

**U.S. Department of Commerce  
NOAA**



**Privacy Impact Assessment  
for the  
West Coast Region Local Area Network  
NOAA4500**

Reviewed by: \_\_\_\_\_ Mark 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

**Catrina D. Purvis**

Digitally signed by Catrina D. Purvis  
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open  
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US  
Date: 2016.12.05 11:36:02 -05'00'

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

Date

## **U.S. Department of Commerce Privacy Impact Assessment West Coast Region Local Area Network (LAN), NOAA4500**

**Unique Project Identifier:** 006-48-01-14-02-3305-00

### **Introduction:**

#### **System Description**

NOAA Fisheries is dedicated to protecting and preserving our nation's living marine resources through scientific research, fisheries management, enforcement, and habitat conservation. The West Coast Region of NOAA Fisheries administers fisheries programs along the coasts of Washington, Oregon and California; and in the vast inland habitats of Washington, Oregon, California and Idaho. We work to conserve, protect, and manage salmon and marine mammals under the Endangered Species Act and Marine Mammal Protection Act, and sustainably manage West Coast fisheries as guided by the Magnuson-Stevens Fisheries Conservation Act. 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.

The NOAA4500 (West Coast Region [WCR] LAN) functions as the overall office automation support system for WCR, National Marine Fisheries Service (NMFS), National Oceanic Atmospheric Administration (NOAA) in multiple physical locations throughout the western United States.

The purpose of the NOAA4500 Information System is to provide access to automated systems typically found in administrative offices within the federal government. The Information System supports all offices within the WCR.

#### **Authorizations and Permits for Protected Species (APPS)**

The web based system contains applications for permits required by the Marine Mammal Protection Act and the Endangered Species Act. Researchers use the system to submit an application for a scientific research permit.

---

#### **NOAA4500 System Maintenance Information**

PII and BII information contained within the NOAA4500 system boundary provide the System Owner, ISSO, and administrators with the identity and contact information of all authorized users of the system. This information is used to reset passwords, notify users of outages, and support NOAA4500 COOP operations.

**Information Sharing:**

**Authorizations and Permits for Protected Species (APPS)**

Researchers may include a curriculum vitae or resume with their application. Information collected is not shared outside of NOAA4500.

In the event that the agency initiates an enforcement action against a permit holder, PII/BII may be used by the Department of Justice (DOJ in litigation and/or criminal law enforcement actions. In the event that a civil enforcement case is brought against a permit holder, the agency may share PII/BII with DOJ.

-----  
**NOAA4500 System Maintenance Information**

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

**Authorities:**

**Authorizations and Permits for Protected Species (APPS)**

The Endangered Species Act of 1973 and the Marine Mammal Protection Act of 1972, amended 1994, require us to validate the researcher’s qualifications for conducting research on protected species. Fishing permits under the Magnuson-Stevens Act are handled through a separate permit process.

-----  
**NOAA4500 System Maintenance Information**

5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

The Federal Information Processing Standard (FIPS) 199 security impact category for the system is 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.)*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>			
a. Conversions		d. Significant Merging	g. New Interagency Uses
b. Anonymous to Non-		e. New Public Access	h. Internal Flow or

Anonymous			Collection	
c. Significant System Management Changes		f. Commercial Sources	i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):				

X This is an existing information system in which changes do not create new privacy risks.

## **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.)*

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

<b>General Personal Data (GPD)</b>					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

<b>Work-Related Data (WRD)</b>					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X*
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

\*Researcher resumes

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	

c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

<b>System Administration/Audit Data (SAAD)</b>					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X*	d. 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.

<b>Other Information (specify)</b>

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

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

<b>Government Sources</b>					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify)					

<b>Non-government Sources</b>					
Public Organizations	X	Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</b>			
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.)*

<b>Activities</b>			
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.)*

<b>Purpose</b>			
To determine eligibility		For administering human resources programs	
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	
		For employee or customer satisfaction	
For web measurement and customization technologies (single-session )		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.

In the event that the agency initiates an enforcement action against a permit holder, PII/BII may be used by the Department of Justice (DOJ in litigation and/or criminal law enforcement actions. In the event that a civil enforcement case is brought against a permit holder, the agency may share PII/BII with DOJ.

-----  
**NOAA4500 System Maintenance Information**

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.

**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			
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			

Other (specify):			
*DOJ if a criminal case resulting from research activity			
The PII/BII in the system will not be shared.			

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

	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:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

<b>Class of Users</b>			
General Public		Government Employees	X
Contractors	X		
Other (specify): General public access is limited to the data fields that they complete in APPs.			

## **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: <a href="https://apps.nmfs.noaa.gov/docs_cfm/privacy_statement.cfm">https://apps.nmfs.noaa.gov/docs_cfm/privacy_statement.cfm</a>	
X	Yes, notice is provided by other means.	Specify how:  NOAA4500 System Maintenance Information: 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.
	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.	<p>Specify how:</p> <p>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..</p> <p>NOAA4500 System Maintenance Information: 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.</p> <p>Employees may decline to provide account information by not applying for an account, but this may be required for their job duties.</p>
	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.	<p>Specify how: 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.</p> <p>NOAA4500 System Maintenance Information: Where specified in NOAA WFMO forms (<a href="http://www.wfm.noaa.gov/forms/noaa_forms.html">http://www.wfm.noaa.gov/forms/noaa_forms.html</a>), employees have the opportunity to consent to particular use of their PII/BII. Employee and contractor General Personal Data information is required for badging 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.</p>
	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	Specify how:
---	---	--------------

them.	<p>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.</p> <p>NOAA4500 System Maintenance Information: Instructions for updating contact information fields are provided in the forms the customer fills out.</p> <p>NOAA Employees can update PII for COOP and Emergency contact information on an as needed basis, by a written update/request to their supervisors.</p>
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: NOAA4500 locations where PII/BII is present are monitored for successful and failed logons. Database activity is audited, stored locally and reported to the NOAA Security Operations Center (SOC).
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ___ October 13, 2016 ___ <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 and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM). The privacy controls assessment submitted with this PIA has been reviewed by the BCPO.
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 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.

**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:**

NOAA4500 utilizes Data Resource Accounts and Group Memberships 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.

**Section 9: Privacy Act**

- 9.1 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	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i>:</p> <p>Authorizations and Permits for Protected Species (APPS): Commerce/NOAA-12</p> <ul style="list-style-type: none"> <li>- COMMERCE/NOAA-12, Marine Mammals, Endangered and Threatened Species, Permits and Exempted Applicants <a href="http://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/noaa-12.html">http://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/noaa-12.html</a></li> </ul> <p>NOAA4500 System Maintenance Information:</p> <ul style="list-style-type: none"> <li>- Commerce/Department 18 - "Employees Personnel Files Not Covered by Notices of Other Agencies"</li> <li>- Commerce/Department 25 – "Access Control and Identity Management System"</li> </ul>
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

**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	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p> <p>Authorizations and Permits for Protected Species (APPS):</p> <ul style="list-style-type: none"> <li>- NOAA Records Schedule Chapter 1500 - Marine Fisheries, Section 1514-01. Available at <a href="http://www.corporateservices.noaa.gov/audit/records_management/schedules/">http://www.corporateservices.noaa.gov/audit/records_management/schedules/</a></li> </ul> <p>NOAA4500 System Maintenance Information:</p> <ul style="list-style-type: none"> <li>- GRS 1: Civilian Personnel Records,</li> <li>- GRS 3.1 General Technology Management Records, Item 040: Information technology oversight and compliance records,</li> <li>- GRS 3.2 Information Systems Security Record, Items 030, 031: System access records,</li> <li>- NOAA Records Schedules 1406-01: In Situ and Remotely Sensed Environmental Data; 1406-02, Order Processing Information Systems, 1406-03, Metadata Management Database</li> </ul>
	<p>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:</p>
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.)*

<b>Disposal</b>			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

### **Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels**

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.

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 levels.  
*(Check all that apply.)*

Identifiability	Provide explanation:
-----------------	----------------------

X	Quantity of PII	Provide explanation: The PII we collect <u>does not</u> 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 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.

12.2 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.