

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



Privacy Impact Assessment
for the
NOAA4200
Northeast Fisheries Science Center (NEFSC)

Reviewed by: Mark H. Graff, Bureau Chief Privacy Officer

- ☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- ☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

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

Date

**U.S. Department of Commerce Privacy Impact Assessment
NOAA/NEFSC/NOAA4200**

Unique Project Identifier: NOAA4200

Introduction: System Description

Provide a brief description of the information system.

The primary mission of the Northeast Fisheries Science Center (NEFSC) is to provide multidisciplinary scientific and technical information to the Greater Atlantic Regional Field Office (GARFO) of NOAA Fisheries, other NOAA line offices, co-managers, stakeholders and other constituents to inform decision and policy-making processes. The NEFSC Network is used to provide information technology support to all federal employees, contractors and volunteers. A volunteer is subject to the same security clearance requirements as an employee or contractor. Volunteers would assist with rudimentary tasks, such as stuffing envelopes for fish age structure collection or serving as an unpaid student intern for fieldwork experience for a short period of time. The network provides access to essential NOAA services such as email, the Internet, shared printer, copiers, plotters, software applications and files. Information and data that are processed, analyzed and summarized include environmental, biological, chemical, technical, contact and procurement documentation and other administrative data that scientists, managers and administrators use to support the NMFS mission related research and management programmatic decision processes. The network provides a mechanism to monitor and store facility's external camera systems and also serves as a repository for data such as network access forms that contain information for center personnel that includes, but is not limited to signatures.

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

NOAA4200 is a General Support system (GSS).

(b) System location

NOAA4200 supports local area network infrastructure in:
Woods Hole, MA
Narragansett, RI
Milford, CT
Highlands, NJ
Orono, ME

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

NOAA4200 has established inter-connect service agreements with:

- *NOAA0100 - NOAA Cyber Security Center (H)
- NOAA4000 - NMFS Wide Area Network (WAN)
- NOAA4100 - Greater Atlantic Regional Fisheries Office (GARFO)
- NOAA4400 - Southeast Fisheries Science Center (SEFSC)
- NOAA4600 - Northwest Fisheries Science Center (NWFSC)
- AFCIN - Atlantic Coastal Cooperative Statistics Program (ACCSP)

*NOAA0100 - NOAA Cyber Security Center (H) - Used for security monitoring of the NOAA4200 Information System. This is not a new interconnection, it was just recently documented by NOAA0100. This does not create any privacy posture changes to NOAA4200.

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

The network provides access to essential NOAA services such as email, the Internet, shared printer, copiers, plotters, software applications and files. Information and data that are processed, analyzed and summarized include environmental, biological, chemical, technical, and other administrative data that scientists, managers and administrators use to support the NMFS mission related research and management programmatic decision processes. Information and data that are processed, analyzed and summarized include environmental, biological, chemical, technical, contact and procurement documentation and other administrative data that scientists, managers and administrators use to support the NMFS mission related research and management programmatic decision processes.

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

Users access the data using NOAA4200 GSS. NOAA4200 personnel utilize Government Furnished Equipment (GFE) to access network resources. Two factor authentication is implemented for access to system resources. System access occurs from within the system boundary and via the NOAA4000 VPN appliance. Information can only be accessed by permitted NOAA personnel. The system provides current, relevant information to support science-based stewardship of natural resources. The primary mission of the NEFSC is to provide multidisciplinary scientific and technical information to the Greater Atlantic Regional Office (GARFO) of NOAA Fisheries, other NOAA line offices, co-managers, stakeholders and other constituents to inform decision and policy-making processes. Connections with ACCSP are to pull data from ACCSP to NOAA4200. This is a one-way connection via the NOAA4000 managed VPN tunnel.

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

The network provides access to essential NOAA services such as email, the Internet, shared printer, copiers, plotters, software applications and files. Information and data that are processed, analyzed and summarized include environmental, biological, chemical, technical, and other administrative data that scientists, managers and administrators use to support the NMFS mission related research and management programmatic decision processes. Information is also shared via internal and external system NMFS interconnections. These connections occur through encrypted My Structured Query Language (SQL) sessions or Secure Shell (SSH) sessions established between entities. These processes can be manual or automated through the use of scripting service accounts. Information

and data that are processed, analyzed and summarized include environmental, biological, chemical, technical, contact and procurement documentation and other administrative data that scientists, managers and administrators use to support the NMFS mission related research and management programmatic decision processes.

(g) Any information sharing conducted by the system

The system provides current, relevant information to support science-based stewardship of natural resources. The primary mission of the NEFSC is to provide multidisciplinary scientific and technical information to GARFO of NOAA Fisheries, other NOAA line offices, co-managers, stakeholders and other constituents to inform decision and policy-making processes. Connections with ACCSP are to pull data from ACCSP to NOAA4200. This is a one-way connection via the NOAA4000 managed VPN tunnel.

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

1.	Public Health Emergency Info & Reasonable Accommodation	COMMERCE/DEPT-31	Rehabilitation Act, 29 U.S.C. 701 et. seq Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d) 29 CFR parts 1602, 1630, 1904, 1910, and 1960 29 USC chapter 15 (e.g., 29 U.S.C. 668) Executive Order 12196 5 U.S.C. 7902
2.	Building Entry/Access & Surveillance and System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301 Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors Electronic Signatures in Global and National Commerce Act, Public Law 106-229 28 U.S.C. 533-535
3.	Collection & Use of SSN	COMMERCE/DEPT-18	44 U.S.C. 3101 Executive Order 12107
4.	Visitor Logs & Permits for Facilities	COMMERCE/DEPT-6	5 U.S.C. 301 44 U.S.C. 3101
5.	Fishermen's Statistical Data	NOAA-6	Fish and Wildlife Act as amended (16 U.S.C. 742 et seq.) Fishery Conservation and Management Act of 1976

			as amended (16 U.S.C. 1852)
6.	NOAA Health Services Questionnaire (NHSQ) and Tuberculosis Screening Document (TSD)	NOAA-22	National Marine Sanctuaries Act. 16 U.S.C. 1440)
			Office of Personnel Management regulations: 5 CFR 339.102—Purpose and Effect
			5 CFR 339.202—Medical Standards
			5 CFR 339.205—Medical Evaluation Programs
			5 CFR 339.206—Disqualification on the Basis of Medical History
			5 CFR 229.301—Authority to Require an Examination
			5 CFR part 339—Medical Qualification Determinations
7.	NMFS Observers	NOAA-15	Magnuson-Stevens Fishery Conservation and Management Act, as amended, Public Law 109-479 16 U.S.C. 1853
8.	Fisheries Permits & Registrations	NOAA-19	Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq.
			High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 et seq.
			International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters, 50 CFR 300.120
			American Fisheries Act, Title II, Public Law No. 105-277
			Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101-5108, as amended 1996
			Tuna Conventions Act of 1950, 16 U.S.C. 951-961
			Atlantic Tunas Convention Authorization Act, 16 U.S.C., Chapter 16A
			Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 et seq.
			Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431-2444
			Western and Central Pacific Fisheries Convention Implementation Act, 16 U.S.C. 6901 et seq.
			Dolphin Protection Consumer Information Act, 16 U.S.C. 1385
			Marine Mammal Protection Act, 16 U.S.C. 1361 et seq
			Commerce, Justice, Science and Related Agencies Act, 2018, Division B, Section 539 (Pub. L. 115-141)
			Taxpayer Identifying Number, 31 U.S.C. 7701

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

NOAA4200 is categorized as Moderate.

Section 1: Status of the Information System

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

☐ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks.
(Check all that apply.)

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

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*	x	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport	x	k. Financial Transaction	
c. Employer ID		h. Alien Registration	x	l. Vehicle Identifier	x
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): Other identifying numbers (specify): Vessel federal and/or state fishing permit number; vessel ID (US Coast Guard (USCG) or state registration); Dealer federal and/or state permit number; Fishing trip identifier.					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: NOAA4200 collects and maintains OF 306, SF-85, SF-86, SF-50, SF-52 forms as this is a requirement for Federal Employment.					

General Personal Data (GPD)					
a. Name	x	h. Date of Birth	x	o. Financial Information	x
b. Maiden Name	x	i. Place of Birth	x	p. Medical Information	x*
c. Alias	x	j. Home Address	x	q. Military Service	x
d. Sex	x	k. Telephone Number	x	r. Criminal Record	x
e. Age		l. Email Address	x	s. Marital Status	
f. Race/Ethnicity		m. Education	x	t. Mother's Maiden Name	
g. Citizenship	x	n. Religion			
u. Other general personal data (specify): *The NOAA Health Services Questionnaire and TB Screening form collect information to determine if an individual is fit for a trip on a research vessel. The only other medical information that might be collected would be for an injury, i.e. filing a Worker's Compensation report.					

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	x
b. Palm Prints		g. Hair Color	x	l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color	x	m. DNA Sample or Profile	
d. Video Recording	x	i. Height	x	n. Retina/Iris Scans	
e. Photographs	x*	j. Weight	x	o. Dental Profile	
p. Other distinguishing features/biometrics (specify): *Likeness and profile release forms are on file with NOAA4200.					

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) Other data collected includes electronic vessel logbook data and dealer reports. Data elements reported include catch, effort, and value data.

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

Directly from Individual about Whom the Information Pertains					
In Person	x	Hard Copy: Mail/Fax	x	Online	x
Telephone	x	Email	x		

Other (specify): Administrative personnel who handle paper documentation follow the Social Security Number Fraud Prevention Act (SSNFPA).

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

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

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

Federal employees, contractors and volunteers provide their own information directly. NOAA4200 utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise service application for audit log management. All data/validation is completed at the statistical and or scientific level.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0648-0803 3206-0182 3206-0261 3206-0005 0648-0824
	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	x	Building entry readers	x
Video surveillance	x	Electronic purchase transactions	
Other (specify): Building entry readers are required to maintain secure physical access to federal facilities and video surveillance is required to record activities for security reasons, occurring on the grounds of federal facilities. Notices are posted on all buildings which notify that security cameras are in use.			

	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	x
For administrative matters	x	To promote information sharing initiatives	x
For litigation	x	For criminal law enforcement activities	x
For civil enforcement activities	x	For intelligence activities	
To improve Federal services online	x	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	x	For web measurement and customization technologies (multi-session)	
Other (specify): To aid the fishing industry to meet federal regulatory requirements for reporting.			

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).

For administrative matters: Work-Related Data is required to determine eligibility for access to federal buildings and information technology (IT) resources. Resumes, which contain work history, may be included on employee profile websites. The posting of employee profiles is voluntary. Information is collected from federal employees, contractors and volunteers. Identifying Numbers: Vehicle identifiers are used to match to parking decals which are placed on the vehicle of each person to authorize parking at the federal facility. The parking decal may be a sticker or a temporary parking pass. The license plate number is collected so the parking pass or decal can be linked to the proper vehicle. This information is required of all persons parking at the federal facility, i.e. federal employees, contractors, volunteers, and all visitors.
--

General Personal Data: Name, Home Address, Home telephone number, and Personal Email Address are required for telework agreements, emergency contact forms, and emergency notification systems. Medical data is required to determine eligibility to participate on research cruises as a member of the scientific party. General personal data is required for employees if they have a telework agreement. Personal data for emergency notification systems are required for federal employees, contractors, and volunteers. Medical information is collected from federal employees, contractors and visitors if requesting to participate in research cruises. NOAA4200 provides compensating security controls to protect sensitive data to include Social Security numbers. These controls include SC-08 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection, SC-28 Protection of Information at Rest, Homeland Security Presidential Directive (HSPD) 12, and the use of Kiteworks to safely transmit sensitive data.

Distinguishing Features/Biometrics: Building entry readers are required to maintain secure physical access to federal facilities and video surveillance is required to record activities, for security reasons, occurring on the grounds of federal facilities. Notices are posted on all buildings which notify that security cameras are in use. Likeness and profile release forms are on file with NOAA4200.

System Administration/Audit Data (SAAD) is required to monitor, maintain and report IT security related activities on NOAA4200. This information is collected from federal employees and contractors.

For civil and criminal enforcement activities and litigation:

Identifying numbers on data collected from the fishing industry are shared (securely) with other intra-agency users such as the GARFO and the NMFS Office of Law Enforcement (OLE) who are required to use the data to regulate the fishing activities. The vessel and dealer ID numbers allow these data to be matched to each other and to other data sets collected by observers and OLE, such as VMS data. The Observer data are reviewed for quality and assurance by the NOAA4200 Fishery Monitoring and Research Division (FMRD) Training and Data Quality (TDQ) Branch personnel. The interconnect agreements for the NOAA4200 provide the details on information sharing with other offices in NMFS. This information is collected from members of the public.

To aid the fishing industry to meet federal regulatory requirements for reporting:

Identifying numbers: Vessel federal and/or state fishing permit number; Dealer federal and/or state permit number; Fishing trip identifier; vessel registration numbers: The identifiers are required to be on commercial fisheries statistics data collected or reported by the fishing industry so these data can be associated with the proper entity. This information is collected from members of the public. Access to legal guidance and regulations are provided on or through the NEFSC public web servers. Members of the public and employees, contractors, and volunteers are provided the laws and regulations under which these data are required or needed; i.e. 50 CFR 648 and 697. NOAA regulations for work related data and employee rights are posted on <https://www.fisheries.noaa.gov/topic/laws-policies> and are available to all employees.

- 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.)

Privacy data is subject to the same level of information security as system specific, in this case fisheries. Therefore, all applicable controls such as AC, AU, MP, and PE families are enforced for the system components and software that store, process, and transmit PII. Least privilege is the default policy in NOAA4200 and is implemented through file share permissions and access control lists to ensure privacy and open only to those demonstrating a "need to know."

NOAA's use of the information would still be subject to any insider threats, as individuals with authorizations and need-to-know will have access to the PII within the system. All individuals must complete the mandated NOAA IT Security awareness training. Additionally, as a separate standalone system, damage or corruption of the system or its data could result in the loss of PII or NOAA's ability to use the system. NOAA's privacy controls, including the controls referenced above and in particular the access controls, significantly mitigate the risk of either of these threats.

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

*Maine Department of Marine Resource (Maine DMR), Mid-Atlantic Fisheries Management Council (MAFMC), Rhode Island Department of Environmental Management (RI DEM), Massachusetts Division of Marine Fisheries, New England Fisheries Management Council, ACCSP. **Volunteers with limited access.

☐	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 other IT systems authorized to process PII and/or BII.

x	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: The following list of controls are applicable per NOAA4200 Continuous Monitoring: AP-01 Authority to Collect AP-03 Purpose Specification AR-01 Governance and Privacy Program AR-02 Privacy Impact and Risk Assessment AR-04 Privacy Monitoring and Auditing AR-06 Privacy Reporting NOAA4200 has established inter-connect service agreements with: NOAA0100 - NOAA Cyber Security Center (H) NOAA4000 - NMFS Wide Area Network (WAN) NOAA4100 - Greater Atlantic Regional Fisheries Office (GARFO) NOAA4400 - Southeast Fisheries Science Center (SEFSC) NOAA4600 - Northwest Fisheries Science Center (NWFSC) AFCIN - Atlantic Coastal Cooperative Statistics Program (ACCSP) *NOAA0100 - NOAA Cyber Security Center (H) - Used for security monitoring of the NOAA4200 Information System. This is not a new interconnection, it was just recently documented by NOAA0100. This does not create any privacy posture changes to NOAA4200.
	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): Volunteers: Volunteers are not permitted access to PII/BII.			

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/privacy-policy

x	Yes, notice is provided by other means.	Specify how: Personnel/contracting: Federal employees/Contractors voluntarily submit this data as part of the hiring process for the hiring process cannot be properly conducted. Once the applicant is hired, and the paperwork is completed (OF-306) etc.), copies of these documents are provided to the new employee on day one of employment. The employee is then briefed that the forms will be retained on the NOAA4200 network and is available to them upon request. Privacy Act Statements for phone, mailings, and in person collections are provided the statement as identified here: https://www.noaa.gov/sites/default/files/legacy/document/2020/Apr/Grants_Online_Privacy_Act_Statement.pdf
	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: Individuals may decline to provide voluntary PII/BII, and also required information, although access to certain services and/or eligibility for employment may be affected. The refusal would be in writing to the office or the official requesting the information, such as a hiring specialist at workforce management. Prospective participants on research cruisers may decline to complete the NOAA Health Services Questionnaire and TB Screening Document, but then would not be able to participate. Fishermen would decline to provide PII/BII by not completing and submitting the fishing trip reports; however, they would then be out of compliance with their permit responsibilities.
	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: NOAA4200 employees have an opportunity to decline to consent to particular uses of their PII to their supervisors, in writing. If a request to collect PII is declined by an employee, then access to services may be limited or denied. By consenting to collection of PII, the employee is agreeing with the intended use. There is only one use for the medical information collected from prospective participants in research cruisers. Individuals consent to this use by signing the NOAA Health Services Questionnaire and Tuberculosis Screening Document. There is only one use for the trip report information. The reporting requirements are included in the letter accompanying
---	--	---

		the permit, explaining that vessel trip reporting is a requirement of the permit, and necessary for maintenance of the permit.
	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: Individuals may review/update PII/BII in the same manner in which it is originally reported. Individuals would need to contact the office to whom the PII/BII was provided and state the reason for review or update. If the reason is substantiated, the individual would update the information by submitting it in the same form as originally provided or granted secure access to make an update. Secure access requires a username and password and signed authorization for access to the system. The individual would only be authorized to update information they submitted. For example, if a vessel operator sends in a logbook and is later notified that there is an error, the operator is authorized to logon to the system and correct the data they submitted. All changes are logged so the agency will know what was changed, by whom and when it was changed. Medical information would be updated in the applicable forms if an individual was planning to go on another research group.
	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: Databases and servers containing PII/BII log successful and failed access attempts. Audit Logs are maintained locally and forwarded to the NOAA SOC ArcSight Loggers.
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): <u>2/7/2025</u> ☐ 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: 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 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.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

All system users are required to authenticate their logon session via 2-factor authentication. (Reference: NIST 800-53, Rev.4, IA-02, User Identification and Authentication, Organizational Users). User accounts that are dormant in excess of 90 days are automatically disabled. (Reference NIST 800-53, rev.4, AC-02, Account Management). Data is encrypted during transfer. Servers that house PII/BII information use secure connection protocols (ssh;). Backup disks are encrypted.

Section 9: Privacy Act

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

X Yes, the PII/BII is searchable by a personal identifier.

 No, the PII/BII is not searchable by a personal identifier.

- 9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

x	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> COMMERCE/DEPT-31 Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations COMMERCE/DEPT-25 Access Control and Identity Management Systems & Surveillance and System Administration/Audit Data (SAAD) COMMERCE/DEPT-18 Employees Information Not Covered by Other Notices of Other Agencies; COMMERCE/DEPT-6, Visitor Logs and Permits for Facilities Under Departmental Control; NOAA-6, Fishermen's Statistical Data; NOAA-22, NOAA Health Services Questionnaire and Tuberculosis Screening Document, NOAA-15, Monitoring of National Marine Fisheries Service Observers. NOAA-19 Permits and Registrations
---	--

	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Observer Databases: -1502-02 Survey Operations Files and -1513-10 Observer Program Files Economic Data Collection: -All records are retained and disposed of in accordance with National Archives and Records Administration regulations (36 CFR Subchapter XII, Chapter B-Records Management); -Departmental directives and comprehensive records schedules; NOAA Administrative Order 205-01; and the NMFS Records Disposition Schedule, Chapter 1500. Groundfish Permits: -NOAA 1504-11; NOAA 1514-01 NOAA4200 System Maintenance Information: -GRS 1: Civilian Personnel Records, -GRS 3.1 General Technology Management Records, Item 040: Information technology oversight and compliance records, -GRS 3.2 Information Systems Security Record, Items 030, 031: System access records, NOAA Records Schedules 1406-01: In Situ and Remotely Sensed Environmental Data; 1406-02, Order Processing Information Systems, 1406-03, Metadata Management Database For PII/BII, the relevant NOAA records control schedule are 1507-11 and 1507-15.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

- 11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	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.
X	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.)*

X	Identifiability	Provide explanation: Industry related data, not easy to identify individuals.
X	Quantity of PII	Provide explanation: All PII collected is done so with the scope minimized to only what data is required to perform the official function.
X	Data Field Sensitivity	Provide explanation: Fishing location information. Medical information (screening forms) and SSN's collected on OF306.
X	Context of Use	Provide explanation: All data is utilized for the sole purpose of its collection.
X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Act and HIPPA
X	Access to and Location of PII	Provide explanation: NOAA4200 is connected to ACCSP; the sharing of information is one-way only and ACCSP does not have access to NOAA4200.
	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.)

Potential threats that exist for information collected include insider mishandling of data and potential breach of network and exfiltration of private data. PII along with any sensitive data at NEFSC is accessed with a least privilege and rule-based access control model. Only approved individuals with a need to know will access the data. Information that is collected is the minimum amount required to support our mission. NOAA4000 utilizes enterprise-wide services to aid in security monitoring, vulnerability scanning, and secure baseline management. The system also uses a NOAA enterprise service application for audit log management.

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

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Kevin Portanova Office: NOAA/NMFS/NEFSC Phone: 508-495-4758 Email: Kevin.Portanova@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed: _____	Information Technology Security Officer Name: Catherine Amores Office: NOAA/NMFS Phone: 301-427-8871 Email: Catherine.Amores@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed: _____
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: _____ Date signed: _____	Authorizing Official Name: Nicole Cabana Office: NOAA/NMFS/NEFSC Phone: 508-495-2279 Email: Nicole.Cabana@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed: _____
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: _____ Date signed: _____	Empty space for additional comments or signatures

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.