

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



**Privacy Threshold Analysis for the
NOAA4700
Alaska Region**

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NWS/Alaska Region

Unique Project Identifier: NOAA4700

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).

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

NOAA4700 is a general support system 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.

Address the following elements:

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

The NMFS Alaska Region 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.

b) System location

Alaska Region has three offices located in the following locations

Juneau Federal Building - Juneau, AK

Anchorage Federal Building - Anchorage, AK

Remote Office, Dutch Harbor - AK

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

Alaska Region has interconnect agreements with the following:

- Elandings application
- NOAA4000 – eDiscovery Application
- NOAA4000 – Enterprise Storage Area Network (SAN)
- NOAA0550 – Fisheries WAN and Enterprise Services
- NOAA4000 – OLE Headquarters
- NOAA4000 – UDC37J National Permit System – BOF Site
- NOAA4800 – Alaska Fisheries Science Center (AKFSC) Network
- NOAA4020, Science and Technology, Network encryption
- NOAA4600, NOAA Seattle Local Area Network, Network encryption

d) The purpose that the system is designed to serve

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. Note: submission by mail cannot immediately be eliminated, as the option is included in the applicable regulations.

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

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
- Recall and notifications for continuity planning
- Incident response plan and outage notification/escalation

- Account management processes (i.e., Requesting accounts, approving accounts, terminating accounts etc.)
- NOAA Staff Directory

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.

e) The way the system operates to achieve the purpose

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
- Recall and notifications for continuity planning
- Incident response plan and outage notification/escalation
- Account management processes (i.e., Requesting accounts, approving accounts, terminating accounts etc.)
- NOAA Staff Directory

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

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. Note: submission by mail cannot immediately be eliminated, as the option is included in the applicable regulations.

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

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

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
- Recall and notifications for continuity planning
- Incident response plan and outage notification/escalation
- Account management processes (i.e., Requesting accounts, approving accounts, terminating accounts etc.)
- NOAA Staff Directory

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

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. Note: submission by mail cannot immediately be eliminated, as the option is included in the applicable regulations.

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

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

Various users have access to the information on the system according to need.

Personnel/Contracting:

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).

Permitting:

Information is shared within the AKR in order to coordinate monitoring and management of sustainability of fisheries and protected resources. 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.

Stranding:

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

- Alaska
 - o Alaska Consortium of Zooarchaeologists
 - o Alaska Department of Fish and Game
 - o Alaska Sea Grant Marine Advisory Program
 - o Alaska Sealife Center
 - o Alaska Veterinary Pathology Services
 - o The Alaska Whale Foundation
 - o Aleut Community of St. Paul and Fur Seal Disentanglement Project
 - o Rachel Berngartt, DVM
 - o Chicago Conservation Council
 - o Glacier Bay National Park and Preserve
 - o NOAA Fisheries Alaska Region
 - o North Slope Borough
 - o The Petersburg Marine Mammal Center
 - o Sitka Sound Science Center
 - o University of Alaska Southeast, Juneau
 - o University of Alaska Southeast, Sitka
 - o University of Alaska Fairbanks, Marine Advisory Program
 - o University of Alaska Fairbanks, Museum of the North
 - o U.S. Fish and Wildlife Service, Alaska Region
 - o U.S. Forest Service, Alaska
- National
 - o Marine Mammal Health and Stranding Response Program
 - o Prescott Marine Mammal Rescue Assistance Grant Program
 - o Unusual Marine Mammal Mortality Events Working Group
- Research
 - o National Marine Mammal Laboratory
- University of Alaska Museum Specimen Database (external website)

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

Information is retrieved by the user using a combination of Database Links, Web Based Applications, and File Format Applications (*Word, Excel, Etc.) over the NOAA4700 system and various web access applications available via the Internet.

i) *How information is transmitted to and from the system*

Information is transmitted across approved encryption protocols such as HTTPS, SSH, and SSL. Sensitive data transmissions are encrypted according to NIST 800-18, Federal Information Processing Standards (FIPS) 186, Digital Signature Standard and FIPS 180-1, and Secure Hash Standard issued by NIST when necessary.

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.*

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.*

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.

Yes. (*Check all that apply.*)

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

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.

_____ 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

_____ 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.

Social Security and tax identification numbers as well as employee ID are all required for the hiring and employment process in order to conduct background checks, issue ID, and file proper tax documents for the Federal Employee or Contractor.

Social Security numbers and tax identification numbers (TIN) allow positive identification for cost recovery billing of IFQ holders. Also, as stated in COMMERCE/NOAA-19, a TIN is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a Federal agency including, but not limited to, if the person is an applicant for, or recipient of, a Federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c) (2) (B) of this statute.

Provide the legal authority which permits the collection of SSNs, including truncated form.
5 U.S.C. 1301.

- 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
- Fur Seal Act
- The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.

— 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

The criteria implied by one or more of the questions above **apply** to the NOAA4700 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 NOAAXXXX and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

<p>Information System Security Officer or System Owner</p> <p>Name: David Hanson Office: NMFS-AKR Phone: 907-586-7054 Email: david.hanson@noaa.gov</p> <p>HANSON.DAVID.W <small>Digitally signed by HANSON.DAVID.WAYNE.10431915 90 Date: 2023.02.15 15:58:11 -09'00'</small></p> <p>Signature: <u>AYNE.1043191590</u></p> <p>Date signed: _____</p>	<p>Information Technology Security Officer</p> <p>Name: Catherine Amores Office: NMFS Phone: 301-427-8871 Email: Catherine.amores@noaa.gov</p> <p>AMORES.CATHERINE.S <small>Digitally signed by AMORES.CATHERINE.SOLEDAD.1 541314390 Date: 2023.02.17 12:25:24 -05'00'</small></p> <p>OLEDAD.1541314390</p> <p>Signature: <u>541314390</u></p> <p>Date signed: _____</p>
<p>Privacy Act Officer</p> <p>Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov</p> <p>BURRESS.ROBIN.SU <small>Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.02.24 10:26:27 -05'00'</small></p> <p>Signature: <u>RRETT.1365847696</u></p> <p>Date signed: _____</p>	<p>Authorizing Official</p> <p>Name: Jon Kurland Office: NMFS-AKR Phone: 907-586-7221 Email: Jon.Kurland@noaa.gov</p> <p>KURLAND.JONATHAN.M <small>Digitally signed by KURLAND.JONATHAN.M.1365896514 Date: 2023.02.15 16:48:10 -09'00'</small></p> <p>Signature: <u>AN.M.1365896514</u></p> <p>Date signed: _____</p>
<p>Bureau Chief Privacy Officer</p> <p>Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov</p> <p>GRAFF.MARK.HYR <small>Digitally signed by GRAFF.MARK.HYRUM.151444789 2 Date: 2023.03.07 09:33:05 -05'00'</small></p> <p>Signature: <u>UM.1514447892</u></p> <p>Date signed: _____</p>	