

**U.S. Department of Commerce
NOAA NMFS**



**Privacy Threshold Analysis
for the
Pacific Islands Regional Office
(PIRO) Local Area Network**

NOAA4920

U.S. Department of Commerce Privacy Threshold Analysis

PIRO LAN – NOAA4920

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

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose:

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.

NOAAA4920 is located at the following locations: Honolulu, HI, American Samoa, the Commonwealth of the Northern Mariana Islands, and Guam. There is information stored onsite at the Saipan location on a full disk FIPS encrypted laptop and hardware FIPS encrypted removable drive. The location is not directly connected to NOAA 4920; they connect directly to the internet via a DSL connection. The single user located in Saipan

connects to the secure NOAA4920 VPN to access NOAA/DOC corporate services and NOAA4920 applications/data. If sensitive PII/BII is transmitted, the user is aware to use Accellion.

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 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.

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.

eDiscovery Application: The eDiscovery Platform system is a web-based application used to simplify agency response to Freedom of Information Act (FOIA) requests, aid in the processing Administrative Records (AR), and to a lesser extent, Congressional Inquiries and Legal Holds. The system serves as a single point for the collection, review, tagging, redaction and export of responsive records.

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 Federal purchaser credit card information is sent to NOAA Human Resources Workforce Division. Human resources staff at PIRO (within NOAA4920) transmit PII (credentials only) to the Army to facilitate access to the NOAA Inouye Regional Center (IRC), using the Army's secured AMRDEC SAFE (Safe Access File Exchange).

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

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

Regional Fisheries Management Organizations:

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: The 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.

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*.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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):			

- 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. *Continue to answer questions and complete certification.*
- This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or later). *Continue to answer questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to

those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Yes. *Please describe the activities which may raise privacy concerns.*

No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII about: (*Check all that apply.*)

Companies

Other business entities

No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: “The term ‘personally identifiable information’ refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc...”

Yes, the IT system collects, maintains, or disseminates PII about: (*Check all that apply.*)

DOC employees

Contractors working on behalf of DOC

Members of the public

No, this IT system does not collect any PII.

If the answer is “yes” to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): _____

Signature of ISSO or SO: TENNEY.NICHOLAS.JAMES.1407926966 Digitally signed by TENNEY.NICHOLAS.JAMES.1407926966 Date: 2019.11.12 07:45:37 -10'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: AMORES.CATHERINE.SOLEIDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEIDAD.1541314390 Date: 2019.11.18 11:05:18 -05'00' Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: TOSATTO.MICHAEL.D.1014020922 Digitally signed by TOSATTO.MICHAEL.D.1014020922 Date: 2019.11.08 17:29:02 -10'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2019.12.02 07:54:10 -10'00' Date: _____