

U.S. Department of Commerce NOAA



Privacy Impact Assessment for the

Southeast Fisheries Science Center (SEFSC) NOAA4400

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: 2017.08.11 16:02:35 -04'00'

8/3/2017

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

Date

U.S. Department of Commerce Privacy Impact Assessment

NOAA4400 - Southeast Fisheries Science Center (SEFSC) Network

Unique Project Identifier: NOAA4400

Introduction: System Description

The Southeast Fisheries Science Center (SEFSC) conducts multi-disciplinary research programs to provide management information to support national and regional programs of NOAA's National Marine Fisheries Service (NMFS) and to respond to the needs of Regional Fishery Management Councils, Interstate and International Fishery Commission, Fishery Development Foundations, government agencies, and the general public.

The SEFSC is headquartered in Miami, FL. The SEFSC is responsible for scientific research on living marine resources that occupy marine and estuarine habits of the continental southeastern United States, as well as Puerto Rico and the U.S. Virgin Islands. The SEFSC is one of the six national marine fishery science centers responsible for federal marine fishery research programs.

The Science: In general, SEFSC develops the scientific information required for:

- Fishery resource conservation
- Fishery development and utilization
- Habitat conservation
- Protection of marine mammals and endangered marine species

The Research: Impact analyses and environmental assessments for management plans and international negotiations are also prepared, and research is pursued to address specific needs in:

- Population dynamics
- Fishery biology
- Fishery economics
- Engineering and gear development
- Protected species biology

The following comprises all PII and BII in the system: NOAA4400 has a Fisheries Logbook System (FLS) which collects vessel and captain's names, numbers of each species caught, the numbers of animals retained or discarded alive or discarded dead, the location of the set, the types and size of gear, the duration of the set, port of departure and return, unloading dealer and location, number of sets, number of crew, date of departure and landing, and an estimate of the fishing time.

The legal authorities for collection of information addressed in this PIA are:

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

Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq (MSA) authorizes the collection of logbook information.

In addition, from DEPT-13: Executive Orders 10450, 11478, 12065, 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

NOAA4400 shares information only within the bureau, with the exception of the Department of Justice as needed regarding law enforcement.

This 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.

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*		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:

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

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

Distinguishing Features/Biometrics (DFB)			
a. Fingerprints		d. Photographs	
b. Palm Prints		e. Scars, Marks, Tattoos	
c. Voice Recording/Signatures		f. Vascular Scan	
g. DNA Profiles			
h. Retina/Iris Scans			
i. Dental Profile			
j. Other distinguishing features/biometrics (specify):			

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input checked="" type="checkbox"/>
g. Other system administration/audit data (specify):					

Other Information (specify): NOAA4400 has a Fisheries Logbook System (FLS) which collects vessel and captains' names, numbers of each species caught, the numbers of animals retained or discarded alive or discarded dead, the location of the set, the types and size of gear, the duration of the set, port of departure and return, unloading dealer and location, number of sets, number of crew, date of departure and landing, and an estimate of the fishing time.

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		Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify)					

Non-government Sources					
Public Organizations		Private Sector	<input checked="" type="checkbox"/>	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.)*

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

<input checked="" type="checkbox"/>	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):					

<input checked="" type="checkbox"/>	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			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		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)		For web measurement and customization technologies (multi-session)	
Other (specify): BII is collected for regulatory requirements with respect to fisheries regulations per MSA.			

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).

NOAA4400 collects PII (captain's name) and BII from logbooks for the purposes of regulating the applicable fisheries.

This information is maintained locally within NOAA4400 system and is used only for research and regulatory purposes. This information is collected from members of the public and shared only within the bureau.

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):			

*Law enforcement and Department of Justice

	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.*)

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: https://www.sefsc.noaa.gov/fisheries/logbook.htm .	
X	Yes, notice is provided by other means.	Specify how: Notice is given on letters to permit holders explaining permit-related responsibilities.
	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: Fishermen may decline to provide PII/BII, by not completing their logbooks, but this information is required under the MSA and also is needed to maintain their permits.
	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: The only uses of the logbook information are research and regulatory purposes. Consent to these uses is implied by completion of the logbook.
	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: Fishermen may contact NOAA4400 offices (the contact information is on the logbook forms) and ask to review their own logbook data.
	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: Monitoring is performed by using an encrypted oracle warehouse application that keeps the record of all logins. Only authorized users have access to confidential data.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 11/17/2016 <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. NOAA4400 has been categorized as MODERATE.

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).
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.
	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.

<p>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.</p> <p>Logbook data, when entered, is stored on our Oracle Database server. This system uses the native database authentication for user access. The only way to read data on the Oracle Database is to have access by authenticating with a username and password.</p> <p>The information is secured via both administrative and technological controls. BII is stored on shared drives that require CAC for access. The principle of least privilege and separation of duties is implemented by SEFSC to ensure that only personnel with the need to know have access to this information.</p> <p>All NOAA4400 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.</p> <p>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 NOAA4400.</p>
--

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	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> :
----------	---

	COMMERCE/NOAA-6 , Fisheries Statistical Data DEPT-13 , Investigative and Security Records
	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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1500: 1505-11 and 1507-11
	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.
	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		Deleting	
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.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	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: Minimal PII in logbooks, i.e. Captain's name
X	Data Field Sensitivity	Provide explanation: Fishing location information.
X	Context of Use	Provide explanation: Information collected is for granted system accounts which include business information to support NMFS's mission.
X	Obligation to Protect Confidentiality	Provide explanation: MSA Section 402b.
X	Access to and Location of PII	Provide explanation: Restricted access.
	Other:	Provide explanation:

Section 12: Analysis

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

X	Yes, the conduct of this PIA results in required business process changes. Explanation: There is now a Privacy Act Statement on the logbook web site.
	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.