Version Number: 01-2017

U.S. Department of Commerce
NOAA

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

U.S. Department of Commerce

Privacy Threshold Analysis

NOAA4930 - Southwest Fisheries Science Center (SWFSC) Network

Unique Project Identifier: 006-03-02-00-01-0511-00

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: NOAA4930 is a General Support System supporting users consisting of scientific, administrative, and support staff distributed among the California cities 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 mission.

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) The NOAA4930 system is a General Support System supporting approximately 332 users consisting of scientific, administrative, and support staff.
b) The NOAA4930 system is comprised of the NOAA/NMFS Southwest Fisheries Science Center facilities located in the cities of La Jolla, Santa Cruz and Monterey in the state of California.
c) The NOAA4930 system is interconnected with the NMFS WAN (NOAA4000).
d) 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 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) The categories of data inputted, stored and processed include administrative, scientific, statistical, economic, research and development, and technical.
g) NOAA4930 information is accessed by NOAA4930 authorized personnel which can include employees, contractors, students and volunteers.
h) NOAA4930 information is retrieved via government furnished IT equipment after verifying authentication and authorization levels.
i) NOAA4930 transmission is protected using defense in depth architecture. Particularly sensitive information is encrypted while in transmission.

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.*

__X__ 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). *Skip 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.*

_X__ 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 about: *(Check all that apply.)*

_X__ 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..."

_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__ 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?

_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.

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.

_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, 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

__X__ I certify the criteria implied by one or more of the questions above **apply** to the NOAA4930 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 NOAA4930 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): Heather Nicholas

Signature of ISSO or SO: NICHOLAS.HEATHER.BIGIO.1545594320 Digitally signed by NICHOLAS.HEATHER.BIGIO.1545594320 Date: 2019.10.08 08:46:43 -07'00' Date: _____

Name of Information Technology Security Officer (ITSO): Catherine Amores

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2019.11.06 15:54:10 -05'00' Date: _____

Name of Authorizing Official (AO): John Crofts

Signature of AO: CROFTS.JOHN.A.1249242388 Digitally signed by CROFTS.JOHN.A.1249242388 Date: 2019.10.08 09:24:20 -07'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Mark Graff

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: 2019.11.20 13:14:41 -05'00' Date: _____