Version Number: 01-2015

U.S. Department of Commerce
NOAA NMFS

Privacy Impact Assessment
for the
Pacific Islands Regional Office (PIRO)
Local Area Network
NOAA4920

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: 2016.10.17 16:35:37 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
PIRO LAN – NOAA4920

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

Introduction: System Description

The NOAA Fisheries Pacific Islands Regional Office (PIRO) Local Area Network (LAN) functions as the overall General Support System (GSS) for PIRO located in Honolulu, Hawaii. Additional remote sites exist in Samoa, Guam and Saipan. The information system is used to provide administrative support typically found in administrative offices within the federal government as well as supplemental operational services.

PIRO consists of the following divisional units:

- PIR Regional Administrators Office
- NOAA Office of General Counsel
- PIR Habitat Conservation Division
- PIR International Fisheries Division
- PIR Observer Program
- PIR Office of Management and Information
- PIR Protected Resources Division
- PIR Sustainable Fisheries Division

The categories of data collected, stored and disseminated include administrative, human resources, operations, statistical, economic, and technical.

NOAA4920 is located at the following locations: Honolulu, HI, American Samoa, the Commonwealth of the Northern Mariana Islands, and Guam.

The primary functions of the NOAA4920 information system are:

- File and printer sharing
- Web applications and database services
- Access to NOAA/DOC web services via wide area network connections
- Pacific region fisheries permit data repository

No major application systems are supported on NOAA4920.

Information collected within the system includes employee personnel data: names, phone numbers, and addresses to support contact rosters, access to facilities, stored official documents such as travel documents, performance plans, etc. by the employees themselves and various support staff such as supervisor or administrative assistants, 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.

Additional information collected: Federal civil servants and private contractors working for the Fisheries Service, and volunteers working on behalf of PIRO access parts of the system in support of job requirements and mission objectives. Volunteers do not have access to PII/BII on the information system. Supervisors collect and maintain information from visitors and foreign nationals for permission to access federal facilities. Government Passports are required for international travelers, which may include staff, members of the public and foreign visitors.

Finally, the permit data repository consists of contents of permit applications and related documents, such as permit holder name, date of birth or incorporation, Taxpayer Identification Number (TIN), business contact information. The application is downloaded from the PIRO website or obtained from a PIRO office, submitted it to a PIRO office by mail or hand delivery, along with any required supporting documentation and non-refundable application processing fee payment. The National Permit System supports online submission and fee payment (through a link to pay.gov) of permit applications and related information, via secure Web pages. After PIRO reviews and approves the online submission, PIRO issues the permit to the applicant.

Information Sharing:
With regards to the transmission of human resource related data, staff utilize the U.S. Department of Commerce (Department) Accellion Secure File Transfer service. Human resource data and credit card information is sent to NOAA. Human resources personnel transmit PII to the Army to facilitate access to the NOAA Inouye Regional Center (IRC) which is transmitted using the Army's secured AMRDEC SAFE (Safe Access File Exchange).

NOAA4920 shares BII and PII with the following independent, private, state and/or foreign entities:

<u>Regional Fisheries Management Organizations:</u>
At the state or interstate level within the applicable Marine Fisheries Commission for the purpose of co-managing a fishery or for making determinations about eligibility for permits when state data are all or part of the basis for the permits.

Additionally, permit-related information may also be disclosed to the applicable Pacific region or international fisheries management body for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by a regional or international fisheries management body, such as:

- At the Pacific region level within the applicable Marine Fisheries Commission for the purpose of co-managing a fishery or for making determinations about eligibility for permits when Pacific region data are all or part of the basis for the permits, such as: The Western and Central Pacific Fisheries Commission, the South Pacific Regional Fisheries Commission; regional fisheries organizations such as the International Scientific Committee for Tuna and Tuna-like Species in the North Pacific Ocean; and regional intergovernmental organizations such as the Secretariat of the Pacific Community, the Pacific Islands Forum Fisheries Agency, and the Parties to the Nauru Agreement.At the applicable international level within the applicable fisheries management body for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by an international fisheries management body, such as: tThe Food and Agriculture Organization of the United Nations, Commission for the Conservation of Antarctic Marine Living Resources, Inter-American Tropical Tuna Commission, International Pacific Halibut Commission, and International Commission for the Conservation of Atlantic Tunas.
- To foreign governments with whose regulations U.S. fishermen must comply.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the Department. These records or information contained therein may specifically be disclosed as a routine use as stated below. The Department will, when so authorized, make the determination as to the relevancy of a record prior to its decision to disclose a document. These routine uses are listed in the System of Records Notices (SORNs) COMMERCE/NOAA-6, Fishermen's Statistical Data, and COMMERCE/NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries.

Sources of information include the permit applicant/holder, other NMFS offices, the U.S. Coast Guard, and State or Regional Marine Fisheries Commissions.

Applications for permits and registrations are collected from individuals under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C 1801 et. seq., the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Western and Central Pacific Fisheries Convention Implementation Act (WCPFCIA; 16 U.S.C. 6901 et seq), The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.

5 U.S.C. § 301 authorizes the operations of an executive agency including the creation, custodianship, maintenance and distribution of records.

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.
____ 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):					

_X__ This is an existing information system without changes that 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*	X	e. File/Case ID		i. Credit Card	
b. Taxpayer ID**	X	f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration	X	l. Vehicle Identifier	
m. Other identifying numbers (specify): Captain's license, State and Federal Dealer Numbers (if applicable), permit or license numbers for Federal or state permit/licenses issued and start and end dates and other permit status codes, vessel registration number					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: SSNs are collected as part of human resources-related documents.

There is currently an outstanding litigation hold requiring NOAA offices to retain documents and other information and evidence, including "*all records and other information in NOAA's possession, custody or control related to promotions, lateral transfers, employment-enhancing assignments, performance ratings, bonuses, cash awards, and quality step increases from January 1, 2007 to the present.*" (Source: Janet Howard v. U.S. Department of Commerce, Agency Case No. 08-67-00082 (NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION OPEN LITIGATION HOLDS), (Jun. 29, 2015).

In addition, as stated in COMMERCE/NOAA-19, a TIN is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a Federal agency including, but not limited to, if the person is an applicant for, or recipient of, a Federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c) (2) (B) of this statute.

** Taxpayer ID is collected on vessel permit applications: may be either EIN or SSN.

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	X
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): Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, spouse, former spouse, decedent.					

*These are government purchase cards only

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
i. Other work-related data (specify): Vessel name, vessel length overall. Name of corporation, state and date of incorporation of business and articles of incorporation. 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):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

h. **Other Information (specify)** Species, aggregate catch data and statistics, quota share balance, quota pound balance, quota pound limits, listings of endorsements and designations (i.e., gear endorsement, size endorsement, sector endorsement, permit tier) associated with the permit, name of physical IFQ landing site, Exemptions (i.e., Owner on Board - Grandfathered Exemption, Owner on Board, as stated in code of federal regulations) and exemption status, contact persons, Catch/Observer Discard Data, Quota Share/Quota Pound Transfer Data, Business Operation Information (Business Processes, Procedures, Physical Maps).

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: X Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

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

Non-government Sources					
Public Organizations	X	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.

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	
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): (litigation above refers to the litigation hold), determination of qualification for fisheries permits.			

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).

PII/BII is used in a variety of ways, many of which are unique to each individual division as determined by the division chief in accordance with record management, functional, operational or litigation requirements. The information collected and how it is used is broken down by each division.

Information collected from federal employees and contractors

PII is collected for the purposes of hiring and conducting performance reviews.

PII is collected from employees and contractors: for emergency management communication and safety (Continuity of Operations Plan (COOP)).

PII is collected for both contractor and federal employee personnel designated to work with PIRO. This is information collected for several administration and business functions for the PIRO including organizational charts, integrated resource planning and outage notification/escalation, purchasing and tracking of Travel Cards, tracking of training, and litigation holds.

A copy of each employee's forms submitted to PIRO is stored in a personnel folder on the network including 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.

Contract managers collect and maintain information from contractors at the time of service to coordinate work orders and to communicate the needs of the agency.

Supervisors collect and maintain employees' information from doctors during extended sick leave to validate legitimacy of absence. Individuals requesting reasonable accommodation

also provide medical information that supervisors maintain to process reasonable accommodation requests.

GDP and IN: Supervisors collect and maintain information from visitors, volunteers and foreign nationals during passport application and for permission to access federal facilities. See NAO 207-12 (http://www.corporateservices.noaa.gov/ames/administrative_orders/chapter_207/207-12.html)

Permitting
The Protected Species Workshop Coordinator collects name, vessel name, mailing address and phone number from vessel owners and operators to register for Hawaii longline protected species training.
Fisheries permit related BII (Vessel Name, Vessel Operator, Vessel Identifier, Fishing Locations, Catch Information, Observer Incidents, and Observer Post Cruise Log data are covered under Non-Disclosure Agreements and Magnuson/Stevens. Permit related information is stored, depending on the related fishery, either in the Permit application database covered under the NOAA4000 PIA or in the PIRO Permit application Database, both of which are covered under the System of Records Notice (SORN) Commerce/NOAA-19, *Permits and Registrations for United States Federally Regulated Fisheries.*

This information is maintained locally within PIRO and is used primarily for regulatory and administrative purposes. This information may be shared with other agencies as listed in the Introduction, having a legitimate business need and authorization. All information collected is extracted from paper records supplied by the individual or derived from other sources listed in the Introduction, scanned to the network and stored in a shared file.

Public
The Division may collect and maintain name, address, email address, and phone number from the public for comments on proposed actions, published in the Federal Register.

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.)*

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

Foreign entities	X	X	
Other (specify):			

	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: NOAA4920 maintains a Microsoft Active Directory Domain, providing authentication and authorization services for employees. The system is not available publicly and remote sites are connected via secure encrypted VPN links. NOAA4920 interconnects for network transit purposes with NOAA1200, National Oceanic and Atmospheric Administration Corporate Services Local Area Network. PIRO has a dedicated WAN link to NOAA4000 to facilitate data interconnection between other systems within the bureau. Any PII/BII transmitted outside the system is done so using Accellion Secure File Transfer. PII/BII should never transit these interconnections unencrypted, although controls do not currently exist to monitor for the presence and alert if detected.
	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.fpir.noaa.gov/Library/SFD/PI_FedFish_Application_NoEx_Fillable_02Feb15.pdf (this is the Federal Fisheries Permit Application) _____.	
X	Yes, notice is provided by other means.	Specify how: System Wide:

		Authorized users of NOAA4920 information technology systems are notified both in the NOAA rules of behavior and system usage consent warning banner that there is no expectation of privacy while using these systems which includes SAAD and directly associated WRD, and GPD information. Unauthorized users have no reasonable expectation of notification. Employees are notified by their supervisors that their personnel files include their performance information. Job applicants are made aware by a Privacy Act notice on the application that their resume information will be forwarded to hiring managers. Supervisors are required to ask for supporting documents when there is a lengthy sick leave request documentation that is tied to the sick leave request made by the employee through WebTA. The sick leave request has a Privacy Act Statement. For personnel management data, all employee, general public and contractor PII is collected directly from the individual through personal contact, by phone, email or mail. Potential employee PII is willingly provided to the division during the application process. All federal forms have Privacy Act Notices. Permit holders: Notice is given on permit applications.
	No, notice is not provided.	

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: For personnel actions, individuals may decline to provide PII, in writing, to their supervisor or to the Human Resources Office; however, their employment status may be affected. Individuals may decline to provide emergency contact notification to their supervisors, in writing; however, their employment status may be affected. Permit applicants: The personal information is collected when the individual completes the appropriate application. On the application, the individual is advised that NMFS will not be able to issue a permit if the individual does not provide each item of information requested. The individual may choose to decline to provide the required personal information at that time, by not completing the application, but will not be able to receive a permit.
	No, individuals do not have an opportunity to decline to provide PII/BII.	

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: System Wide: By supplying the PII/BII, the individual/entity consents to the use of the information for one particular use only (each type of information collection has a specific purpose). An employee that does not consent to use of PII/BII for user credentials would be unable to access the system, and if not consenting to the use of their PII for COOP, their employment might be affected. Permit applicants and holders: Permittees 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."
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	

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: Supervisors review individuals' PII occasionally to ensure that the emergency contact list is accurate. Employees may review PII in their eOPF file at any time. Employees can also review and update their information on the intranet page. Employees are also made aware via annual data calls that their personal contact information will be maintained as an emergency contact list/COOP plan. The HR personnel folders containing scans of federal employee application forms is restricted to only HR and management personnel with need to know. The information can be updated on request to HR. Permit applicants and holders: Information may be reviewed or updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time (information is on permits and permit applications).
	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.)*

	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: NOAA4920 uses centralized logging which can log and alert when sensitive files and folders are accessed.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _____11/17/2015_____ ☐ 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.

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

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-6, Visitor Logs and Permits for Facilities Under Department Control DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/NOAA #19, Permits and Registrations for United States Federally Regulated Fisheries COMMERC/NOAA-6, Fishermen's Statistical Data, 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 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 – Marine Fisheries
	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	X
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.
	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 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.
X	Data Field Sensitivity	Provide explanation: There is sensitive PII for employees and fishermen, and sensitive BII for fishermen.
X	Context of Use	Provide explanation: Permits information and employee/contractor information is stored securely as described in Sections 8.1 and 8.2.
X	Obligation to Protect Confidentiality	Provide explanation: The Magnuson-Stevens Act authorizes confidentiality of fisheries data. The Health Insurance Portability and Accountability Act protects medical information received in relation to a prolonged illness or self-designation of disability, if applicable.
X	Access to and Location of PII	Provide explanation: System is not publicly accessible.
	Other:	Provide explanation:

Section 12: Analysis

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

X	Yes, the conduct of this PIA results in required business process changes. Explanation: The findings indicate cases where PII is being collected without a bona fide mission/operational requirement. Personnel who work with PII/BII must examine processes and determine if reduction, sanitization or elimination of unneeded PII can be performed. Changes in business processes are administrative and will need to be reviewed and modified through management.
	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.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Based on the amount of sensitive PII in the system, additional technological controls need to be implemented. Repositories need to be defined and secured with encrypted file services. Network protocols for transmittal of sensitive information inside the LAN need to be encrypted. Perimeter and software solutions shall identify PII/BII in transit or in use without authorization. See note in cover email.

	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer
Name: Nick Tenney
Office: NOAA Fisheries, Pacific Islands Regional Ofc
Phone: 808-725-5075
Email: Nick.Tenney@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: TENNEY.NICHOLAS.JAMES.1407926966 Digitally signed by TENNEY.NICHOLAS.JAMES.1407926966 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=TENNEY.NICHOLAS.JAMES.1407926966 Date: 2016.10.03 08:14:38 -10'00'

Date signed: 10/03/2016

System Owner
Name: John Kotsakis
Office: NOAA Fisheries, Pacific Islands Regional Ofc
Phone: (808) 725-5070
Email: John.Kotsakis@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.

Signature: KOTSAKIS.JOHN.P.1241974550 Digitally signed by KOTSAKIS.JOHN.P.1241974550 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=KOTSAKIS.JOHN.P.1241974550 Date: 2016.10.03 14:10:39 -10'00'

Date signed: 10/03/2016

Information Technology Security Officer
Name:
Office:
Phone:
Email:

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.

Signature: Digitally signed by STEARN.WILLIAM.IVAN.1384494222 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=STEARN.WILLIAM.IVAN.1384494222 Reason: As the NMFS IT Security Program Manager, I have reviewed this document. Date: 2016.10.14 09:33:16 -04'00'

Date signed:

Authorizing Official
Name:
Office:
Phone:
Email:

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: TOSATTO.MICHAEL.D.1014020922 Digitally signed by TOSATTO.MICHAEL.D.1014020922 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=TOSATTO.MICHAEL.D.1014020922 Date: 2016.10.05 13:19:29 -10'00'

Date signed:

Bureau Chief Privacy Officer
Name: Mark Graff
Office: NOAA OCIO
Phone: 301-628-5658
Email: mark. graff@noaa.gov

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: SWISHER.DONALD.ROBERT.1376511460 Digitally signed by SWISHER.DONALD.ROBERT.1376511460 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SWISHER.DONALD.ROBERT.1376511460 Date: 2016.10.14 12:19:14 -04'00'

Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.