Template Version Number: 01-2020

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

Privacy Impact Assessment
for the
NOAA4500
West Coast Region (WCR) Network

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

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2021.08.02 08:33:51 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NMFS/NOAA4500

Unique Project Identifier: NOAA4500

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 West Coast Region (WCR) of NOAA Fisheries is a General support system.

(b) System location

Seattle, WA Portland, OR Santa Rosa, CA Sacramento, CA Arcata, CA Long Beach, CA Boise, ID Santa Rosa, CA

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

The Information System is interconnected with the NMFS Enterprise Wide Area Network (NOAA4000)

(d) The way the system operates to achieve the purpose(s) identified in Section 4

To achieve this mission and advance sound stewardship of these resources, we work closely with tribes, local, state and federal agencies, our stakeholders, and partners to find science-based solutions to complex ecological issues.

(e) How information in the system is retrieved by the user

Authorizations and Permits for Protected Species (APPS) The web based system contains applications for permits required by the Marine Mammal

Protection Act (MMPA) and the Endangered Species Act (ESA). Researchers use the system to submit an application which contain PII (employment and education information) prior to receiving a scientific research permit. Information collected is not shared outside of NOAA4500. NOAA Fisheries protects PII stored in APPS by minimizing the use and collection of PII. NOAA Fisheries also protects PII stored in APPS by controlling access to the information. APPS requires users to authenticate their identity by entering a username and password.

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 and Legal Holds. The system serves as a single point for the collection, review, tagging, redaction and export of responsive records. The Information System protects PII stored in the eDiscovery Application by minimizing the use and collection of PII. The Information System also protects PII stored in APPS by controlling access to the information. No SSNs or financial information is stored. The eDiscovery Application requires users to authenticate their identity by entering a username and password.

(f) How information is transmitted to and from the system

NOAA4500 System Maintenance Information and COOP PII:

NOAA4500 utilizes Data Resource Accounts and Group Memberships to allow authorized staff to access NOAA4500 Data which may contain PII or BII. Computer account types include, but are not limited to, Domain Accounts, Email/LDAP Accounts, Unix Accounts, Intranet Accounts, and Local System Accounts. Group memberships are used to assign Security Access Levels to authorized Data Resource Accounts. NOAA4500 applies Least Privilege and Least Functionality principles when providing security clearance. Access Enforcement Mechanisms (Encryption-at-Rest, Encryption-in-Transit, Distributed Directory Services) are implemented to prevent malicious or accidental access by unauthorized persons.

NOAA4500 will be voluntarily collecting home addresses in order to create GIS maps of staff impacted in the event of a catastrophic situation. This information will be used for accountability as it relates to protection and safe being.

PII in the form of addresses, will be voluntarily collected from Employees, contractors, and affiliates working for the WCR. The information will be provided via a Google Apps for Government Google Form. Results of these surveys will be locked down to only authorized federal employees and will not be shared. The data is then exported to a .csv file to be stored on the GIS shared drives. The .csv is imported into ArcGIS online and a layer is created. Once supervisory personnel have been notified of affected staff, the layer is deleted. No layers will be saved.

(g) Any information sharing conducted by the system

NOAA4500 does not share any of the Federal or Contractor employee information provided.

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

The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq.

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.

The Electronic Signatures in Global and National Commerce Act, Public Law 106-229
Homeland Security Presidential Directive 12 and IRS Publication-1075
Equal Employment Act of 1972
Federal Preparedness Circular (FPC) 65, July 26, 1999;
Public Law 100-71, dated July 11, 1987.

Executive Orders 10450, 11478, 12065, 12107, 12564, 12656, 13164,

5 U.S.C. 301, 5379, and 7531-332
15 U.S.C. 277 and 278e(b)
15 U.S.C. 1501 et seq.;
28 U.S.C. 533-535 and 1346(b)
31 U.S.C. 240
35 U.S.C. 2
41 U.S.C. 433(d)
42 U.S.C. 3211
44 U.S.C. 3101

5 CFR Part 537

DAO 210-110

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

Moderate

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).

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 01-2019 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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): Addresses					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	x	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	x	q. Military Service	
d. Gender		k. Telephone Number	x	r. Criminal Record	
e. Age		l. Email Address	x	s. Physical Characteristics	
f. Race/Ethnicity		m. Education	x	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	x	e. Work Email Address	x	i. Business Associates	
b. Job Title	x	f. Salary		j. Proprietary or Business Information	X
c. Work Address	x	g. Work History	X*	k. Procurement/contracting records	
d. Work Telephone Number	x	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): *Researcher Resumes					

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

System Administration/Audit Data (SAAD)					
a. User ID	x	c. Date/Time of Access	x	e. ID Files Accessed	
b. IP Address	x*	f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): *IP Addresses are collected for anyone logging on to APPS with a user name and password. We do not collect this information if the person does not log in and is accessing only the publicly available sections of the application. IP addresses are collected for federal employees and staff when logging into NOAA4500 for administrative purposes.					

Other Information (specify)

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): *APPS: Physical copies of APPS Applications are provided in person and submitted via mail if digital access is not available to applicant. - - System Maintenance Information: COOP Information (Home Phone Number, Address, etc...)					

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

Non-government Sources					
Public Organizations	x	Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

The West Coast Region provides a process consistent with the statutory amendment process under 5 USC 552a(f)(4)for each application which collects sensitive information from individuals or business, to have inaccurate personally identifiable information (PII) or Business Identifiable Information (BII) maintained by the organization corrected or amended, as appropriate; If corrections are performed, the West Coast Region provides a process for each application to disseminate corrections or amendments in addition to notifying affected individuals that their information has been corrected or amended.

2.4 Is the information covered by the Paperwork Reduction Act?

x	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0648-0613, -0785, -0498, -0492, -0361, -0223, -0500, -0619, -0402, -0399, -0738, -0387, -0148
	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	
For administrative matters	x	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
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).

Authorizations and Permits for Protected Species (APPS)
The PII/BII collected by the IT system is from federal and state employees, members of the public, and employees/members of Tribal Nations. The information is used to verify that the individual has the necessary qualifications to conduct research on protected species. Applicants provide a curriculum vitae or resume documenting their academic and/or work related experience
with the methods and procedures they plan to use on protected species.

NOAA4500 System Maintenance Information and COOP PII
Federal and Contractor Employee data:
Names, addresses, and email addresses collected from employees and contractors are used to manage account information for access control to systems and web applications.
Names and work email addresses of employees and contractors are used to direct the public to appropriate personnel within the organization.
For emergency, disaster recovery, and continuity of operations, employee and contractor names,
work and home emails and work and home telephone numbers are collected.
---
eDiscovery Application
The information is stored in a NETAPPS filer in Portland, OR, in an unreadable .pst file. The .pst
file is linked to the eDiscovery application in which only authorized Federal Employees have access to. No SSNs or financial information is collected. The information is collected in response
to DOJ request to a specific FOIA event. Information is then reviewed and redacted for final review by DOJ. PII/BII is redacted from its original submission once it enters the eDiscovery Application.

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.)

The West Coast Region performs the following functions and tasks concerning the collection of Sensitive information:
• ensures that organizational business processes are in compliance with laws, regulations, policies, procedures, and standards for IT Security.
• ensures that all business processes are accurately documented and are provided to the

Information System Authorizing Official (AO).
• ensures that all data sharing is documented in a format required by the Authorizing Official.
• ensures that business processes align with an acceptable level of risk to operations, assets, or individuals as identified in all affected IT System Security Plans. Specifically, all changes must be documented and approved by the Authorizing Official.
• ensures that business processes do not circumvent security controls documented in System Security Plans.
• ensures that system users and support personnel receive the appropriate role based security training. This training can range from the basic security awareness training, (for users with limited access to sensitive information) to sophisticated technical training (for developers or users with administrative/root level access).
• ensures that the organization has a documented contingency plan to address scheduled and unscheduled outages that may have widespread or local impact.
• implements a risk and vulnerability management process that complies with DOC, NOAA, and Fisheries processes.
• ensures that all appropriate AOs, SOs and ISSOs are engaged during requirements phase and throughout any project that impacts and/or involves any changes to IT systems that support business processes.
• assumes responsibility for addressing the operational aspects of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements).
• documents business process specific and hybrid controls that are identified as either being wholly or partially within your organizational authority
• ensures documentation of identified security control implementation as appropriate in CSAM. This includes providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs.
• provides support for any system data call, security review, and/or audit.
• ensures that weaknesses, that are identified as either being wholly or partially within your organizational authority, have Plan of Action and Milestones (POA&M) to mitigate the weakness
• ensures that NOAA4500 Configuration Management processes are followed for all changes, including but not limited to:
    - installing or removing hardware or software including updates and patches
    - changes to operating systems and/or software configurations
    - networking changes

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		
DOC bureaus	x		
Federal agencies	x		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	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: NMFS Enterprise Wide Area Network (NOAA4000) - Network firewalls prevent undesired interconnectivity - Logical Access restricts access to NOAA4500 network to NOAA4500 only
	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		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: The Privacy Act statement for eDiscovery can be found at: https://www.veritas.com/content/dam/Veritas/docs/policies/Veritas_Complete_Online_Privacy_Statement-EN.pdf For Apps: https://apps.nmfs.noaa.gov/docs_cfm/privacy_statement.cfm For COOP PII: https://drive.google.com/file/d/1rO5eN4gDDvDrGqsUNfB4Qa0T6GwjNqJP/view?usp=sharing	
x	Yes, notice is provided by other means.	Specify how: Authorizations and Permits for Protected Species (APPS): Furnishing information is voluntary; however, failure to provide accurate information may delay or prevent review of applications. A physical copy of the PAS is provided to applicants when information is collected in person. NOAA4500 System Maintenance Information and COOP PII: Information collected for employee/contractor emergency contact, and disaster recovery/continuity of operations is requested in writing by the employee/contractor's supervisor. Information collected for account management is requested in writing or via email by the user's supervisor, at the time that the user requests an account on the information system. eDiscovery Application: The information is redacted as part of the FOIA review process. The user voluntarily submits the information; if not, the business cannot be conducted
	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: Authorizations and Permits for Protected Species (APPS): The Endangered Species Act and Marine Mammal Protection Act require the applicant provide evidence of their qualifications. The individual would decline to provide PII/BII by not submitting information on his/her qualifications, and thus the application would be denied. NOAA4500 System Maintenance Information and COOP PII: Employees may decline to provide PII /BII for emergency contact and disaster recovery by not filling in the PII/BII

		information. However, they will not be included in the contacts in case of emergency. Employees may decline to provide account information by not applying for an account, but this may be required for their job duties. eDiscovery Application: The BII/PII is collected via email as part of conducting business. Not providing the information affects the ability to conduct business.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

x	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Authorizations and Permits for Protected Species (APPS): When the applicant signs the permit applicant, he/she is consenting to the use of the PII/BII for the sole purpose of processing the application. NOAA4500 System Maintenance Information and COOP PII: https://connection.commerce.gov/sites/connection.commerce.gov/files/media/files/2019/final_doc_it_security_baseline_policy_6.24.19.pdf) Employees have the opportunity to consent to information use. Employee and contractor General Personal Data information is required for HSPD-12 and emergency notifications but users may decline in writing to their supervisors to provide COOP info. Employees and contractors are informed of the use of their data, and these data are not used for any other purpose. eDiscovery Application: The BII/PII is collected via email as part of conducting business.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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: Authorizations and Permits for Protected Species (APPS): Applicant information (e.g. address, phone, CV or resume) is automatically updated when profile information is updated via website. NOAA4500 System Maintenance Information: Instructions for updating contact information fields are provided in the forms the customer fills out. NOAA Employees can update PII for COOP and Emergency contact information on an as needed basis, by a written update/ request to their supervisors.

		eDiscovery Application: The BII/PII is collected via email as part of conducting business.
	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: ArcSight is used to monitor event logs
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): 09/28/2020 ☐ 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.
x	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).*

Authorizations and Permits for Protected Species (APPS)
NOAA Fisheries protects PII stored in APPS by minimizing the use and collection of PII. NOAA Fisheries also protects PII stored in APPS by controlling access to the information. APPS requires users to authenticate their identity by entering a username and password.

NOAA4500 System Maintenance Information and COOP PII:
NOAA4500 utilizes Data Resource Accounts and Group Memberships to allow authorized staff to access NOAA4500 Data which may contain PII or BII. Computer account types include, but are not limited to, Domain Accounts, Email/LDAP Accounts, Unix Accounts,

Intranet Accounts, and Local System Accounts. Group memberships are used to assign Security Access Levels to authorized Data Resource Accounts. NOAA4500 applies Least Privilege and Least Functionality principles when providing security clearance. Access Enforcement Mechanisms (Encryption-at- Rest, Encryption-in-Transit, Distributed Directory Services) are implemented to prevent malicious or accidental access by unauthorized persons.

eDiscovery Application:

The Information System protects PII stored in the eDiscovery Application by minimizing the use and collection of PII. The Information System also protects PII stored in APPS by controlling access to the information. The eDiscovery Application requires users to authenticate their identity by entering a username and password.

Section 9: Privacy Act

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

x 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. *(list all that apply)*: Authorizations and Permits for Protected Species (APPS): COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Exempted Applicants For civil or criminal actions: COMMERCE/DEPT-13, Investigative and Security Records NOAA4500 System Maintenance Information: Commerce/Department 18 - "Employees Personnel Files Not Covered by Notices of Other Agencies" eDiscovery Application: Commerce/DEPT-5, Freedom of Information Act and Privacy Act Request Records. COMMERCE/DEPT-14, Litigation, Claims, and Administrative Pro COMMERCE/DEPT-25, Access Control and Identity Management
	Yes, a SORN has been submitted to the Department for approval on (date).
	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.)*

x	There is an approved record control schedule. Provide the name of the record control schedule: Authorizations and Permits for Protected Species (APPS): - NOAA Records Schedule Chapter 1500 - Marine Fisheries, Section 1514-01. NOAA4500 System Maintenance Information: - NOAA Records Schedules 200-01: Office Administrative Files
	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:
x	Yes, retention is monitored for compliance to the schedule.
	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	x	Overwriting	x
Degaussing		Deleting	x
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.)*

x	**Low –** the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	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: The PII we collect does not include sensitive identifying numbers or Distinguishing Features/Biometrics – or any other sensitive PII or BII.
x	Data Field Sensitivity	Provide explanation: Much of the information we collect (e.g. name, address, phone number) is available through business and phone directories.

x	Context of Use	Provide explanation: The information is used by NMFS to verify that the individual has the necessary qualifications to conduct research on protected species.
x	Obligation to Protect Confidentiality	Provide explanation: The Endangered Species Act of 1973 and the Marine Mammal Protection Act of 1972
	Access to and Location of PII	Provide explanation:
	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.)

No Identified threats to privacy other than possible insider threat.

NOAA4500 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.