Version Number: 01-2020

U.S. Department of Commerce
National Oceanic & Atmospheric Administration

Privacy Threshold Analysis
for the
NOAA4920
NMFS Pacific Islands Region Office (PIRO)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NMFS/Pacific Islands Region

Unique Project Identifier: NOAA4920

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: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system

The NOAA Fisheries Pacific Islands Regional Office (PIRO) Local Area Network (LAN) functions as an overall General Support System (GSS).

b) System location

PIRO maintains offices in Honolulu, Hawaii, American Samoa, Guam and Saipan.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NOAA4920 interconnects for network transit purposes with NOAA1200, NOAA Corporate Services Local Area Network.

NOAA4920 interconnects with NOAA4960 to facilitate exchange of fisheries observer and logbook data.

PIRO has a dedicated WAN link to NOAA4000 to facilitate connectivity to NMFS Enterprise Active Directory, data interconnection between other systems within the bureau, and access to

corporate services.

d) The purpose that the system is designed to serve

The PIRO LAN exists to support the primary mission, which is to protect and preserve the nation's living marine resources through scientific research, fisheries management, enforcement and habitat conservation. PIRO maintains commercial and recreational fisheries and continues to focus its efforts on sustaining marine resources. The information system provides IT services in support of the following divisional units which perform business operations in support of the primary mission:

- 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

e) The way the system operates to achieve the purpose

The information system provides administrative support typically found in administrative offices within the federal government as well as supplemental operational services. The primary functions of the NOAA4920 information system are:

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

f) A general description of the type of information collected, maintained, used, or disseminated by the system

Divisional unit functions store, process and transmit the following information types:

- Conservation, Marine, and Land Management
- Environmental Remediation

- Legal Prosecution and Litigation
- Standards Setting / Reporting Guideline Development
- Permits and Licensing
- Federal Grants (Non-State)
- Program Monitoring
- Public Comment Tracking
- Regulatory Creation
- Rule Publication
- Budget Execution
- Contingency Planning
- Continuity of Operations
- Service Recovery
- Public Relations
- Administrative
- Travel
- Human resources
- Financial Management
- Information Technical & Management

The information collected contains some sensitive PII/BII, non-sensitive PII, work-related data and video surveillance. This information could be collected from federal employees or contractors for human resource purposes, or from the general public for various permit applications.

g) Identify individuals who have access to information on the system

Government Employees and Contractors have access to the information on the system.

h) How information in the system is retrieved by the user

Information in the system is retrieved by users operating government furnished equipment such as desktops or laptops connected to the LAN or VPN.

i) How information is transmitted to and from the system

Information is transmitted to and from the system by:

- Direct data entry
- Data exchange via interconnected services to facilitate sharing of statistical observer data collected at sea
- Use of Google G.Suite (E-mail, Google Docs)
- Use of DOC Kiteworks to transmit sensitive PII
- Download of publicly available fisheries research data from various internet sources
- All PII/BII is encrypted during transit.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____X 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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Security cameras recording video at the Samoa office.					

____ 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 01-2017). *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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

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.

____X Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): Video surveillance at the Samoa and Pier 38 facilities.			

____ 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.)."

____X Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when

combined with other information that is linked or linkable to a specific individual."

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

X DOC employees
X Contractors working on behalf of DOC
___ Other Federal Government personnel
X 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 Social Security numbers (SSNs), including truncated form?

X Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. PII (SSN, Driver's License, Passport #) are required for new federal hires, various forms pertaining to onboarding are scanned at a multifunction device, stored on administrative personnel folders, and transmitted securely via Kiteworks.
Provide the legal authority which permits the collection of SSNs, including truncated form. DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies, E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

___ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

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

X 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.

4d. 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.

_X_ 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, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

X I certify the criteria implied by one or more of the questions above **apply** to the NOAA4920 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.

Information System Security Officer or System Owner Name: John Kotsakis Office: Phone: Email: John.Kotsakis@noaa.gov Signature: KOTSAKIS.JOHN.P.1241974550 Digitally signed by KOTSAKIS.JOHN.P.1241974550 Date: 2021.10.06 09:28:36 -10'00' Date signed: 0	**Information Technology Security Officer** Name: Catherine Amores Office: Phone: Email: Catherine.Amores@noaa.gov Signature: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2021.10.12 16:51:46 -04'00' Date signed:
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 240-577-2372 Email: Adrienne.Thomas@noaa.gov Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.10.19 07:12:49 -05'00' Date signed: 0	**Authorizing Official** Name: Michael Tosatto Office: Phone: Email: Michael.Tosatto@noaa.gov Signature: TOSATTO.MICHAEL.D.1014020922 Digitally signed by TOSATTO.MICHAEL.D.1014020922 Date: 2021.10.06 10:33:53 -10'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.11.16 11:17:26 -05'00' Date signed: 47892	