Version Number: 01-2017

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

Privacy Threshold Analysis
for the
National Marine Fisheries
Alaska Region

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/National Marine Fisheries, Alaska Region

Unique Project Identifier: [Number]

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 Alaska Region (AKR) of National Oceanic & Atmospheric Administration (NOAA) Fisheries is one of six regional offices. The AKR oversees sustainable fisheries that produce about half the fish caught in US waters, with responsibilities covering 842,000 square nautical miles of water surrounding Alaska. The AKR also works to ensure the viability of protected species—principally marine mammals—and to protect and enhance Alaska's marine habitat.

The AKR Local Area Network (LAN) NOAA4700 is one of NOAA's general support systems (GSS), an interconnected information resource under direct management control with shared common functionality. NOAA4700 is a GSS that supports the AKR's mission with the following major applications: office automation; public interface via the Internet; and fisheries information management, including permits and catch accounting. NOAA4700 is a **Moderate** impact system.

The PII and BII that NOAA4700 collects may be categorized as **Personnel/Contracting**, **Permitting**, and **Strandings**. Each category is further discussed below.

Personnel/Contracting: In the course of daily business, the following information is routinely collected and maintained on AKR federal employees and contractors:

- Employee/Contractor Name
- Address
- Date of birth
- Social Security Number
- Business Email
- Business Address
- Business Phone Number
- Alternate phone number (i.e. cell phone)

This information is used for:

- Security investigations

- Federal employee personnel actions
- Federal employee performance reviews
- Federal employee payroll
- Federal employee awards
- HSPD-12 Common Access Cards

Information Sharing: The information is shared with NOAA Fisheries, the Office of Personnel Management, the Department of Commerce (DOC) Office of Security, the Defense Enrollment Eligibility Reporting System (DEERS), and the Real-Time Automated Personnel Identification System (RAPIDS).

Statutory Authority: 5 U.S.C. 1301.

Permitting: In order to manage U.S. fisheries, the NOAA Fisheries requires the use of permits or registrations by participants in the United States. Information in the NOAA4700 system consists of contents of permit applications and related documents, such as permit transfers and percentage of ownership in a corporation. A typical transaction is an initial or renewal permit application: the permit holder or applicant completes an application downloaded from the AKR website, submits it to the AKR by mail, along with any required supporting documentation and/or required fee payment, and receives a new permit once approved by the AKR. AKR also provides the option of online submission of permit applications and related information, via secure web pages.

The following information may be collected:

- Name
- Address
- Date of birth
- Social Security Number/Tax Identification Number
- Marriage certificates
- Divorce decrees
- Death certificates
- Vessel name

Information Sharing: Information is shared within the AKR in order to coordinate monitoring and management of sustainability of fisheries and protected resources (see next paragraph for additional sharing information). Sources of information include the permit applicant/holder, other NMFS offices, the U.S. Coast Guard, and the Pacific States Marine Fisheries Commission (PSMFC).

Information may also be disclosed:

- At the state or interstate level within the PSMFC for the purpose of co-managing a fishery or for making determinations about eligibility for permits when state data are all or part of the basis for the permits.

- To the North Pacific Fishery Management Council staff and contractors tasked with development of analyses to support Council decisions about Fishery Management Programs.
- To the International Pacific Halibut Commission (IPHC) for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by the IPHC.
- To the public: Vessel Owner Name, Name of Vessel and Permit Number are made publically available through our website. Notice of this is given on the permit application. We also allow other regions, centers and state organizations access to the publically available information directly from our database through a secure connection. This information is considered part of the public domain.

Statutory Authorities: Applications for permits and registrations are collected from individuals under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the High Seas Fishing Compliance Act, the American Fisheries Act, the Northern Pacific Halibut Act, the Marine Mammal Protection Act, the Endangered Species Act, and the Fur Seal Act. The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.

Strandings: The AKR collects and compiles data about marine mammal strandings throughout Alaska. The network is composed of state and federal wildlife and fisheries agencies, veterinary clinics, Alaska Native organizations, academic institutions, and individuals who respond to or provide professional advice on handling strandings.

Information collected includes:

- Name
- Telephone Number
- Email

Information Sharing: Strandings information may be shared with members of the AKR Strandings Network including:

- Alaska
    - Alaska Consortium of Zooarchaeologists
    - Alaska Department of Fish and Game
    - Alaska Sea Grant Marine Advisory Program
    - Alaska Sealife Center
    - Alaska Veterinary Pathology Services
    - The Alaska Whale Foundation
    - Aleut Community of St. Paul and Fur Seal Disentanglement Project
    - Rachel Berngartt, DVM
    - Chicago Conservation Council
    - Glacier Bay National Park and Preserve
    - NOAA Fisheries Alaska Region
    - North Slope Borough

- The Petersburg Marine Mammal Center
- Sitka Sound Science Center
- University of Alaska Southeast, Juneau
- University of Alaska Southeast, Sitka
- University of Alaska Fairbanks, Marine Advisory Program
- University of Alaska Fairbanks, Museum of the North
- U.S. Fish and Wildlife Service, Alaska Region
- U.S. Forest Service, Alaska

- National
  - Marine Mammal Health and Stranding Response Program
  - Prescott Marine Mammal Rescue Assistance Grant Program
  - Unusual Marine Mammal Mortality Events Working Group
- Research
  - National Marine Mammal Laboratory
  - University of Alaska Museum Specimen Database (external website)

Statutory Authorities: The Marine Mammal Protection Act, the Endangered Species Act, and the Fur Seal Act.

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.*

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): Implementation of E-Discovery software for FOIA, Administrative Record, and litigation purposes.					

____ 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). *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.)*

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 NOAA4700 and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of Information System Security Officer (ISSO) or System Owner (SO):
Kenneth J. Brainard

BRAINARD.KENNETH.J.1162337811

Digitally signed by BRAINARD.KENNETH.J.1162337811
Date: 2018.04.25 10:38:53 -07'00'

Signature of ISSO or SO: _____ Date: _____

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

AMORES.CATHERINE.SOLEDAD.1541314390

Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390
Date: 2018.04.27 13:22:34 -04'00'

Signature of ITSO: _____ Date: _____

Name of Authorizing Official (AO):
Dr. James Balsiger

BALSIGER.JAMES.W.DR.1365862962

Digitally signed by BALSIGER.JAMES.W.DR.1365862962
Date: 2018.04.27 08:00:37 -08'00'

Signature of AO: _____ Date: _____

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

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: 2018.04.30 08:03:56 -04'00'

Signature of BCPO: _____ Date: _____