

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



**Privacy Threshold Analysis  
for the  
NOAA4960  
Pacific Islands Fisheries Science Center (PIFSC)**

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

### NOAA/NMFS/ Pacific Islands Fisheries Science Center (PIFSC)

**Unique Project Identifier: NOAA4960**

**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 NOAA Fisheries Pacific Islands Fisheries Science Center (PIFSC) Local Area Network (LAN) functions as an overall General Support System (GSS).

b) *System location*

PIFSC is located in Honolulu, Hawaii.

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

NOAA4960 interconnects for network transit purposes with NOAA1200, NOAA Corporate Services Local Area Network.  
NOAA4960 interconnects with NOAA4920 to facilitate exchange of fisheries observer and logbook data.

PIFSC has a dedicated WAN link to NOAA4000 to facilitate data interconnection between other systems within the bureau and access to various corporate services. NOAA4960 interconnects with NOAA4020 to facilitate transmission of fishing electronic logbooks.

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

The PIFSC LAN exists to support the primary mission which is to protect and preserve the nation's living marine resources through scientific research, fisheries management, enforcement and habitat conservation. PIFSC maintains commercial and recreational fisheries and continues to focus its efforts on sustaining marine resources. The LAN provides access to automated systems typically found in fishery science centers and administrative offices within the federal government. The LAN supports all the following units: The Director's Office; Operations, Management, and Information Services; The Ecosystem Sciences Division; The Fisheries Research and Monitoring Division; The Protected Resources Division; and The Science Operations Division. The categories of data utilized include administrative, oceanographic, fishery, graphical, statistical, economic, and technical.

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

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 used for human resources, Federal budget, Federal property, procurement (pre-decisional documents), and safety information.

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

PII is collected for both contractor and federal employee personnel designated to work with PIFSC. A digital and hard copy of each federal employee's hiring package submitted to PIFSC is collected and physically or electronically submitted to their respective agency for processing. Employee contact information is maintained for emergency call tree in the event of a disaster. Supervisors collect and maintain information from federal employees requiring federal passports. The passport data is shared within NOAA to facilitated processing of the passport. PII is shared with the Department of Commerce Western Region Security Office to process security clearances.

Procurement and contract information are stored on the LAN and share with external parties

associated with the procurement/contract, if applicable.

PII is collected from visitors, volunteers and foreign nationals to facilitate access to federal facilities. The information is shared with NOAA to grant access to the NOAA Inouye Regional Center located on Ford Island, Hawaii.

PII and BII are collected from the NOAA Fisheries National Permit System.

PII and proprietary BII are collected from fishermen's logbooks. The information is shared within NOAA Fisheries to allow fisherman access to their own data.

Observer BII data collected at sea is collected from the NOAA Fisheries Pacific Islands Region Office.

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

Users who will have access to the IT system include Government Employees and Contractors. Users are required to have an account to access and retrieve information.

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

Information in the system is retrieved by users operating government furnished equipment such as desktops or laptops connected to the LAN or VPN. Users are required to have an account to access and retrieve information.

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

Information is transmitted to and from the system by:

- Direct data entry
- Electronically transmitted by vessels at sea
- Data exchange via interconnected services to facilitate sharing of vessel logbook data
- Use of Google G.Suite (E-mail, Google Docs)
- Use of DOC Kiteworks to transmit sensitive PII
- Download of publicly available research data from various internet sources

--

**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):					
Vessel electronic logbook data is being shared with NOAA Fisheries Office of Science and Technology.					

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 01-2017). *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 01-2019 or later). *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	<u>X</u>	Building entry readers	
Video surveillance	<u>X</u>	Electronic purchase transactions	
Other (specify): Transmission of fishing vessel logbook data to the NOAA Fisheries Office of Science and Technology containing PII/BII from members of the public. Voice/audio recording and video recording onboard fishing vessels.			

       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

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.

<p>Provide an explanation for the business need requiring the collection of SSNs, including truncated form.          PII (SSN, Driver’s License, Passport #) are required for new federal hires, various forms pertaining to onboarding are scanned at a multifunction device, stored on administrative personnel folders, and transmitted securely via Kiteworks.</p>
<p>Provide the legal authority which permits the collection of SSNs, including truncated form.           DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies, 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.</p>

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 SAOP 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 system 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.

<p><b>Information System Security Officer or System Owner</b>  Name: Nick Tenney  Office:  Phone:  Email:</p> <p>Signature: <u>TENNEY.NICHOLAS.JAMES.1407926966</u> Digitally signed by TENNEY.NICHOLAS.JAMES.1407926966 Date: 2020.12.08 10:08:58 -10'00'</p> <p>Date signed: _____</p>	<p><b>Information Technology Security Officer</b>  Name: Catherine Amores  Office:  Phone:  Email:</p> <p>Signature: <u>AMORES.CATHERINE.SOLEDA.D.1541314390</u> Digitally signed by AMORES.CATHERINE.SOLEDA.D.1541314390 Date: 2020.12.10 16:06:13 -05'00'</p> <p>Date signed: _____</p>
<p><b>Privacy Act Officer</b>  Name: Adrienne Thomas  Office: NOAA OCIO  Phone: 828-257-3148  Email: Adrienne.Thomas@noaa.gov</p> <p>Signature: <u>THOMAS.ADRIENNE.M.1365859600</u> Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2020.12.14 14:09:08 -05'00'</p> <p>Date signed: _____</p>	<p><b>Authorizing Official</b>  Name: Michael Seki  Office:  Phone:  Email:</p> <p>Signature: <u>SEKI.MICHAEL.PAUL.YUKIO.1365894473</u> Digitally signed by SEKI.MICHAEL.PAUL.YUKIO.1365894473 Date: 2020.12.08 10:41:32 -10'00'</p> <p>Date signed: _____</p>
<p><b>Bureau Chief Privacy Officer</b>  Name: Mark Graff  Office: NOAA OCIO  Phone: 301-628-5658  Email: Mark.Graff@noaa.gov</p> <p>Signature: <u>GRAFF.MARK.H.YRUM.1514447</u> Digitally signed by GRAFF.MARK.H.YRUM.1514447 Date: 2021.01.19 14:38:26 -05'00'</p> <p>Date signed: <u>892</u></p>	