

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



**Privacy Impact Assessment
for the
NOAA4960
Pacific Islands Fisheries Science Center (PIFSC)**

Reviewed by: Mark H. Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

03/01/2021

Date

**U.S. Department of Commerce Privacy Impact Assessment
NOAA/NMFS/Pacific Islands Fisheries Science Center (PIFSC)**

Unique Project Identifier: NOAA4960

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

The NOAA Fisheries Pacific Islands Fisheries Science Center 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 way the system operates to achieve the purpose(s) identified in Section 4

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.

(e) 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.

(f) 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 and longline observer data
- Hand-carried data on removable media gathered from research expeditions
- 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

(g) Any information sharing conducted by the system

With regard to the transmission of human resource related data, staff utilize the U.S. Department of Commerce (Department) Kiteworks Secure File Transfer service. Human resource information is sent to NOAA Office of Human Capital Services (OHCS).

PII is shared with the Department of Commerce Western Region Security Office to process security clearances.

Human resources staff at PIFSC (within NOAA4960) provide PII data contained within the SECNAV form to NOAA Inouye Regional Center (IRC) personnel to facilitate building

access.

Foreign national PII is gathered and shared with NOAA headquarters Foreign National Registration System to approve access.

Trip, effort, and catch information for the longline logbook electronic submissions is shared with the NOAA Fisheries Office of Science and Technology. The fisherman reported longline data includes vessel permit and name; departure/return dates and ports; set dates, times, and locations; retained/discarded fish counts; and any protected species interactions (if any).

Information may be shared within the bureau, with DOC bureaus and other Federal agencies in case of breach.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C 1801 et. seq.

Additional authorities from NOAA-6: 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, the Antarctic Marine Living Resources Convention Act, the Western and Central Pacific Fisheries Convention Implementation Act, the International Dolphin Conservation Protection Act, international fisheries regulations regarding U.S. Vessels Fishing in Colombian Treaty Waters, and the Marine Mammal Protection Act and the Fur Seal Act. For seafood companies, the Agriculture and Marketing Act of 1946 and Fish & Wildlife Act of 1956.

The following System of Record Notices (SORNs) apply to information collected, used and disseminated:

DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C 3101, 3309.

DEPT-5: Freedom of Information Act, [5 U.S.C. 552](#); Privacy Act of 1974 as amended, [5 U.S.C. 552a](#).

DEPT-6: Visitor Logs and Permits for Facilities Under Department Control, 44 U.S.C. 3101.

DEPT-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons; Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

DEPT-13: Investigative and Security Records, Executive Orders 10450, 11478, 12065, 5 U.S.C. 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

DEPT-14: Litigation, Claims, and Administrative Proceeding Records, 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.

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.

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

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The FIPS security impact category is **Moderate**.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

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 now 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.
- 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).
- 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).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	
c. Employer ID		h. Alien Registration	X	l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: PII (SSN, Driver's License, Passport #) 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.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X*
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	
c. Alias	X	j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	X
g. Citizenship		n. Religion			
u. Other general personal data (specify):					
*Sales costs in fishing logbooks					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X*	k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify):					
Cell phone or other alternate work/contact number, name of manager/supervisor. Records of classes taken, with names of employees who took them. For federal employees, pay plan, occupational code, grade/level and state/rate for personnel actions.					
Work History data is contained within resumes of applicants. Salary information is stored within employee onboarding documents.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X*	f. Scars, Marks, Tattoos	X**	k. Signatures	X
b. Palm Prints		g. Hair Color	X	l. Vascular Scans	
c. Voice/Audio Recording***	X	h. Eye Color	X	m. DNA Sample or Profile	
d. Video Recording	X	i. Height	X	n. Retina/Iris Scans	
e. Photographs	X	j. Weight	X	o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					
*For onboarding personnel: These are recorded on a stand-alone station and retained only until receipt is confirmed by OSY.					
** These may be on photographs of employees.					
*** Observer or camera on vessel recording video and audio monitoring bycatch.					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X

g. Other system administration/audit data (specify):

Other Information (specify)
 Vessel permit and name; departure/return dates and ports; set dates, times, and locations; retained/discarded fish counts; and any protected species interactions.

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal	X	Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The PII is scanned and stored, not inputted. BII obtained by logbook is hand input via data entry or electronically transmitted. Once input, a series of quality control error checking processes are performed to validate the accuracy of the data. Access to BII/PII is only provided on a need to know basis and the principle of least privilege is applied.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0648- 0214, -0218, -0360, -0441 -0456, -0462, -0463, -0490, -0577, -0612, -0635, -0649, -0664, -0755.
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance	X	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.			

	There are not any IT system supported activities which raise privacy risks/concerns.
--	--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): To facilitate vessel owner/operator access to electronic logbook data which is to be hosted by the NOAA Fisheries Office of Science and Technology.			

Section 5: Use of the Information

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

(a) PII is collected for both contractor and federal employee personnel designated to work with PIFSC. This is information collected for several administration and business functions for the PIFSC:

1. Recall and notifications for CP Planning
2. IRP and outage notification/escalation
3. System Account Management process (i.e. Requesting accounts, approving accounts, terminating accounts etc.)
4. Records of required classes and participants to ensure completion by applicable employees.

(b) A digital and hard copy of each federal employee's hiring package submitted to PIFSC is stored in a secured environment. This includes background checks, Employee Address CD-525, Declaration for Federal Employment OF-306, Health Benefits Election Form OPM SF-2809, Direct Deposit Sign-Up Form SF-1199A, Designation of Beneficiary SF-1152, Self-Identification of Handicap SF-256, Designation of Beneficiary - FERS SF-3102, Statement of Prior Service SF-144, Instructions for Employment Eligibility Verification Form I-9 (with copies of identification), and employee benefits. In some cases these forms are digitally scanned and transmitted within the bureau or inter-governmentally.

(c) For contractual purposes, the PIFSC LAN stores procurement and contract information, stored in a restricted area of the shared drive accessible only by authorized personnel.

(d) Supervisors collect and maintain information from federal employees requiring federal passports, and visitors, volunteers and foreign nationals for permission to access federal facilities. See NAO 207-12

(<https://www.noaa.gov/organization/administration/nao-207-12-technology-controls-and-foreign-national-access>)

(e) Other PII and proprietary BII from fishermen's logbooks include:

1. Captain and vessel name
2. Permit number
3. Fishing locations
4. Fishing methods
5. Catch information
6. Sales costs

Collection of fisherman logbook data helps ensure accurate and timely records about the fishing activity of persons licensed to participate in fisheries under Federal regulations in the Pacific Islands Region. This information is maintained locally with PIFSC systems and is used for research and regulatory purposes (the latter may include civil and criminal law enforcement

and possible litigation) with respect to the fisheries regulation in the Magnuson-Stevens Fishery Conservation and Management Act. Electronic logbook data collected is shared with the NOAA Fisheries Office of Science and Technology to facilitate online hosting of logbook data for vessel owner/operators. This information is collected from members of the public.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

To address insider threat and ensure information is handled, retained, and disposed appropriately, users are required to take IT privacy and security awareness and records management training annually. Other mitigating controls include:

- User acknowledgement of policies, procedures and best practices
- Identification and authentication (multifactor, CAC) before accessing PII
- Least privilege network and systems configuration for systems hosting PII/BII
- Access control to PII through access control lists
- Separation of duties involving access to PII
- Enforcement of least privilege
- File system auditing, review, analysis and reporting
- Log aggregation
- Data loss prevention
- Incident response planning, testing and training
- Encryption of removable media, laptops and mobile devices
- Labeling of digital media to secure handling and distribution
- Sanitization of digital and non-digital media containing PII
- Use of encryption to securely transmit PII
- Encryption of data at rest
- Paper records are maintained in secured file cabinets in areas that are accessible only to authorized personnel of NOAA4960.
- PII/BII is stored on systems with security configuration checklists applied.
- System admins, developers, data users, scientists, administrative assistants and supervisors/managers have access to PII/BII on a need to know basis. Requests to access BII data are handled by a data steward.
- Personnel requiring access to BII are required to sign a non-disclosure agreement, at a minimum annually. Systems transmitting or receiving PII or BII to or from NOAA4960 are required to have an Interconnection Services Agreement.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. (Check all that apply.)

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

<input type="checkbox"/>	The PII/BII in the system will not be shared.
--------------------------	---

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>NOAA4960 interconnects for network transit purposes with NOAA1200. PII and BII is transmitted using DOC Kiteworks. NOAA4960 connects with NOAA4920, the NOAA Fisheries Pacific Islands Region Office, to facilitate exchange of fisheries logbook data. Interconnection communications are secured with encrypted VPN tunnels, and transmitted with secure file transfer protocols such as TLS. Access to the system is protected with multifactor authentication. Access control lists restrict access to sensitive and confidential information on a need to know basis.</p> <p>NOAA4960 connects with NOAA4000 to store employee performance review information. Communications are secured via TLS.</p> <p>NOAA4960 connects with NOAA4020 to facilitate transmission of electronic logbook data. Communications are secured via TLS</p>
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. (Check all that apply.)

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: The Privacy Act statement and/or privacy policy can be found here: https://www.fisheries.noaa.gov/privacy-policy	
X	Yes, notice is provided by other means.	Specify how: The PIFSC/NOAA4960 web site does not collect any personal information from website users. Notice is given to federal employees and contractors, in writing, by their supervisors. For responses to solicitations, notice is given on the request for information (RFI) or request for proposal (RFP). Notice is provided by receipt of the logbooks. There are Pacific Islands Fisheries Science Center logbooks for catching different types of fish and/or using different gear types. These logbooks are printed by PIFSC and distributed to the vessels.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Federal employees and contractors may decline to provide information in writing to their supervisors, but it may affect their job status or their ability to obtain user credentials for the NOAA4960 Information System.
---	---	---

		<p>Responses to RFPs/RFIs are voluntary, based on the offeror’s decision to respond.</p> <p>Fishermen may decline, by not completing their logbooks, but this information is required under the Magnuson-Stevens Act and also to maintain their permits.</p> <p>Visitors and foreign nationals may decline, but they may be denied access to facilities.</p>
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	<p>Specify how: Employees and users accessing the system are provided with the link to NOAA’s privacy policy which states: “Submitting voluntary information constitutes your consent to the use of the information for the stated purpose.”</p> <p>There is only one use for proposals in response to RFIs or RFPs.</p> <p>The only uses for the logbook information are research and regulatory. Completion is required by the Magnuson-Stevens Act, as explained in the NMFS letter to the fisherman, accompanying the permit. Consent to those uses is implied by completion of the logbook.</p>
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	<p>Specify how: All federal/contractor user information is maintained within NOAA Enterprise Messaging System (NEMS) database where users can review and update their contact information.</p> <p>Offerors will contact the office which issued the solicitation, with updated information.</p> <p>Fishermen may contact the PIFSC office and ask to review their own logbook data and request for the information to be updated by the data manager.</p> <p>For eLogbook, data remains stored on the tablet and the captains can log into their account to review any submissions.</p>
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Repositories containing PII/BII have enhanced auditing features enabled.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>7/28/20</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The potential risk of inappropriate disclosure and/or unauthorized disclosure is mitigated by limiting the number of authorized system users, providing initial and annual system security training, monitoring authorized user activity, automatic and immediate notification of unauthorized system access or usage to the system administrator, documenting user violations, and gradually increasing user reprimands for system violations ranging from a verbal warning with refresher security training to denial of system access.

The information is secured via both administrative and technological controls. Users are required to abide by HSPD-12 multifactor authentication to access the system. The principle of least privilege and separation of duties is implemented by PIFSC to ensure that personnel with the need to know only have access to this information. The campus has controlled access. The IT spaces have a sub-set on the controlled access. Access into the data center has an even smaller sub-set of access. Access to the file cabinets has the smallest sub-set of people able to access the systems directly.

All NMFS personnel and contractors are instructed on the confidential nature of this information. Through acknowledgement of the NOAA rules of behavior, account request agreements etc. all users are instructed to abide by all statutory and regulatory data confidentiality requirements, and will only release the data to authorized users.

NOAA4960 connects with NOAA4920, the NOAA Fisheries Pacific Islands Region Office, and NOAA4020, NOAA Fisheries Office of Science and Technology, to facilitate exchange of fisheries logbook data. Communications are secured with encrypted VPN tunnels, and transmitted with FIPS-compliant encryption protocols. Access to the system is protected with multifactor authentication. Access control lists restrict access to sensitive and confidential information by IP and user identity on a need-to-know basis.

Buildings employ security systems with locks and access limits. Only those that have the need to know, to carry out the official duties of their job, have access to the data. The computerized data base 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 NOAA4960.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

 No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (*A new system of records notice (SORN) is required if the system is not covered by an existing SORN*).

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. (list all that apply):</p> <p>NOAA-6: Fishermen's Statistical Data (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/noaa-6.html)</p> <p>DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-1.html), Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C 3101, 3309.</p> <p>DEPT-5: Freedom of Information Act (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-5.html), 5 U.S.C. 552; Privacy Act of 1974 as amended, 5 U.S.C. 552a.</p> <p>DEPT-6: Visitor Logs and Permits for Facilities Under Department Control (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-6.html), 44 U.S.C. 3101.</p>
--	--

	<p>DEPT-9: Travel Records (Domestic and Foreign) of Employees and Certain Other Persons (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-9.html). Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.</p> <p>DEPT-13: Investigative and Security Records (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-13.html), Executive Orders 10450, 11478, 12065, 5 U.S.C. 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.</p> <p>DEPT-14: Litigation, Claims, and Administrative Proceeding Records (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-14.html), 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.</p> <p>DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html), 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> <p>DEPT-25: 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act (https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html), Public Law 106-229; 28 U.S.C. 533-535; Homeland Security Presidential Directive 12 and IRS Publication-1075.</p>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	<p>There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules: Chapter 100 – General Chapter 200-Administrative and Housekeeping Records Chapter 300 - Personnel Chapter 400 – Finance Chapter 500 – Legal Chapter 600– International Chapter 900-Facilities Security and Safety Chapter 1200 – Scientific Research Chapter 1500: 1505-11 and 1507-11</p>
	<p>No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:</p>
X	Yes, retention is monitored for compliance to the schedule.
	<p>No, retention is not monitored for compliance to the schedule. Provide explanation:</p>

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified with the information stored in the system.
X	Quantity of PII	Provide explanation: The quantity of records containing sensitive PII consists of Federal employees and contractors. Sensitive PII collected from employees are maintained within the information system and a physical copy is stored. BII collected on all PIFSC logbooks, consisting of sales costs and fishing location.
X	Data Field Sensitivity	Provide explanation: Logbook BII is sensitive.
X	Context of Use	Provide explanation: Information collected is for granted system accounts and maintaining employee emergency notification lists, as well as in Fisheries Logbooks. Other than business information or emergency contact information no other PII/BII is stored in the information system. Sensitive PII is obtained and transmitted electronically, by fax or mail. The data is eventually removed from information system based on disposition guidelines.
X	Obligation to Protect Confidentiality	Provide explanation: The Magnuson-Stevens Fishery Conservation and Management Act authorizes confidentiality. Privacy Act. OMB M-06-15 Safeguarding Personally Identifiable Information.
X	Access to and Location of PII	Provide explanation: System is not publicly accessible.

	Other:	Provide explanation:
--	--------	----------------------

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Insider threat or malware.
 To ensure information is handled, retained, and disposed appropriately, users are required to take IT security awareness and records management training annually. Other mitigating controls include:
 Identification and authentication (multifactor, CAC) before accessing PII
 Access control to PII through access control lists
 Authorization of users to access BII
 Separation of duties involving access to PII
 Enforcement of least privilege
 System log auditing, review, analysis and reporting
 Encryption of removable media, laptops and mobile devices
 Labeling of digital media to secure handling and distribution
 Sanitization of digital and non-digital media containing PII
 Use of encryption to securely transmit PII
 Encryption of data at rest
 COTS backup and disaster recovery solutions.
 Paper records maintained in secured file cabinets in areas that are accessible only to authorized personnel of NOAA4960.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.