Version Number: 01-2017

U.S. Department of Commerce
NOAA NMFS

Privacy Impact Assessment
for the
Pacific Islands Fisheries Science Center
(PIFSC) Local Area Network (LAN) –
NOAA4960

Reviewed by: Mark 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

for Dr. Catrina Purvis LISA MARTIN Digitally signed by LISA MARTIN Date: 2020.05.09 20:40:02 -04'00' 02/26/2020

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

U.S. Department of Commerce Privacy Impact Assessment
PIFSC LAN – NOAA4960

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

Introduction: System Description

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 then immediately removed from 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 and OMI staff collect PII from visitors and foreign nationals for permission to access federal facilities via fax or email; the information is not stored in the PIFSC information system. 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/drivers license, passport number, date of birth, alien registration number, weight/height, hair color, and 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 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.

Statutory Authority: 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.

PIFSC also stores procurement and contract information, stored in a restricted area of the shared drive accessible only by authorized personnel.

Although this system does not collect, maintain and disseminate badging information, which is collected and stored on paper only, this System of Record Notice (SORN) covers this information:
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 and Privacy Act Request Records, 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: Access Control and Identity Management System, 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.

This system is classified as a moderate system under the Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.

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.
__X__ 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	X
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.

___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

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	e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: PII (SSN, Drivers License, Passport #) for new federal hires, various forms pertaining to onboarding are scanned at a multifunction device, stored on administrative personnel folders, transmitted securely via Kiteworks, and then deleted, this is to facilitate access to our office, which is on a naval base.					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X*
c. Alias	X	i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	X

f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	X
s. Other general personal data (specify):					

*Sales costs in fishing logbooks

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. 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.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X*	d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos	X**	h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. 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.

Note: Photograph referenced in here is passport photo. These are provided by the employee. We don't take photographs.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
Vessel name, fishing locations and methods; Catch information to include count and species; Sales costs.					
Contract proposal-related pre-decisional information.					
Other Information (specify)					

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, -0360, -0441 -0456, -0462, -0463, -0490, -0577, -0612, -0664.
	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): Satellite transmission of logbook (BII) data.			
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		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			
X	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):			

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 hard copy of each federal employee's hiring package submitted to PIFSC is stored in a secured file cabinet. 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. Once the forms are transmitted, they are deleted from the information system.

(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 (http://www.corporateservices.noaa.gov/ames/administrative_orders/chapter_207/207-12.html)

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

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

This information is maintained locally with PIFSC systems and is used only 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. This information is collected from members of the public.

5.2 Describe any potential threats to privacy 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 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
- Separation of duties involving access to PII
- Enforcement of least privilege
- File system 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
- 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.

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):			

* PII is shared within NOAA and DOC or OPM for security vetting purposes/ Law enforcement/privacy breaches.

	The PII/BII in the system will not be shared.

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

X	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: NOAA4960 connects with NOAA4920, the NOAA Fisheries Pacific Islands Region Office, to facilitate exchange of fisheries logbook data. Communications are secured with encrypted VPN tunnels, and transmitted with secure file transfer protocol. 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. NOAA4960 connects with NOAA4000 to store employee performance review information.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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: http://www.nmfs.noaa.gov/aboutus/privacy.html The PIFSC/NOAA4960 web site does not collect any personal information from website users.	
X	Yes, notice is provided by other means.	Specify how: 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. Responses to RFPs/RFIs are voluntary, based on the offeror's decision to respond. Fishermen may decline, by not completing their logbooks, but this information is required under the Magnuson-Stevens Act and also to maintain their permits. Visitors and foreign nationals can say no to providing the information. If they decline to provide the information they

		won't be given access. We can't process a request without it, and would not even attempt to.
	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.	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." There is only one use for proposals in response to RFIs or RFPs. 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.
	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.	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. Offerors will contact the office which issued the solicitation, with updated information. 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.
	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: Servers containing PII/BII are configured to log to the NOAA ArcSight. ArcSight is a NOAA Enterprise application being used to monitor and track activity. NOAA 4960 will open a POA&M to implement monitoring, tracking, and recording access.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 5/1/2019 ☐ 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 supporting 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 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, to facilitate exchange of fisheries logbook data. Communications are secured with encrypted VPN tunnels, and transmitted with secure file transfer protocol. 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.

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 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: NOAA-6, Fishermen's Statistical Data 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 and Privacy Act Request Records, 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: Access Control and Identity Management System, 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.
	Yes, a SORN has been submitted to the Department for approval on (date).
	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	There is an approved record control schedule. Provide the name of the record control schedule: NOAA Records Schedules: Chapter 100 – General Chapter 200-Adminstrative 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
	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:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

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

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 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.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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 levels. *(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 Total quantity of information is minimal and primarily pertains to local Federal employees and contractors. Sensitive PII collected from employees are maintained within the information system but 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
- 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.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Sensitive BII stored in databases must be encrypted at rest. Access to sensitive data must be logged. PII is stored in FIPS compliant encrypted datastores. BII is also stored in encrypted datastores with the exception of two databases for which a POA&M exists to migrate to encrypted datastores.
	No, the conduct of this PIA does not result in any required technology changes.