 has been provided the estimated completion dates for the following critical

milestones from Tesa for the CSOS migration:

- Application migration – August 4th, 2023
- Functionality and data reviews - August 15th, 2023
- Production cutover – August 25th, 2023

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 is required to share permit holders' date of birth (DOB) and email addresses with ACCSP.

This interconnection agreement with ACCSP was established in November, 2020, and will continue to be renewed annually, contingent upon ACCSP providing documentation to NMFS OCIO (NOAA4000) 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 on an annual basis. In 2021, a centralized Interconnection Agreement with ACCSP was created by NOAA4000 in order to prevent duplication of effort in terms of system interconnection agreements between ACCSP and multiple regional offices. NOAA4000 is responsible for ensuring ACCSP remains certified as a FIPS 199 Moderate (equivalent) system and that it complies with all applicable security policies, rules, and requirements. Regional offices send in their updates annually or as needed so that the central document is kept up to date.

In order to maintain this system interconnection, ACCSP will be required to provide annual verification of Continuous Monitoring methodology practices and current FIPS199/NIST SP800-171 compliance through third party audit results prior to the renewal of any system interconnect or data sharing agreements. NMFS OCIO will also be required to provide annual documentation indicating their approval of ACCSP's Authority to Connect to NMFS systems.

A replacement for the NOAA4300 Permits Information Management System (PIMS) went into production in September 2021. This upgrade is a complete rewrite of the old application, whose programming code had reached End of Life. The upgraded version of PIMS is now hosted in an AWS instance held under contract with NOAA4000, where NOAA4300 occupies an instance within that environment for the PIMS application. The application is hosted by Appian, a FEDRAMP approved vendor, and managed by Nuvitek. Connectivity to NOAA4300 is secured through VPN. The Appian instance hosting PIMS is within the NOAA4300 system boundary.

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. 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.

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.

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.

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, used, 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.

Data is sent to ACCSP via encrypted connection (using AES-256 Encryption). Once transferred, authorized SER staff can access the data through the SAFIS web interface, which uses HTTPS to secure the connection.

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.

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 | X |
| Video surveillance | X | Electronic purchase transactions | |
| Other (specify): The facility housing NOAA4300 maintains a video surveillance and access control system, which is used only for the purposes outlined in DEPT-13 Routine Uses (security-related and law enforcement records access requirements). | | | |

____ 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
- X 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?

 X 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. SSNs are also collected from federal employees and contractors for security clearance purposes.

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.

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.

Executive Orders:

10450 – Security Requirements for Government Employment

12656 – Assignment of emergency preparedness responsibilities

15 U.S.C. 277 Secretary of Commerce Regulations

28 U.S.C. 534-535 FBI / Acquisition, preservation, and exchange of identification records and information; Investigation of crimes involving government officers and employees, limitations

31 U.S.C. 240 Endorsement and Payment of Checks Drawn on the U.S. Treasury

44 U.S.C. 3101 Records management by agency heads; general duties

42 U.S.C. 3211 Powers of Secretary.

 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 NOAA4300 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 NOAA4300 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 Name: Eric Barton Office: NMFS Southeast Regional Office Phone: 727-551-5746 Email: Eric.Barton@noaa.gov</p> <p style="text-align: right;">BARTON.ERIC.HILL. <small>Digitally signed by BARTON.ERIC.HILL.1365837321 Date: 2023.07.27 13:16:26 -04'00'</small></p> <p>Signature: <u>1365837321</u></p> <p>Date signed: <u>7/27/2023</u></p> | <p>Information Technology Security Officer Name: Catherine Amores Office: NMFS OCIO Phone: 301-427-8871 Email: Catherine.Amores@noaa.gov</p> <p style="text-align: right;">AMORES.CATHERINE. <small>Digitally signed by AMORES.CATHERINE.SOLEIDAD.1541314390 Date: 2023.08.02 12:13:11 -04'00'</small></p> <p>Signature: <u>SOLEIDAD.1541314390</u></p> <p>Date signed: <u>8/2/2023</u></p> |
| <p>Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov</p> <p style="text-align: right;">BURRESS.ROBIN.SU <small>Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.08.07 07:20:52 -04'00'</small></p> <p>Signature: <u>RRETT.1365847696</u></p> <p>Date signed: <u>08/07/2023</u></p> | <p>Authorizing Official Name: Andrew Strelcheck Office: NMFS Southeast Regional Office Phone: 727-551-5702 Email: Andy.Strelcheck@noaa.gov</p> <p style="text-align: right;">STRELCHECK.ANDRE <small>Digitally signed by STRELCHECK.ANDREW.JAMES.1365863152 Date: 2023.07.27 09:29:40 -04'00'</small></p> <p>Signature: <u>W.JAMES.1365863152</u></p> <p>Date signed: <u>7/27/2023</u></p> |
| <p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov</p> <p style="text-align: right;">GRAFF.MARK.HYRU <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.08.08 05:50:18 -06'00'</small></p> <p>Signature: <u>M.1514447892</u></p> <p>Date signed: <u>8.8.23</u></p> | |