Version Number: 01-2017

U.S. Department of Commerce
NOAA Fisheries

Privacy Impact Assessment (PIA)
for the
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

for Dr. Catrina D. Purvis LISA MARTIN Digitally signed by LISA MARTIN Date: 2020.04.14 21:14:00 -04'00' 02/26/2020
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA Fisheries

Unique Project Identifier: NOAA4400

Introduction: System Description and Purpose

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 Southeast Fisheries Science Center (SEFSC) is headquartered in Miami, FL. and interconnects with NOAA4000; NOAA4020; NOAA4200, and NOAA4300. These NMFS interconnections all connect via the NMFS WAN and are primarily used for database connections to provide data to NMFS science centers and regional offices. The data being shared amongst these systems consists of aggregated fishery and marine life data and does not include PII or BII. Authorized personnel use this data for research purposes, and they access this data following access controls put in place by each system following the guidelines of the current NIST IT Security standard. 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 and conservation
Fishery development and utilization
Habitat conservation
Protection of marine mammals and endangered marine Species

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.

According to FIPS 199, NOAA4400 is classified as a Moderate Impact System. NOAA4400 is a General Support System (GSS) providing infrastructure as well as application support for internal systems and data to external NMFS systems. NOAA4400 has a major application component within its systems, The Log Book System along with its database and applications which support a major program within the SEFSC.

Southeast Coastal Fisheries Logbook Trip reporting is required under and is authorized under 50 CFR 622.5 (a)(1). The Highly Migratory Species Logbook Trip reporting is mandatory for the purpose of managing HMS fisheries in accordance with the Atlantic Tunas Convention Act (16 U.S.C. 971 et. seq.) and the Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 1801 et. seq.)

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8). The E-Government Act of 2002 also determines the legal authorities for the collection of the data.

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.

__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.

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: NOAA4400 collect Vessel ID/Documentation # in order to trace information back to the required permit.					

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

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates	X		

i. Other work-related data (specify): NOAA4400 collect the job title of individual completing the logbook.

Distinguishing Features/Biometrics (DFB)					
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):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
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	X	Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
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.

Multiple conditions have been implemented, system wide, to restrict user from selecting incorrect options, including database field and values, and in addition, after the data is collected and validated, numerous QAQC reports are ran to confirm the data accuracy. Access to the system is granted base on specific roles and very few users have the ability to access the whole system. Logs for every single operation, (no exceptions), are generated, collected, and kept indefinitely, which allows the reconstruction and analysis of any event that might happen at a particular point. Operation logs are generated with time and location.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. The OMB control number and the agency number for the collection is EDC Control No. 0648-0016, 0648-0371
	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	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):			

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, other DOC bureaus, and other federal agencies on a case by case basis. The OMB forms used for data collection are:

- ATLANTIC HIGHLY MIGRATORY SPECIES LOGBOOK TRIP SUMMARY FORM: 0648-0371
- ATLANTIC HIGHLY MIGRATORY SPECIES LOGBOOK - SET FORM: 0648-0371
- NO FISHING REPORTING FORM: 0648-0016
- SE COASTAL FISHERIES TRIP REPORT FORM: 0648-0016
- SUPPLEMENTAL DISCARD AND GEAR INTERACTION TRIP REPORT FORM: 0648-0016

5.2 Describe any potential threats to privacy 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.)

All personnel that work with The Logbook Data are trained annually to help reduce the risk and minimize the impact of an authorized user intentionally or unintentionally disclosing data, and causing adverse impact to sensitive data and mission. The Logbook data is collected on paper and submitted by the fishermen via U.S. mail. Some logbooks are submitted via fax. When received, logbooks are scanned and loaded into a database, validated and corrected by data entry personnel at SEFSC. The application is for internal use only, intranet access only, and has username/password authentication.

In terms of data access, only the following personnel have access: (a) 4 System Administrators/Developers; (b) 24 NOAA Data users; (c) 76 users have access to the Logbook images: NOAA Officials, including Southeast Regional Office, OLE, NE HMS, SA & GOM Council. To access the data, all personnel have a signed NDA. Logbook data is permanently retained.

All data is encrypted at rest, ~~use,~~ and during transit and is handled by the Database Administrator in an Oracle System. Considering the measures in place, unauthorized access is not likely. More information about access to the data is given in Section 8.2 as well.

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 is not and 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	This IT system connects to NOAA4000, NOAA4020, NOAA4200, and NOAA4300 but

	does not 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	Specify how: The only uses of the logbook information are research and regulatory purposes.

	particular uses of their PII/BII.	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): **07/03/2019** ☐ 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 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 supporting 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 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.

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.

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.

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.

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 database 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.

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, number, and link. *(list all that apply)*: SORN numbers: NOAA-6 and NOAA-19 https://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/noaa-6.html https://www.corporateservices.noaa.gov/audit/privacy_act/systems-of-records/noaa-19-copy.html
	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.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
X	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: No Retention Schedule has been written by the National Archive. NOAA4400 have been in contact with the National Archive in attempts to get a Retention Schedule created for the Southeast Logbook Reports.
X	Yes, retention is monitored for compliance to the schedule. This retention that we marked as YES, is related to the Logbook Data that we kept in a secure manner, permanently, in the Oracle System.

	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	
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 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 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 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.)

	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 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.