

**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 D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.09.30 12:24:33 -04'00'

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 Fisheries Science Center (PIFSC) System Local Area Network (LAN) is one of the National Oceanic & Atmospheric Administration's (NOAA) general support systems (GSS). 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 time and attendance, payroll information, personnel, pass and identification, budget, procurement, property, safety, training, and other administrative data

PIFSC collects BII as part of its process to grant access to the information system and for collection of economic data related to US fisheries. 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:

- Employee/Contractor Name
- Business Email
- Business Address
- Business Phone Number
- Alternate phone number (i.e. Cell phone)

Statutory Authority: 5 U.S.C. 1301.

The following information is collected from Pacific Islands Regions fisheries:

- Fishing location
- Fishing gear
- Catch information to include count and species

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

PIFSC does not share this information outside of the system boundary. The information collected is for internal use only.

For economic and regulatory information concerning US fisheries, information collected is considered proprietary in that it can reveal a competitor's primary fishing locations, methods, annual catch information, and sales costs etc. This information is maintained locally with PIFSC systems and is used only for research and regulatory purposes. This information may be shared with other agencies having a legitimate business need and authorization.

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.

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): Identification of the use of BII within the PIFSC information system					

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	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		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):					

--

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					

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

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	X
Other (specify):			

	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	X
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

	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	X	For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):BII is collected for regulatory requirements with respect to fisheries regulation in Magnuson - Stevens			

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).

<p>(a) PII information 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:</p> <ol style="list-style-type: none"> 1. Recall and notifications for CP Planning 2. IRP and outage notification/escalation 3. Account Management process (i.e. Requesting accounts, approving accounts, terminating accounts etc.) 4. NOAA Staff directory <p>(b) Other PII and proprietary or BII information from fishermen’s logbooks includes:</p> <ol style="list-style-type: none"> 1. Captain and vessel name 2. Fishing locations 3. Fishing methods 4. Catch information <p>This information is maintained locally with PIFSC systems and is use only for research and regulatory purposes. This information may be shared with other agencies having a legitimate business need and authorization. This information is collected from members of the public.</p>

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

<input type="checkbox"/>	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:
X	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	
X	Yes, notice is provided by other means.	Specify how: Printed directly on the Logbook
	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, but it may affect their job status. 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: This information is required to obtain user credentials for the NOAA4960 Information System

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 are provided with the link to NOAA's privacy policy where it states: "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose". The only uses for the logbook information are research and regulatory. Consent 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 user information is maintained within NOAA NEMS database where users can review and update their contact information. Fishermen may contact the PIFSC office and ask to review their own logbook data.
	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.
	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: NOAA NEMS manages the database and conducts auditing as required
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>10 AUG 2015</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 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 privileged and separation of duties is implemented by PIFSC to ensure that personnel with the need to know only have access to this information.

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.

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. 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 <i>(list all that apply)</i> : The existing Privacy Act System of records for DEPT-18 Employees Personnel Files Not Covered by Notices of Agencies, apply to the personal information in this system. NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	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	
Degaussing	X	Deleting	
Other (specify):			

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:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
X	Context of Use	Provide explanation: Information collected is for granted system accounts and maintaining employee emergency notification lists. Other than business information or emergency contact information no other PII/BII is collected or maintained
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:

	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.