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

Privacy Impact Assessment
for the
NOAA4400 (SEFSC)

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 PrivacyOfficer

Jennifer Goode 1/19/2022

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA4400 – Southeast Fisheries Science Center

Unique Project Identifier: NOAA4400

<u>Introduction</u>: System Description

The Southeast Fisheries Science Center (SEFSC) is a general support system that 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 provides the scientific advice and data needed to effectively manage the living marine resources of the Southeast region and Atlantic high seas. We work closely with NOAA Fisheries Southeast Regional Office to provide independent, objective science.

Our multidisciplinary research informs natural resource management. Fisheries management councils, fisheries commissions, and federal, state and local agencies depend on our science to make decisions that protect and conserve the region’s living marine resources.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

The Southeast Fisheries Science Center (SEFSC – FISMA NOAA4400) is a general support system

(b) System location

The Southeast Fisheries Science Center (SEFSC) is headquartered in Miami, FL

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

The Southeast Fisheries Science Center (SEFSC) is headquartered in Miami, FL and interconnects with Atlantic Coastal Cooperative Statistics Program (ACCSP); NOAA4000; NOAA4020; NOAA4200, and NOAA4300. The 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; and as per the connection with ACCSP, all data is encrypted using the oracle native encryption (sqlnet.ora), and TLS. If the VPN works, we have an
encrypted connection plus a VPN, and in case the VPN does not work, we still protected by

using our existing encrypted connection.

The data being shared amongst these systems consists of aggregated fishery and marine life data; and minimum PII and BII needed to maintain the system operation. 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.

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

PII/BII in the IT system is being collected, maintained, or disseminated for (a) administrative matters, (b) civil enforcement activities, and (c) criminal law enforcement activities if needed.

NOAA4400 does not collect SSNs or EINs; however, the organization gathers some minimum PII as captain's names, addresses, and phone numbers, and this information is used for processes such as (d) compliance - ensuring logbooks are submitted as required; (e) mailing (logbooks, permits, etc.); (f) uses mailing address of record; (g) providing HMS regulations and species guides to Atlantic Tournaments; and (h) for online no-fish electronic reporting - account creation and mailing.

The integration of drones (UAS) into SEFSC Protected Resources and Biodiversity Division operations allow for additional information to be gathered during operations, including aerial photo-identification and dorsal photography that allow for assessments of individual organism growth, health, body condition, and reproductive status and provide more accurate estimates of group sizes and group membership.

NOAA4400 could also utilize UAS to locate and assess stranded animals in areas difficult to access. Outside of the protected resources applications, regular or opportunistic UAS deployments could also be used to identify and, if coupled with acoustic data, determine the three-dimensional extent and density of schooling pelagic fishes (e.g., menhadens, tunas), which could ultimately be utilized to estimate the biomass. UAS could also be utilized to support additional projects yielding data on the marine environment, including on critical habitats and seawater chemistry, to name a few.

UAS: As outlined in DEPT-29, the use of UAS has the potential for inadvertent collection of PII, such as images of individuals along the coastlines that are within the area of study by the UAS vehicle. However, no information retrieval using any unique identifier within Survey datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. NOAA4400 does not use any application capable of facial recognition within any captured images. It is anticipated that the UAS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to identify any individuals uniquely.

If the drone goes down during flight, the retrieval of the unit would be at the operator's discretion based on safety and technical factors. Inadvertently obtained PII captured during the flight could be retrieved by others if technically possible from the damaged drone. NOAA4400 closely collaborate with OCS, and OCS is compliant with all policies and procedures posted on the UAS.noaa.gov site along with the NOAA Unmanned Aircraft System Privacy Policy.

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

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. NOAA4400 collect the job title of individual completing the logbook, and their telephone numbers as well.

The user retrieves information in the system after following multiple conditions that have been implemented, system-wide, to restrict the user from selecting incorrect options, including database fields and values. In addition, after the data is collected and validated, numerous Quality Assurance Quality Control (QAQC) reports are run to confirm the data's accuracy.

The specific ways a user can retrieve the information are through SQL, SAS, R, Oracle, and APEX queries. Access to the systems requires special permissions, and the data is encrypted at rest.

Access to the system is granted based on specific roles and very few users can access the whole system.

Logs for every operation (no exceptions) are generated, collected, and kept indefinitely, allowing the reconstruction and analysis of any event that might happen at a particular point.

Operation logs are generated with time and location.

Atlantic Coastal Cooperative Statistics Program (ACCSP) pulls data using an encrypted sqlnet connection over a dynamic virtual private network (VPN) to NOAA Head Quarters (4000). Data are retrieved by the authenticated end-users and state fisheries administrators through the ACCSP Warehouse. Federal agencies who have an Interconnect Security Agreement may retrieve the data from the ACCSP Warehouse or Standard Atlantic Fisheries Information System (SAFIS) databases, follow agreed-upon secure data transfer protocols, and provide access to their users through their local data delivery processes appropriate.

All internal data and resources are retrieved using Government Furnished Equipment (GFE) through approved applications to open, review, verify, and securely delete information. Internal resources are secured through defense-in-depth with layered security such as physical access, firewalls, active directory, access controls, permission, etc.).

Internal Common Access Card (CAC) authenticated users can utilize (based on permissions) data stored in PDF, Files, and databases through networked client's devices and NOAA VPN service for remote access. NOAA4400 uses Google services for email and collaboration services.

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

All data is encrypted at rest and during transit and is handled by the Database Administrator in an Oracle System. The information is secured via both administrative and technological controls. Business Identifiable Information (BII) is stored on shared drives that require Common Access Card (CAC) for access. Southeast Fisheries Science Center (SEFSC) implements the principle of least privilege and separation of duties to ensure that only personnel with the need to know to have access to this information.

Logbook data, when entered, is stored on our Oracle Database server. This system uses native database authentication for user access. The only way to read data on the Oracle Database is to have access by authenticating it with a username and password.

A 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.

ACCSP pulls data using an encrypted sqlnet connection over a dynamic virtual private network (VPN) to NOAA HQ (4000). Data is passed through FIPS 140-2 approved encryption mechanisms (SQLNET AES256 encrypted sessions) if networks are interconnected. When the information is transmitted to and from the ACCSP*,* ACCSP pulls data using an encrypted sqlnet connection over a dynamic VPN to NOAA Head Quarters (4000). The connections at each end must be located within controlled access facilities and protected 24 hours a day. Individual users will not have access to the data except through their system's security software inherent to the operating system.

(g) Any information sharing

The Southeast Fisheries Science Center (SEFSC) is headquartered in Miami, FL, and interconnects with ACCSP; NOAA4000; NOAA4020; NOAA4200, and NOAA4300. The 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, and as per the connection with ACCSP, all data is encrypted using the oracle native encryption (sqlnet.ora), and TLS. If the VPN works, we have an encrypted connection plus a VPN, and in case the VPN does not work, we are still protected by using our existing encrypted connection.

The SEFSC is responsible for scientific research on living marine resources that occupy marine and estuarine habits of the continental southeastern United States, 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. NOAA4400 intends to share the collected PII/BII with (a) within the bureau, (b) with DOC bureaus, and (c) with other federal agencies as needed.

As per the connection with ACCSP, data are passed through FIPS 140-2 approved encryption mechanisms (SQLNET AES256 encrypted sessions) if networks are interconnected. When the information is transmitted to and from the ACCSP, ACCSP pulls data using an encrypted sqlnet connection over a dynamic VPN to NOAA HQ (4000). The connections at each end must be located within controlled access facilities and protected 24 hours a day. Individual users will not have access to the data except through their system's security software inherent to the operating system.

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

Southeast Coastal Fisheries Logbook Trip reporting is required under and is authorized under 50 C.F.R. 622.5 (a)(1). The Highly Migratory Species Logbook Trip reporting is mandatory for the purpose of managing H.M.S. 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.)

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

According to FIPS 199, NOAA4400 is classified as a Moderate Impact System, providing infrastructure and application support for internal systems and data to external NMFS systems.

<u>Section 1</u>: Status of the Information System

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

_____ This is a new information system.

_X___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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	

j. Other changes that create new privacy risks (specify):

NOAA4400 have a relatively new interconnection with ACCSP. Through this association commercial dealer, as well as permit-based commercial and for-hire fishermen data is collected by ACCSP and exchanged with NOAA4400. Individual fishermen trip data, dealer report data, and permit data are shared between SEFSC and ACCSP. The permit data does not include PII.

Also, NOAA4400 is now collecting fisherman trip and landing statistics to meet a federal mandate under the Magnuson-Stevens Act to collect and report recreational and commercial fisheries data. There are no other ways to operate without this collection. The collected data is accessed by ACCSP Staff, SEFSC Staff, and ACCSP partners with individual user confidential access approved by SEFSC staff. Confidential named user access is for a set period and is automatically revoked at the expiration date.

The integration of drones (UAS) into SEFSC Protected Resources and Biodiversity Division operations allow for additional information to be gathered during operations, including aerial photo-identification and dorsal photography that allow for assessments of individual organism growth, health, body condition, and reproductive status and provide more accurate estimates of group sizes and group membership.

____ 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.

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):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: NOAA4400 collects vessel ID/Documentation # in order to trace information back to the required permit.					

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		q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Telephone number is collected as another means of contact.					

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

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	X	i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify): It is anticipated that the UAS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to identify any individuals uniquely.					

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

Other Information (specify)

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.

Fisherman trip and landing statistics are now being collected as well.

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	X	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 a user from selecting incorrect options, including database fields and values, and in addition, after the data is collected and validated, numerous QAQC reports are run to confirm the data accuracy.

The system's access is granted based on specific roles, and very few users can access the whole system.

Logs for every 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. Provide the OMB control number and the agency number for the collection. The OMB control numbers are 0648-0670, 0648-0013, 0648-0543, 0648-0371, 0648-0247, 0648-0151, 0648-0591, 0648-0016, 0648-0542, 0648-0631, 0648-0770.
	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): UAS is now being used.			

	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	X	Electronic purchase transactions	
Other (specify): NOAA4400 makes use of UAS and has the potential for inadvertent collection of PII. However, no information retrieval using any unique identifier within Survey datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. NOAA4400 does not use any application capable of facial recognition within any captured images. It is anticipated that the UAS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to identify any individuals uniquely.			
	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, ordisseminated. *(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 the 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

NOAA4400 makes use of UAS and has the potential for inadvertent collection of PII. However, no information retrieval using any unique identifier within Survey datasets will be conducted, and any PII inadvertently collected will be deleted within 30 days. NOAA4400 does not use any application capable of facial recognition within any captured images. It is anticipated that the UAS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to identify any individuals uniquely.

·

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.)

All personnel that works 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 effect 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, 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 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.

Any PII collected by UAS is incidental, unintentional, and not retained. It is anticipated that the UAS collected imagery will be at a resolution to meet organizational needs, but it would not have the ability (resolution or clarity) to identify any individuals uniquely.

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 *	X		X
Public			
Private sector			
Foreign governments			
Foreign entities			

Other (specify):			

* The Atlantic States Marine Fisheries Commission is where ACCSP / ACFIN is located. As an interstate Commission created by Congress – they are between a federal government and state/local government designation.

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

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

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

6.3 Indicate whether the IT system connects with or receives information from any otherIT 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: This IT system connects to ACCSP; NOAA4000, NOAA4020, NOAA4200, and NOAA4300 but does not receive information from another IT system(s) authorized to process PII and/or BII.
	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): Contract system developers working for ACCSP have access to the PII/BII collected.			

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.fisheries.noaa.gov/national/fisheries-observers/privacy-act-statement .	
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: Fishers 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: Fishers may contact NOAA4400 offices (the contact information is on the logbook forms) and ask to review their 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:** The minimum PII and BII the system collects have the same protection that the Database server, and all information related to both components is encrypted.
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): **11/16/2021** ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

The potential risk of inappropriate disclosure and/or unauthorized disclosure is mitigated by limiting the number of authorized system users, providing initial and annual system security training, monitoring authorized user activity, automatic and immediate notification of unauthorized system access or usage to the system administrator, documenting user violations, and gradually increasing user reprimands for system violations ranging from a verbal warning with refresher security training to denial of system access.

Logbook data, when entered, is stored on our Oracle Database server. This system uses native database authentication and encryption for user access. The only way to read data on the Oracle Database is to have access by authenticating it 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. SEFSC implements the principle of least privilege and separation of duties to ensure that only personnel with the need to know to have access to this information.

All NOAA4400 personnel and contractors are instructed on the confidential nature of this information. By acknowledging the NOAA rules of behavior, account request agreements, etc., all users are recommended to abide by all statutory and regulatory data confidentiality requirements and 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. A computerized database is password- protected, and access is limited. Paper records are maintained in secured file cabinets in areas accessible only to authorized personnel of NOAA4400.

Section 9: Privacy Act

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

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)*: NOAA-6 SYSTEM NAME: "Fishermen's Statistical Data." https://www.osec.doc.gov/opog/PrivacyAct/SORNs/noaa-6.html NOAA-19 SYSTEM NAME: "Permits and Registrations for United States Federally Regulated Fisheries."
	https://www.osec.doc.gov/opog/PrivacyAct/SORNs/noaa-19.html COMMERCE/DEPT-29 SYSTEM NAME: "Unmanned Aircraft Systems." https://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-29.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: NOAA4400 does not enforce a records retention schedule. It is on our list of things to do, but this is not going to happen immediately.
X	Yes, retention is monitored for compliance to the schedule. This retention that we marked as YES relates to the Logbook Data that we kept securely and 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):			

<u>Section 11</u>: 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 <u>Confidentiality Impact Level is not the same, and does not have to be the same, as the</u> Federal Information Processing Standards (FIPS) 199 security impact category.)*

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

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

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: The quantity is minimal. NOAA4400 does not collect SSNs or EINs; however, the organization gathers some minimum PII as captain's names, addresses, and phone numbers.
X	Data Field Sensitivity	Provide explanation: Sensitive PII such as SSN and sensitive BII for fishermen is not collected by NOAA4400, neither sensitive data for business.

X	Context of Use	Provide explanation: Permits information and fishers business data is stored securely as described in Sections 8.1 and 8.2. Administrative and Technological Controls are in place to protect the minimum PII/BII the system collects.
X	Obligation to Protect Confidentiality	Provide explanation: The Magnuson-Stevens Act authorizes confidentiality of fisheries data.
X	Access to and Location of PII	Provide explanation: System is not publicly accessible. Access to PII/BII is controlled through access control lists, separation of duties, and enforcement of least privilege access. We also limit the number of authorized system users, providing initial and annual system security training, monitoring authorized user activity; through an 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.
	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, the conduct of this PIA does not result in any required business process changes. Other than the accidental release of confidential information, no other threats have been identified. NOAA4400 exclusively gathers what the councils decide we need to collect to support management, and this is minimum PII/BII such as business name and address for mailing. This information is stored in an Oracle Database and requires a username/password for access. Backups are encrypted. All online entries (i.e., web applications) are reviewed to mitigate any security threats and have passed security scanning (i.e., Apex SERT).

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.