

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



**Privacy Threshold Analysis
for the
NOAA4960 – NMFS PIFSC LAN**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA – NMFS PIFSC LAN

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

Introduction: The Pacific Islands Fishery Science Center (PIFSC) Local Area Network (LAN) functions as the overall general support system (GSS) for the NOAA Fishery PIFSC offices and servers located in Honolulu, Hawaii. A GSS is an interconnected information resource under the same direct management control that shares common functionality.

The PIFSC servers and workstations are designed and configured to satisfy the complex scientific and general data process computer needs of fishery, ecologic, stock assessment, oceanographic and protected resources data as well as administrative data that contains no PII or BII used for the Federal budget, Federal property, procurement (pre-decisional documents), safety information only (accident records are not in the system), training (records of classes and who attended).

Information collected from federal employees includes names, phone numbers, addresses, to support contact rosters, access to facilities, stored official documents such as travel documents, performance plans, etc., by the employees' supervisors and the pay pool manager, and collection by IT staff and system logs as part of day-to-day operation and maintenance such as usernames, addresses, system and network activity logging, etc.

Forms for federal employees containing sensitive PII including social security numbers, date of birth, and financial information are scanned, transmitted and stored in a secure file share in the information system. A hard copy of employee onboarding forms is maintained in a secure file cabinet.

Volunteers do not have access to PII/BII on the information system.

Supervisors collect PII from visitors and foreign nationals for permission to access federal facilities via fax or email. Visitors submit a SECNAV 5512 form via fax, phone or hard copy in person. Visitors are instructed not to send the SECNAV form via e-mail. Information on the form includes name, address, telephone number, social security number, state ID/driver's license, passport number, date of birth, alien registration number, weight/height, hair color, eye color. The form is hand carried to NOAA Inouye Regional Center staff to coordinate access with Joint Base Pearl Harbor-Hickam base staff. A digital copy is stored in a secure file share and a hard copy is maintained in a secure file cabinet.

Government Passports are required for federal employee international travelers. Passport data is stored in file shares and encrypted at rest.

Information collected for general account access for federal employees, contractors and

volunteers is required to be included in notification and escalation call lists and is stored within a Contingency Plan (CP) and/or Incident Response Plan (IRP). These documents are maintained on a shared drive within the system boundary. Only system administrators with approved privileges have access to this information. The following information is collected and maintained on PIFSC designated federal and contractor employees:

1. Employee/Contractor Name
2. Business Email
3. Business Address
4. Business Phone Number
5. Alternate phone number (i.e., Cell phone)
6. Home Address
7. Home Phone Number
8. Name of Manager/Supervisor

System administration/audit data, including user ID and date/time of access, is collected when authorized users access the system.

PIFSC collects Business Identifiable Information (BII) as part of its process for collection of economic data related to US fisheries. This information is used for research and regulatory purposes.

The following information is collected from Pacific Islands Regions fisheries:

- Vessel Name
- Fishing location
- Fishing gear
- Catch information to include count and species
- Sales costs

For economic and regulatory information concerning US fisheries, this information collected is considered proprietary. This information is maintained locally with PIFSC systems and is used only for research and regulatory purposes. Regulatory purposes include enforcement of regulations. Civil or criminal law enforcement may result from information collected, leading to possible litigation.

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 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. *Please describe the activities which may raise privacy concerns.*
- 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 about: (*Check all that apply.*)

- Companies
- Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

Yes, the IT system collects, maintains, or disseminates PII about: (*Check all that apply.*)

- DOC employees
- Contractors working on behalf of DOC
- 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 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.

4c. 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, and/or 4c 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 NOAA4960 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 [IT SYSTEM NAME] 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): Nick Tenney

Signature of ISSO or SO: TENNEY.NICHOLAS.JAMES.1407926966 Digitally signed by TENNEY.NICHOLAS.JAMES.1407926966 Date: 2019.10.23 07:53:33 -10'00' Date: _____

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

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2019.11.08 10:01:24 -05'00' Date: _____

Name of Authorizing Official (AO): Evan Howell

Signature of AO: 52 HOWELL.EVAN.A.1365831552 Digitally signed by HOWELL.EVAN.A.1365831552 Date: 2019.10.31 08:18:37 -10'00' Date: _____

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

Signature of BCPO: UM.1514447892 GRAFF.MARK.HYR Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2019.11.21 15:19:44 -05'00' Date: _____