

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



**Privacy Impact Assessment
for the
NOAA4700
Alaska Region**

Reviewed by: Mark H. Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

04/14/2021

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA/NMFS/ Alaska Region

Unique Project Identifier: NOAA4700

Introduction: System Description

Provide a description of the system that addresses the following elements:

The response must be written in plain language and be as comprehensive as necessary to describe the system.

(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)
- NOAA4000 – 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 way the system operates to achieve the purpose(s) identified in Section 4

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)
- Physical Characteristics

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

eDiscovery Application: The eDiscovery Platform system is a web-based application used to simplify agency response to Freedom of Information Act (FOIA) requests, aid in the processing Administrative Records (AR), and to a lesser extent, Congressional Inquiries.

(e) 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.

(f) 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.

(g) Any information sharing conducted 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

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

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.

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

Strandings information including reporter's contact 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 Bergartt, 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)

eDiscovery Application: The eDiscovery Platform system is a web-based application used to simplify agency response to Freedom of Information Act (FOIA) requests, aid in the processing Administrative Records (AR), and to a lesser extent, Congressional Inquiries.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Personnel/Contracting:

- 5 U.S.C. 1301.

Permitting:

- 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.

Stranding:

- The Marine Mammal Protection Act
- The Endangered Species Act
- Fur Seal Act.

Other:

- Freedom of Information Act, 5 U.S.C. 552; Privacy Act of 1974 as amended, 5 U.S.C. 552a; 5 U.S.C. 301, and 44 U.S.C. 3101.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531- 332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
- 42 U.S.C. 3211; 31 U.S.C. 240; 28 U.S.C. 533-535 and 1346(b); 15 U.S.C. 277 and 278e(b); E.O. 10450; E.O. 11478, as amended and all other authorities of the Department.
- E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

NOAA4700 is a FIPS 199 **Moderate** impact system.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

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.
- 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 01-2017).
- 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 01-2019 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. (Check all that apply.)

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	X
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X**
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify): 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					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, 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.

**Financial transactions are for cost recovery in catch share programs. Cost recovery is a means by which NMFS recovers administrative costs, by charging a set percentage of the ex-vessel value each year. The ex-vessel value is the post-season adjusted price per pound for the first purchase of commercial harvest. Certain items under "Other Information" are components of ex-vessel value.

For permit fees, checks may be submitted by mail to AKR, per regulation.

- AKR electronically scans the checks into an OTCnet (Treasury) application.
- OTCnet processes the payment.
- OTCnet returns a report to AKR that the check has been processed, including bank and account numbers, but without names.

After matching the check to OTCnet report, AKR shreds the check and deletes the report, both on paper and electronically.

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X***
b. Maiden Name		i. Place of Birth		p. Medical Information	X
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	X
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, spouse, former spouse, and descendent. *** Refers to the transaction and accounts boxes checked in Identifying Numbers.					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	x
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	x
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify): Other work-related data (specify): Cell phone or other alternate work/contact number, name of manager/supervisor, vessel name, vessel length overall, name of corporation, state and date of incorporation of business and articles of incorporation. This data is required to perform the personnel actions required by the Federal Govt such as: 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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	x
b. Palm Prints		g. Hair Color	x	l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color	x	m. DNA Sample or Profile	
d. Video Recording		i. Height	x	n. Retina/Iris Scans	
e. Photographs	X*	j. Weight	x	o. Dental Profile	
p. Other distinguishing features/biometrics (specify): *Required to be submitted with permit applications					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
Fishing locations and methods. Catch information to include species, aggregate catch data and statistics, quota share balance, quota pound balance, quota pound limits, listings of endorsements and designations (i.e., gear endorsement, size endorsement, sector endorsement, permit tier) associated with the permit, name of physical IFQ landing site, exemptions (i.e., owner on board - grandfathered exemption, owner on board, as stated in Code of Federal Regulations) and exemption status, contact persons, catch/observer discard data, quota share/quota pound transfer data, business operation information (business processes, procedures, physical maps).

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					

Other (specify):

2.3 Describe how the accuracy of the information in the system is ensured.

Accuracy in the NOAA4700 system is maintained using NIST 800-53 controls. By limiting who can change and submit the data the reliability and integrity of the information system is ensured. NOAA4700 utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise service application for audit log management. eDiscovery collects data directly from Google Vault extraction in order to retain the parent-child relationship in email threads.

2.4 Is the information covered by the Paperwork Reduction Act?

X	<p>Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.</p> <p>0648-0206, -0213, -0269, - 0272, -0316, -0318, -0334, -0353, -0393, -0401, -0428, -0445, -0512, -0513, -0514, -0515, -0516, -0545, -0564, -0575, -0592, -0665, -0678, -0699, -0700,- 0711, -0330, -0518, -0565, -0633, -0759, -0766, -0786, and -0792.</p>
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (Check all that apply.)

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X | There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. (Check all that apply.)

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

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

<p>Personnel/Contracting: PII information is collected for both contractor and federal employee personnel designated to work with AKR. This is information collected for several administrative and business functions for the AKR:</p> <ul style="list-style-type: none"> ● 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 <p>Permitting: This information will allow NMFS to identify owners and holders of permits and non-permit registrations and vessel owners and operators for both civil and criminal enforcement activities, evaluate permit applications, and document agency actions relating to</p>

the issuance, renewal, transfer, revocation, suspension or modification of a permit or registration. NMFS may use lists of permit holders or registrants as sample frames for the conduct of surveys to collect information necessary to the administration of the applicable statutes (see NOAA-19 SORN).

NMFS may post non-sensitive permit holder, vessel-related, and/or IFQ information for the public, via Web sites and Web Services, per notice given on permit applications. This information is considered to be part of the public domain.

Strandings: Stranded animals may provide information on geographical distribution, feeding habits, reproduction, age distribution, diseases, parasites, and contaminant levels. If strandings are reported quickly, the network also may facilitate the rapid identification of mass mortalities or strandings caused by disease or toxicity/pollution problems. By conducting necropsies on dead stranded animals, it is also possible to learn more about the basic physiology and biology of animals not accessible in the wild or by any other means. Necropsies also have provided data on the incidence of human interactions including ship strikes, shootings, entanglements, and marine debris ingestions. These data help NMFS to make better management decisions about these stocks of marine mammals.

Without authorization from NMFS, the public cannot pick up stranded marine mammals. However, assistance in documenting the incident is helpful and will allow stranding network members to respond. The most important information to collect is the date, location of stranding (including latitude and longitude), number of animals and species, if known

eDiscovery Application: The information is used in the review process and redacted before it is released to the requestor. The application does not actually save the data; it only save the metadata or pointers to the scanned document

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

NOAA4700 limits the threats to privacy by limiting access to the content and encrypting the PII in electronic form. Insider threat is a possibility that is mitigated by requiring that all users receive yearly training that highlights proper handling of PII. Commonly used forms list PII items such as Social Security Number with "On File" vs the actual SSN to prevent the document from being classified as PII. Forms printed with PII material produce a banner indicating that the material is PII. Files are stored both electronically and on paper in stored cabinets.

NOAA4700 utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise service application for audit log management.

There is a risk of inadvertent disclosure of PII/BII through FOIA releases, but employees are provided training throughout the year to reduce the likelihood of disclosure.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X
DOC bureaus	X		
Federal agencies	X*		
State, local, tribal gov't agencies	X	X	X
Public		X	
Private sector	X		
Foreign governments			
Foreign entities			
Other (specify):			

*For privacy breach, security investigations and CAC

The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

x	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA4000, Network encryption NOAA4020, Science and Technology, Network encryption NOAA4600, NOAA Seattle Local Area Network, Network encryption NOAA4800, Alaska Fisheries Science Center (AKFSC) Network
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. (Check all that apply.)

Class of Users			
General Public	X	Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.nmfs.noaa.gov/aboutus/privacy.html	
X	Yes, notice is provided by other means.	Specify how: Permitting: Notice is provided on the permit or related application. Personnel/contracting: Federal Employees/Contractors voluntarily submits this data as part of the hiring process or the hiring process cannot be properly conducted. Once the applicant is hired, and the paperwork is completed (OF-306 etc), copies of these on-boarding documents are provided to the new employee on day one at the new workstation. He/she is instructed to retain these for their own records in a fire-proof safe at his/her own residence. This is the same process followed NOAA-wide. eDiscovery Application: The information is redacted as part of the FOIA review process. This is not the original submission of the information
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Personnel/Contracting: Federal employees and contractors may decline to provide PII/BII in writing to their respective supervisor and contracting officer's
---	---	--

		<p>representative, however, doing so may affect the status of employment and contract.</p> <p>Permitting: The personal information is collected when the individual completes the appropriate application. On the application, the individual is advised that NMFS will not be able to issue a permit if the individual does not provide each item of information requested. The individual may choose to decline to provide the required personal information at that time, by not completing the application, but will not be able to receive a permit.</p> <p>Strandings: Individuals may decline to submit strandings reports, by not submitting them.</p> <p>eDiscovery Application: The BII/PII is collected via email as part of conducting business. This is not the original submission of the data.</p>
	<p>No, individuals do not have an opportunity to decline to provide PII/BII.</p>	<p>Specify why not:</p>

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<p>X</p>	<p>Yes, individuals have an opportunity to consent to particular uses of their PII/BII.</p>	<p>Specify how:</p> <p>Personnel/Contracting: Employees and Users are provided with the link to NOAA’s privacy policy where it states: “Submitting voluntary information constitutes your consent to the use of the information for the stated purpose”.</p> <p>Permitting: Permittees are provided with the link to NOAA’s privacy policy where it states: “Submitting voluntary information constitutes your consent to the use of the information for the stated purpose”.</p> <p>Strandings: Strandings reporters are provided with the link to NOAA’s privacy policy where it states: “Submitting voluntary information constitutes your consent to the use of the information for the stated purpose”.</p> <p>eDiscovery Application: The BII/PII is collected via email as part of conducting business. This is not the original submission of the data</p>
	<p>No, individuals do not have an opportunity to consent to particular uses of their PII/BII.</p>	<p>Specify why not:</p>

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Personnel/Contracting: Individuals may update PII/BII upon written request to Chief, Operations and Management Division, Alaska Region, NOAA Fisheries. Permitting: Information may be reviewed or updated when completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time: 978-282-8438 (information is on permits and permit applications). Strandings: Individuals may update PII/BII upon written request to Chief, Protected Resources Division.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access to PII in the database is tracked by logging the Oracle database according to DISA baselines.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>8/4/20</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The potential risk of inappropriate disclosure and/or unauthorized disclosure is mitigated by limiting the number of authorized system users. Providing initial and

annual system security training, monitoring authorized user activity, automatic and immediate notification of unauthorized system access or usage to the system administrator, documenting user violations, and gradually increasing user reprimands for system violations ranging from a verbal warning with refresher security training to denial of system access. Our permitting data is encrypted at rest and our backup tapes are encrypted.

The information is secured via both administrative and technological controls. PII and BII are stored on shared drives that require common access card (CAC) for access. The principle of least privileged and separation of duties is implemented by AKR to ensure that only personnel with the need to know have access to this information.

All NMFS personnel and contractors are instructed on the confidential nature of this information. Through acknowledgement of the NOAA rules of behavior, account request agreements etc. all users are instructed to abide by all statutory and regulatory data confidentiality requirements, and will only release the data to authorized users.

Buildings employ security systems with locks and access limits. Only those that have the need to know, to carry out the official duties of their job, have access to the data. Computerized data base is password protected, and access is limited. Paper records are maintained in secured file cabinets in areas that are accessible only to authorized personnel of NOAA4700.

eDiscovery is encrypted at rest and in transit (through the use of Kiteworks) before ingest into Clearwell.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

Yes, the PII/BII is searchable by a personal identifier.

No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> Security or Privacy Breach: COMMERCE/DEPT-13 , , Investigation and Security Information Personnel/Contracting: The existing Privacy Act System of records for DEPT-18 Employees Personnel
---	---

Files Not Covered by Notices of Agencies. Permitting: COMMERCE/NOAA-19 , Permits and Registrations for United States Federally Regulated Fisheries. Strandings: Information is not retrieved by individual name or identifying number. eDiscovery Application: COMMERCE/DEPT-5 , Freedom of Information Act and Privacy Act Request Records COMMERCE/DEPT-14 , Litigation, Claims, and Administrative Proceeding Records COMMERCE/DEPT-25, Access Control and Identity Management System OPM/GOVT-1, General Personnel Records
Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: (Personnel Files) and Chapter 1500: 1505-11, 1507-11, and 1514-01
<input type="checkbox"/>	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	<input checked="" type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
--

X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level.
(Check all that apply.)

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: For permitting, the AKR maintains a significant quantity of sensitive PII.
X	Data Field Sensitivity	Provide explanation: The AKR maintains sensitive PII, especially Social Security numbers and tax identification numbers
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: Permits data confidentiality is authorized by the Magnuson-Stevens Fishery Conservation and Management Act.
X	Access to and Location of PII	Provide explanation: Sensitive data is encrypted at rest and access is also restricted.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There are no obvious threats to privacy that exist from the sources or type of information collected. Alaska Region collects the minimum amount of sensitive information that is required to complete the mission.

NOAA4700 utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise service application for audit log management

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.