Version Number: 01-2015

U.S. Department of Commerce
NOAA

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

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 DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=LISA MARTIN, 0.9.2342.19200300.100.1.1=13001000105292 Date: 2018.05.24 10:44:19 -04'00' 05/12/2018

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA4200 - Northeast Fisheries Science Center (NEFSC) Network

Unique Project Identifier: NOAA4200

Introduction: System Description

The Northeast Fisheries Science Center 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 field work 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, and other administrative data that scientists, managers and administrators use to support the NMFS mission related research and management programmatic decision processes.

The types of PII and BII that are collected and maintained are described below.

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, contactors 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 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.

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.

Technologies Used Containing PII/BII not Previously Deployed: 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.

For civil and criminal enforcement activities:
Identifying numbers on data collected from the fishing industry are shared (securely) with other intra-agency users such as the Greater Atlantic Regional Fisheries Office 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 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.csp.noaa.gov/policies/ and are available to all employees.

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

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

The Magnuson-Stevens Act, 16 U.S.C. 1801 et seq., authorizes the collection of information related to fisheries activities.

The Health Insurance Portability and Accountability Act, Pub. L. 104–191, 110 Stat. 1936, authorizes the collection of medical information for cruise eligibility.

The FIPS 199 impact level for this system is High.

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):

__X___ This is an existing information with no changes that create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

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

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	**X**	o. Medical Information	**X***
d. Gender		j. Telephone Number	**X**	p. Military Service	
e. Age		k. Email Address	**X**	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. 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**	d. Telephone Number	**X**	g. Salary	
b. Job Title	**X**	e. Email Address	**X**	h. Work History	**X**
c. Work Address	**X**	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	**X***	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)					

*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**	d. Queries Run	**X**	f. Contents of Files	**X**
g. Other system administration/audit data (specify): **Routine system audit logs of network activities for all users**					

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):					

Government Sources					
Within the Bureau	**X**	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal	**X***	Foreign			
Other (specify): *State/Federal Program: Atlantic States Coastal Cooperative Statistics 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 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	**X**
Video surveillance	**X**	Electronic purchase transactions	
Other (specify): All main entryways to NOAA4200 facilities have a placard present that indicates that video surveillance is being used a security method.			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	**X**	To promote information sharing initiatives	
For litigation	X	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): **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, contactors 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 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.

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.

Technologies Used Containing PII/BII not Previously Deployed: 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.

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 Greater Atlantic Regional Fisheries Office 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 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.csp.noaa.gov/policies/ and are available to all employees.

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

* 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

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

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

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: NOAA4000 - NMFS Wide Area Network (WAN) NOAA4011 - National Fishing Permit and Landing Reporting System (NFPLRS) NOAA4100 - Greater Atlantic Regional Fisheries Office (GARFO) NOAA4400 - Southeast Fisheries Science Center (SEFSC) WHOINet – a local high speed internet service provider for the Woods Hole LAN; internet traffic is redirected through a NOAA Trusted Internet Connection. WHOINet also provides support for the fiber backbone which connects the 5 office buildings. These buildings are distributed over a 7 mile radius. If any sensitive PII is transmitted, it is done so through Accellion.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public		Government Employees	**X**
Contractors (under federal employment)	**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: http://www.greateratlantic.fisheries.noaa.gov/aps/evtr/vtr_inst.pdf Page 4 .	
X	Yes, notice is provided by other means.	Specify how: DOC, NOAA and NMFS Web sites. See section 5.1 above, last paragraph.
	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 but 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	Specify how: NOAA4200 employees have an opportunity to decline to consent to particular uses of their PII to their

	PII/BII.	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 resubmitting 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: Access to PII requires a named account ID and DOC compliant password. Access is logged in audit logs. Paper documents are kept in locked cabinets. Only authorized personnel have keys,
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): _10/12/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
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 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.

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 are encrypted during transfer. Servers that house PII/BII information use secure connection protocols (ssh; sftp). Backup disks are encrypted.

Section 9: Privacy Act

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: DEPT-18, Employees Information Not Covered by Other Notices of Other Agencies; 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.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

Addendum: DEPT-18 covers all employee information not covered by the other SORNs listed here. DEPT-6 covers visitor logs in conjunction with the video surveillance system NOAA-6 covers Fisheries Logbooks/Vessel Trip Reports; NOAA-22 covers the medical examinations for participation in vessel research trips.

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. User level back-ups are performed on an hourly basis and stored locally on the network. Differential backups for system level servers are performed every night. Full backups for system level servers are also performed weekly.(Reference: NIST 800-53, Rev.4, CP-09 Information System Backup and CP-09(1) Information System Backup (Testing). For PII/BII, the relevant NOAA records control schedules are 1507-11 1507-15; All backups are retained on site for a minimum period of 2 years. Fisheries statistics data are not destroyed or deleted; therefore the current copy is year to date for a time series. Backups of the data and information are for contingency planning for the entire network and includes more than PII/BII content.
	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 Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse

	effect on organizational operations, organizational assets, or individuals.
	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 levels. *(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)
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 HIPAA.
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

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

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

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

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