Version Number: 01-2015

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2017.09.07 17:25:26 -04'00'

8/24/2017

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 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), and other administrative data that contains no PII or BII.

The information collected for general account access is also 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.

Statutory Authority: 5 U.S.C. 1301. Additional authorities from DEPT-18: 44 U.S.C. 3101; 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.

Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 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.

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 is 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.

PIFSC does not share any of this information outside of the bureau, with the exception of law enforcement agencies when needed.

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-25, Access Control and Identity Management System.

The PIFSC is a **Moderate** impact system.

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):					

*See Section 6.2.

_____ This is an existing information system in which changes do not create new privacy risks.

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		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:

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X*
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

*Sales costs in fishing logbooks

Work-Related Data (WRD)					
a. Occupation		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.					

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

Recording/Signatures					
j. Other distinguishing features/biometrics (specify):					

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

Other Information (specify)
Vessel name, fishing locations and methods; Catch information to include count and species; Sales costs.
Contract proposal-related pre-decisional information.

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		Foreign			
Other (specify					

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

2.3 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		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			
To determine eligibility		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): Research			

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) 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.

(c) 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.

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):			

*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.
	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 policy can be found at: __http://www.nmfs.noaa.gov/aboutus/privacy.html and has a link on all Web sites. There is a privacy act statement at: https://www.pifsc.noaa.gov/fmb/fmap/federal_forms/	
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.
	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: Auditing turned on in the Oracle database but it only records database changes. We do not have auditing turned on in the shared drives.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 1/9/2017 ☐ 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 and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
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.

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. PII and BII is stored on shared drives that require CAC for access. 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 and number *(list all that apply)*: DEPT-18 Employees Personnel Files Not

	Covered by Notices of Agencies NOAA-6, Fishermen's Statistical Data DEPT-13, Investigative and Security Records DEPT-25, Access Control and Identity Management System.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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 Disposition Handbook Chapter 200-23 (Personnel Files) and 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 Levels

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.

	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.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: There is BII collected on all PIFSC logbooks, consisting of sales costs and fishing location. Little PII is collected from employees and contractors.
X	Data Field Sensitivity	Provide explanation: Logbook BII is sensitive. There is no sensitive PII collected from employees or contractors.
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 collected or maintained.
X	Obligation to Protect Confidentiality	Provide explanation: The Magnuson-Stevens Fishery Conservation and Management Act authorizes confidentiality.
X	Access to and Location of PII	Provide explanation: System administrator access only.
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.