U.S. Department of Commerce
National Marine Fisheries Service (NMFS)

Privacy Threshold Analysis
for the
NOAA4000 - Fisheries WAN and Enterprise Services

U.S. Department of Commerce Privacy Threshold Analysis
NOAA4000 - Fisheries WAN and Enterprise Services
**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 NMFS Headquarters information system (NOAA4000) is divided up into the following major components or areas of responsibility: IT Infrastructure and IT Services. IT Infrastructure is comprised of the hardware and software used within the environment to support the NMFS mission. The IT Services component on the other hand are those technology services provided to the NMFS organization that are supported by the IT infrastructure. The final component of the NOAA4000 system are the physical locations where the end-users and IT infrastructure reside.

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) General Support System with these applications: Seafood Inspection Services Portal (SISP), Foreign National Registration System (FNRS), Electronic Document Management System (EDMS), Vessel Monitoring System (VMS), Trident (law enforcement), Natural Resources Damage Assessment Database (NRDA, Restoration and Conservation Database (RCDB), Electronic Annual Operating Plan (eAOP), Marine Mammal Health and Stranding Response Program (MMHSRP), Public Consultation Tracking System (PCTS), General Counsel Litigation Database (GCLD), Rhythmx CMS (web content management system, National Permit System (NPS) and eDiscovery Application.

b) Silver Spring, MD (SSMC3)
Interconnects with several systems. NOAA's firewalls are configured to allow incoming connections from predetermined external IPs. We also use SSL public key encryption.

c) i) US Coast Guard
   ii) Pacific States Marine Fisheries Commission
   iii) US Custom and Border Protection
   iv) Information Technology Center (ITC - NOAA1101)
v) Other NOAA NMFS Systems (Permits, S&T, GARFO, NEFSC, SER, SEFSC, NWR, NWFSC, AKR, AKFSC, SWR, PIR, SWFSC, PIFSC)

vi) TRIDENT/Justware interconnection

d) The primary purpose of NMFS WAN connectivity:
   • Connectivity to Fisheries sites throughout the United States.
   • Access to electronic messaging to allow employees to send messages to Fisheries employees and external colleagues
   • Internet access

e) IT Services
   HQ based services
      Local Area Network (LAN)
      VoIP
   Enterprise services
      Wide Area Network (WAN)
      Service Desk
      Application Hosting
      Security Services
      Enterprise Active Directory

f) Identifying numbers: Social Security, Taxpayer ID, Driver’s License, Employer ID, Passport, Financial Transaction, Employee ID, Voice Recordings. Permits - Captain’s license, State and Federal Dealer Numbers (if applicable), permit or license numbers for Federal or state permit/licenses issued and start and end dates and other permit status codes, vessel registration number; General personal data: Name, maiden name, alias, gender, race/ethnicity, age DoB, Place of Birth, home address, telephone number, email address, financial information, medical information, physical characteristics; Work-related data: Occupation, job title, work address, work telephone number, email address, salary, work history, job description, grade, performance appraisals (EDMS); photographs, approved fishing licenses, type of fishing gear being used, vessel location (VMS, TRIDENT) case files, file/case id and information on the catch (TRIDENT), sworn witness accounts, and (web facing) publicly available information, audit data, seized property (TRIDENT), Vessel ID Number for VMS and TRIDENT; photographs, voice recordings (TRIDENT).

g) All users authorized to access the WAN using 2-factor authentication. Public Web - any user.

h) Via WAN connection and web interface.

i) Via WAN connection and web interface.

Questionnaire:
1. 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.*

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
</tbody>
</table>
| j. Other changes that create new privacy risks (specify): Implementation of E-Discovery software for FOIA, Administrative Record, and litigation purposes. *Explanation of significant merging:* addition of TRIDENT and decommissioning of NERI.

____ 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). *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. 

__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.)

__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 NOAA4000 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):

BRIDGETT.CYNTHIA.MCCANN.1460827074

Signature of ISSO or SO: Digitally signed by BRIDGETT.CYNTHIA.MCCANN.1460827074 827074 Date: 2018.02.08 07:03:11 -05'00'

Name of Information Technology Security Officer (ITSO):

AMORES.CATHERINE.SOLEDAD.1541314390

Signature of ITSO: Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 390 Date: 2018.02.06 16:42:33 -05'00'

Name of Authorizing Official (AO):

VARGHESE.KOYICKAL.ROY.1400785496

Signature of AO: Digitally signed by VARGHESE.KOYICKAL.ROY.1400785496 496 Date: 2018.02.14 16:30:01 -05'00'

Name of Bureau Chief Privacy Officer (BCPO):

GRAFF.MARK.HYRUM.1514447892

Signature of BCPO: Digitally signed by GRAFF.MARK.HYRUM.1514447892 892 Date: 2018.02.06 10:16:46 -05'00'