Version Number: 01-2021

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

Privacy Threshold Analysis for the
NOAA4930
Southwest Fisheries Science Center (SWFSC)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NMFS/Southwest Fisheries Science Center (SWFSC)

Unique Project Identifier: NOAA4930

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: *Provide a brief description of the information system.*

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).

NOAA4930 is a General Support System supporting users consisting of scientific, administrative, and support staff distributed among the California cities/communities of La Jolla, Monterey, and Santa Cruz. There are a variety hardware platforms and operating systems interconnected on this network system. The systems are designed and configured to support the staff in meeting the agency scientific mission. No information or applications have been removed from the system.

Address the following elements:

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

The NOAA4930 system is a General Support System supporting approximately 300 personnel consisting of scientific, administrative, and support staff.

b) System location

The NOAA4930 system is comprised of the NOAA/NMFS Southwest Fisheries Science Center facilities located in the cities/communities of La Jolla, Santa Cruz and Monterey in the state of California.

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

The NOAA4930 system is interconnected with the NMFS WAN (NOAA4000), NMFS NWFSC (NOAA4600), NMFS Office of Science and Technology (NOAA4020), N-Wave (NOAA0550), University of California, San Diego, and University of California, Santa Cruz.

d) The purpose that the system is designed to serve

The NOAA4930 system is designed and configured to support the staff in meeting the agency mission in fisheries research, the management of local human resources and facilities.

e) The way the system operates to achieve the purpose

The operational system functions that are provided include:

- Network File Storage, Sharing, and Printing
- Internet Access
- NMFS Wide Area Network Connectivity
- Administrative Support Systems
- Scientific Database Access
- Scientific Statistical Data Analyses
- Geographic Information Systems
- Web Based Information Dissemination
- Telecommunications

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

The categories of data inputted, stored and processed include administrative, scientific, statistical, economic, research and development, and technical.

As a requirement of the Highly Migratory Species (HMS) Fisheries Management Plan (FMP) implemented in 2005, participants (captains of permitted vessels) in HMS fisheries in the Pacific arc required to submit logbook information on fishing activities. In addition, to monitor these fisheries and provide accurate catch estimates as required under the FMP and international obligations, landings information is collected and maintained. Biological and life history data arc also collected and maintained to supplement stock assessment information used to assess and monitor fish stocks.

The logbook and landings data contain information that identifies fishery participants and contains information related to the business practices of those participants: Names, contact information, including work and home e-mail and mailing addresses and phone numbers, vessel and processor identifiers and sales information including dates, buyers, sellers, amounts and

prices .

These data are submitted to the Southwest Fisheries Science Center (SWFSC), where the information is entered into a centralized Oracle database, in an encrypted table space, that is located and maintained at the National Marine Fisheries Service (NMFS) Office of Science and Technology in Silver Spring, Maryland. These data are maintained by SWFSC staff and summarized for reporting. Summarization of the data follows established business rules for maintaining confidentiality of the summaries. Any information obtained from fewer than three persons is further aggregated and combined with other data.

The maintaining of physical security for NOAA4930 facilities includes the use of building entry (keycard) readers and video surveillance. For the building entry readers, the NOAA4930 system employs the CCure system. This system uses HID keycards for the readers. The information collected and stored for each staff member consists of the unique ID number on the HID card and the staff member's name. No other information is collected. For the video surveillance system, signs are present around the facility perimeters informing all individuals that video surveillance is being conducted. The data is only accessible to authorized administrative personnel who monitor the physical security of the building and IT system administration staff. The data that is stored is retained for 30 days and is then overwritten. The data in both of these systems is not disseminated.

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

NOAA4930 information is accessed by NOAA4930 authorized personnel which can include employees, contractors, cooperative institute employees, students and volunteers.

Authorized users (NMFS employees and contractors) have access to the confidential logbook and landings information and access is controlled through database roles. All authorized users that access confidential information must sign a non-disclosure agreement that certifies that the user has read and understands NOAA Administrative Order on Confidentiality of Statistics (NAO 216-100). These non-disclosure agreement are maintained at SWFSC.

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

NOAA4930 information is retrieved via government furnished IT equipment after verifying authentication and authorization levels.

Local data are stored on a Windows network fileshare. Access to data stored locally is restricted to authorized personnel only via Windows AD group. Authorized users authenticate to access the data via two factor authentication (CAC card). For authorized users who are in the process of obtaining a CAC card, they access the system via username and strong password that meet the DOC password requirements. The principle of least privilege and separation of duties is implemented by SWFSC to ensure that personnel with the need to know only have access to this information.

Authorized users who access the data from outside of the NOAA4930 boundary may only do so via NMFS VPN concentrators (East or West). The NMFS VPN connections are encrypted, the users must authenticate onto the VPN via two factor authentication, and the authorized user may only connect to the

NMFS VPN with government furnished equipment (GFE) that is subject to all FISMA system requirements.

i) How information is transmitted to and from the system

NOAA4930 transmission is protected using defense in depth architecture. Particularly sensitive information is encrypted while in transmission.

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): Video surveillance and building entry readers information is now being collected.					

____ 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. *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	X
Video surveillance	X	Electronic purchase transactions	
Other (specify):			

___ 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
X 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. The business need for collecting SSN data is with personnel management – human resources. This information is required on forms for onboarding new hires.
Provide the legal authority which permits the collection of SSNs, including truncated form. 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107

____ 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 The criteria implied by one or more of the questions above **apply** to the NOAA4930 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the NOAA4930 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: Richard Cosgrove Office: NMFS SWFSC Phone: 858-546-7057 Email: Rich.Cosgrove@noaa.gov Signature: COSGROVE.RICHARD.E.III.1365890672 Digitally signed by COSGROVE.RICHARD.E.III.1365890672 Date: 2023.02.03 14:53:55 -08'00' Date signed: _____	**Information Technology Security Officer** Name: Cathy Amores Office: NMFS OCIO Phone: 301-427-8871 Email: Catherine.Amores@noaa.gov Signature: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2023.02.08 10:24:45 -05'00' Date signed: _____
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.02.13 08:39:55 -05'00' Date signed: _____	**Authorizing Official** Name: John Crofts Office: NMFS SWFSC Phone: 858-546-7150 Email: John.Crofts@noaa.gov Signature: CROFTS.JOHN.AARON.1249242388 Digitally signed by CROFTS.JOHN.AARON.1249242388 Date: 2023.02.03 15:04:53 -08'00' 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: 2023.02.16 13:14:29 -05'00' Date signed: _____	