Version Number: 01-2017

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

Privacy Threshold Analysis
for the NOAA4800 - Alaska Fisheries Science Center (AKFSC) Network

U.S. Department of Commerce Privacy Threshold Analysis

National Oceanic and Atmospheric Administration
NOAA4800 - Alaska Fisheries Science Center (AKFSC) 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: The NOAA4800 system consists of a series of Local Area Networks (LANs) connected via a shared Wide Area Network (WAN) connection. The LANs are separated from the WAN by a firewall and router. Via the system identified as NOAA4000, NMFS CIO staff manage the WAN and all of the firewalls except for the Seattle LAN firewall. A common Active Directory, managed by the NMFS EAD staff, binds the LANs into one system. See diagram below.

System Specific Information:

a) NOAA4800 is a General Support System.

b) The primary site of NOAA4800 is Seattle, WA. Additional locations are Newport, OR, Juneau, AK, Anchorage, AK, Kodiak, AK, and Dutch Harbor, AK.

c) NOAA4800 is interconnected with the NMFS LAN (NOAA4000), which provides transport services.

d) The purpose of the NOAA4800 system is to provide information storage and computational resources for NOAA Fisheries scientists.

e) In order to achieve its purpose, NOAA4800 provides connectivity between individual end-user computers to infrastructure devices such as files servers, through networking devices such as firewalls, routers, and switches.

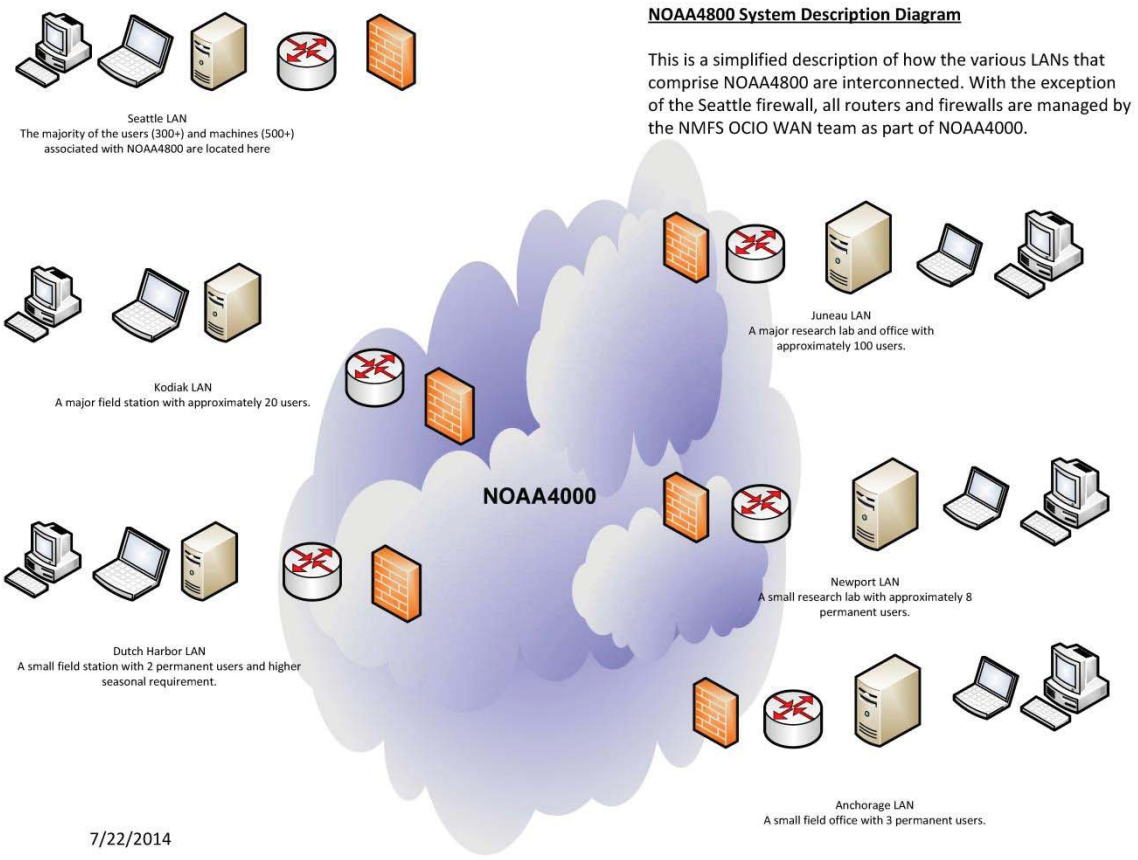
f) NOAA4800 collects, maintains, and uses several types of information, including natural resource data (conservation, marine ecosystems, and mammals), administrative data (budget formulation, budget planning), general workforce management data (number of contractors,

contracting budgets, etc.), and information technology data (help desk, infrastructure, system development, and security.

g) A staff of approximately 500 people composed of biologists, physical scientists, administrative, and support professionals have access to information on the NOAA4800 system.

h) Information is retrieved from servers to desktop and laptop computers via file sharing technologies.

i) Information is transmitted locally via file sharing protocols, and externally via NOAA4000.



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). *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.*

_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
_X__ 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.)*

____ DOC employees
____ 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.

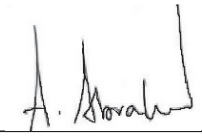
If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the [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 System Owner (SO): _Ajith Abraham_____

Signature of SO:  Digitally signed by ABRAHAM.AJITH.1365899238 Date: 2018.02.07 08:22:31 -08'00' Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2018.02.13 13:20:28 -05'00' Date: _____

Name of Authorizing Official (AO): _Jeremy Rusin_____

Signature of AO: RUSIN.JEREMY.DEWITT.1380624407 Digitally signed by RUSIN.JEREMY.DEWITT.1380624407 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=RUSIN.JEREMY.DEWITT.1380624407 Date: 2018.02.07 13:35:40 -08'00' 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: 2018.02.14 09:16:08 -05'00' Date: _____