

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



Privacy Impact Assessment
for the
NOAA4100
Greater Atlantic Regional Office (GARFO) 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

Tahira Murphy for Charles Cutshall 5/25/2023
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA/ NMFS/ Greater Atlantic Regional Office (GARFO) Network

Unique Project Identifier: NOAA4100

Introduction: System Description

The Greater Atlantic Regional Fisheries Office (GARFO) Local Area Network (LAN) Infrastructure (System NOAA4100) is one of the National Oceanic & Atmospheric Administration's (NOAA) general support systems (GSS). A GSS is an interconnected information resource under the same direct management control that shares common functionality. The computer systems within GARFO provide service to our ultimate end beneficiaries, the habitat, the fish, and the environment; and to the biologists, scientists, statisticians, and economists within the region and nation; and all fishers who depend on our data.

The GARFO network operates using BII/PII for the purpose of administrative matters, litigation, civil enforcement activities, web measurement and customization technologies (single-session), administering human resource programs, promoting information sharing initiatives, criminal law enforcement activities and in support of GARFO business functions.

Address the following elements:

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

The Greater Atlantic Regional Fisheries Office Local Area Network (LAN) Infrastructure (System NOAA4100) is one of the National Oceanic & Atmospheric Administration's (NOAA) general support systems (GSS). A GSS is an interconnected information resource under the same direct management control that shares common functionality. The computer systems within GARFO provide service to our ultimate end beneficiaries, the habitat, the fish, and the environment; and to the biologists, scientists, statisticians, and economists within the region and nation; and all fisheries who depend on our data.

(b) System location

GARFO Primary location is in Gloucester, Ma with several satellite offices in: Hampton, VA; Northfield, NJ; New Bedford, MA; Point Judith, RI; Portland, ME; Annapolis, MD; and Orono, ME.

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

The GARFO network maintains interconnection agreements with NMFS Headquarters in Silver Spring, MD

(NOAA4000), NOAA Web Operation Center (NOAA0201) and the NMFS Northeast Fisheries Science Center (NOAA4200).

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

Information on the GARFO network is retrieved through access controlled secure data applications and through secure database connections. All connections to the data have access control mechanisms in place and are encrypted.

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

Information retrieval on NOAA4100 is done securely in a variety of ways. The majority of access is through the Greater Atlantic Region's website. The information that is shared and collaborated with other organizations is done securely through hardwired interconnections and through the NOAA4000 controlled non-permanent VPN.

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

Information is transmitted to and from the system through secure encrypted channels

(g) Any information sharing

GARFO Employee PII is available only to the IT Staff and HR staff that is authorized to handle it, the IT Staff who handle this data is made up of both federal employees and contract. HR Staff is only federal.

Permit information is shared within NMFS offices in order to coordinate monitoring and management of sustainability of fisheries and protected resources. Sources of information include the permit applicant/holder, other NMFS offices, the U.S. Coast Guard, the Northeast Fishery Management Council (NEFMC) and the Mid-Atlantic Fishery Management Council (MAFMC).

Permits BII is shared with State Fish and Game. The information (data for issuing fishing permits and permit histories, catch data collected from fishing vessels, landings data collected from fish dealers, and effort or catch based allocation data) shared within NMFS and State Fish and Game is to support both our mission and theirs. The State *Department of Fish & Game* works to preserve the state's natural resources and people's right to conservation of those resources, as protected by Article 97 of the Massachusetts Constitution. This includes civil and criminal law enforcement. The Department exercises responsibility over the Commonwealth's marine and freshwater fisheries, wildlife species, plants, and natural communities, as well as the habitats that support them.

The information listed above is also shared with:

The Northeast Fisheries Sciences Center (NEFSC), since we share some fisheries management responsibilities in the same regional area, much of our data collection, data analysis, and data

dissemination roles either overlap or complement each other.

The Southeast Regional Office, as there is overlap in vessel activity with the Southeast Region, with vessels operating in both regions.

The Northeast Fishery Management Council (NEFMC) and the Mid-Atlantic Fishery Management Council (MAFMC) for the purpose of co-managing a fishery or for making determinations about eligibility for permits when state data are all or part of the basis for the permits. For purposes of data analysis. These Magnuson-Stevens Act (MSA) authorized fisheries management organizations have teams of analysts who use GARFO data to help drive fisheries management decision making.

The NEFMC and MAFMC and the North Atlantic Fisheries Organization for the purposes of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures.

The Office of Law Enforcement for purposes of civil and criminal investigation and enforcement.

The Atlantic Coastal Cooperative Statistics Program (ACCSP). ACCSP is a critical data management partner to GARFO. Currently they are the data collection point for all federally permitted dealers, and the future vision is to make them the warehouse for all east coast federal fisheries data. Data exchanges between GARFO and ACCSP have been integral to fisheries management for many years.

State fishery managers of the Atlantic Coastal States of Maine, Massachusetts, and Rhode Island, because there is overlap between state management and some federal fish activity reporting requirements.

USCG Reciprocal information (data for issuing fishing permits and permit histories, catch data collected from fishing vessels, landings data collected from fish dealers, and effort or catch based allocation data). USCG access to GARFO Data requires NDA for each individual accessing the data. We do not access any confidential data from the USCG.

Army Corps of Engineers for support of environmental assessment.

The public: Vessel Owner Name, Name of Vessel and Permit Number are made publically available through our website. Notice of this is given on the permit application. We also allow other regions, centers and state organizations access to the publically available information directly from our database through a secure connection. This information is considered part of the public domain.

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

Applications for permits and registrations are collected from individuals under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Atlantic Coastal Fisheries Cooperative Management Act, the Atlantic Tunas Convention Authorization Act, the Northern

Pacific Halibut Act, the Antarctic Marine Living Resources Convention Act, the Western and Central Pacific Fisheries Convention Implementation Act (WCPFCIA; 16 U.S.C. 6901 et seq.), international fisheries regulations regarding U.S. Vessels Fishing in Colombian Treaty Waters, the Marine Mammal Protection Act, the Endangered Species Act and the Fur Seal Act. The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.

For accounts receivable: 28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); and 31 U.S.C. 3711.

For investigative and security records: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records. In addition: E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

42 U.S.C. 3211; 31 U.S.C. 240; 28 U.S.C. 533-535 and 1346(b); 15 U.S.C. 277 and 278e(b)

35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; Homeland Security Presidential Directive 12 and IRS Publication-1075.

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

This is a FIPS 199 moderate impact system.

Section 1: Status of the Information System

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

_____ This is a new information system.

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	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): New Interconnection with NOAA0201 Web Operations Center					

_____ 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	X	j. Financial Account	X
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Tax Identification Numbers (SSNs or Employer ID Numbers) allow positive identification for cost recovery billing of IFQ holders. Also, as stated in COMMERCE/NOAA-19, a Tax Identification Number is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a Federal agency including, but not limited to, if the person is an applicant for, or recipient of, a Federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c) (2) (B) of this statute.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X
b. Maiden Name		i. Place of Birth		p. Medical Information	X

c. Alias		j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	X
f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder, spouse, former spouse, decedent.					

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			
l. Other work-related data (specify): Vessel name, vessel length overall. Name of corporation, state and date of incorporation of business and articles of incorporation.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X	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		i. Height	X	n. Retina/Iris Scans	
e. Photographs	X	j. Weight	X	o. Dental Profile	
p. Other distinguishing features/biometrics (specify): Medical records for permit disputes.					

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

Other Information (specify)
Species, aggregate catch data and statistics, quota share balance, quota pound balance, quota pound limits, listings of endorsements and designations (i.e., gear endorsement, size endorsement, sector endorsement, permit tier) associated with the permit, name of physical IFQ landing site, Exemptions (i.e., Owner on Board - Grandfathered Exemption, Owner on Board, as stated in code of federal regulations) and exemption status, contact persons, Catch/Observer Discard Data, Quota Share/Quota Pound Transfer Data, Business Operation Information (Business Processes, Procedures, Physical Maps).

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		Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	X	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.

Information accuracy in the system is ensured through ensuring the confidentiality of the data through access control mechanisms and integrity of that data through proper handling techniques and storage methods. The Analysis and Program Support Division (APSD) within GARFO verify data submitted by fishermen. This is to ensure both the fishermen and the dealers have reported accurately. APSD is made up of both Federal employees and Contractors. The Technology and Data Management Division (TDM) ensures accuracy of the data that is handled through programmatically restricted data entry points. Accuracy of the data entered by the public is done through a combination of the controls implemented by TDM and the verification of that data done by APSD.

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- 0202, -0212, -0229, -0350, -0351, -0491, -0546, -0605, -0240, -0364, -0470, -0496, -0590, -0673, -0674, -0679, -0774
	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 (TUCBPNPD)			
Smart Cards		Biometrics	

Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
---	--

Section 3: System Supported Activities

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			
X	There are not any IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	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		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): PII/BII are collected to support NOAA4100 business functions for NOAA employees and personnel with regard to onboarding and HR functions as well as setting up user accounts.			

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).

GARFO also collects and maintains PII for the following administrative support purposes:

1. For employment onboarding process and HR administration: Employee ID, Financial Account (for setting up direct deposit, not kept in system after forwarding to USDA), Date of Birth, Driver's License, Passport, Alias, Gender, Age, Race, Home Address, Military Service, Occupation, Job title, Work History, Salary, Performance Plans, Fingerprints and Photographs (both forwarded to DEERS and not retained).
2. For Establishing Employee IT system user accounts: Name, Office, Government phone number, email address, supervisor.

GARFO collects and maintains Tax ID Numbers, File/Case ID, Financial Account, Financial Transaction, Vessel Owner Name, Name of Vessel, Permit Number through a combination of sources including data from Permits and Dealer data through ACCSP which is a public organization.

1. Collected information is for reporting of trip data and catch landings.
2. Vessel Owner Name, Name of Vessel and Permit Number are made publically available through our website. We also allow other regions, centers and state organizations access to the publically available information directly from our database through a secure connection. This information will allow GARFO to identify owners and holders of permits and non-permit registrations and vessel owners and operators for both civil and criminal enforcement activities, evaluate permit applications, and document agency actions relating to the issuance, renewal, transfer, revocation, suspension or modification of a permit or registration. GARFO may use lists of permit holders or registrants as sample frames for the conduct of surveys to collect information necessary to the administration of the applicable statutes. GARFO may post non-sensitive permit holder, vessel-related, and/or IFQ information for the public, via Web sites and Web Services, per notice given on permit applications. This information is considered to be part of the public domain.
3. Tax Identification Numbers allow positive identification for cost recovery billing of IFQ holders. In addition, as stated in COMMERCE/NOAA-19, a Tax Identification Number is required on all permit applications other than research or exempted fishing permits, under the authority 31 U.S.C. 7701. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a Federal agency including, but not limited to, if the person is an applicant for, or recipient of, a Federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c) (2) (B) of this statute.
4. eDiscovery Application The information is used in the review process and is redacted before it is released to the requestor. The application does not actually save the data; it only saves the metadata or pointers to the scanned document.

- 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.)

Current potential threats to privacy as a result of GARFO's use of the information would come from improperly handled, retained or disposed data and malicious insider actions. These are mitigated through ensuring that employees complete the mandatory trainings which promote awareness and steps towards prevention. Non-Disclosure agreements, and user agreements which outline acceptable use and handling of information. Proper destruction of media and using form 37-45 to account for the destroyed media. Access controls applied to restrict the availability of physical systems, controlled spaces and data. This ensures only authorized personnel whose roles require access to the data will have it.

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

*Law Enforcement

**Public Web site

***ACCSP Bulk Aggregate Data – ACCSP does not receive PII but does receive aggregated data via direct access to the private sector.

	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: NOAA4200, Northeast Fisheries Science Center Network NOAA201 Web Operation Center and NOAA4000, Fisheries Wide Area Network and Enterprise Services. All channels between systems are encrypted. USCG: Access to information is done securely through encrypted web connection, NDAs are in place. State Agencies: Access to information is done securely encrypted through web connection, NDAs are in place. ACCSP: Connections are through a direct encrypted connection. Security controls are outlined in MOA/SLA with NOAA4000 has with ACCSP.
	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):			

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. The Privacy Act statement and notice of how PII/BII is used is available on the Greater Atlantic Region website, vessel and dealer permit applications. GARFO Website: https://www.fisheries.noaa.gov/privacy-policy Clearwell (Internal – however the webpage does have a PAS notifying individuals who login) https://nersclearwell1/esa/public/privacy_act_statement_v2.html **NOTE: NOAA4100 transitioned from accepting digital and paper Vessel and Dealer applications to being fully digital. This is why the links to the paper dealer and vessel applications was removed.

	NOAA Privacy Act Statement Authority: The collection of this information is authorized under 5 U.S.C. 552, the Freedom of Information Act (FOIA), which allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States government. Additional authorities: 15 C.F.R: Commerce and Foreign Trade, Part 4 - Disclosure of Government Information; Executive Order 13392, Improving Agency Disclosure of Information; Executive Memo, Memorandum on Transparency and Open Government; and NOAA Administrative Order (205-14). Purpose: NOAA collects the FOIA requestor's name and contact information as part of processing the FOIA request. In addition, contact information is collected from individuals working on a request, including administrators processing FOIA information for submission to FOIA Online, the Office of the General Counsel, the Department of Commerce, and to the Department of Justice if the FOIA case advances to litigation. Also included are administrators may also review materials for work on litigations and administrative records. Routine Uses: NOAA will use this information as part of reviewing and processing the FOIA, administrative or litigation request. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notices Commerce/DEPT-5, Freedom of Information Act and Privacy Act Request Records, Commerce/DEPT-14, Litigation, Claims, and Administrative Proceeding Records, and Commerce/DEPT-25, Access Control and Identity Management System. NOAA-5 Fisheries Law System. Enforcement Cases , NOAA-6, Fisherman Statistical Data Disclosure: The FOIA requester's identity (name/organization) is recorded in NOAA's FOIA Logs, which are publicly available. NOAA also discloses all contact information with individuals working on a request, including the Office of the General Counsel, the Department of Commerce, and to the Department of Justice if the FOIA case advances to litigation. Failure to provide sufficient identifying information, including but not limited to PII, may result in the FOIA, administrative or litigation request not being processed, and/or for disclosures to be delayed due to inability to respond to the request through FOIAonline.
X	Yes, notice is provided by other means. Specify how: See above regarding fishing and dealer permits. For employee onboarding and Human Resources (HR) administration, forms such as Declaration for Federal Employment (OF-306) provide notice and privacy act statements (OF-306: https://www.opm.gov/forms/pdf_fill/of0306.PDF) (not stored in this system). For system administration, notice is given in writing as part of the supervisor's request for the PII. eDiscovery Application: The information is redacted as part of the FOIA review process. The user voluntarily submits the information; if not, the business cannot be conducted.
	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: Dealers do have the right to decline, by not providing data to ACCSP, but in doing so any trips or landings that they make will be in violation of permit requirements. Permit Data: The personal information is collected when the individual completes the appropriate application. On the application, the individual is advised that NMFS will not be able to issue a permit if the individual does not provide each item of information requested. The individual may choose to decline to provide the required personal information at that time, but will not be able to receive a permit. For employee onboarding and HR administration: Individuals may decline to provide PII to their HR specialist or supervisor, in writing, but this may affect their employment status. Employees may decline to provide PII for system administration (to their supervisors, in writing), but their employment status may be affected. eDiscovery Application: The BII/PII is collected via email as part of conducting business. Not providing the information affects the ability to conduct business.
	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: Individuals have the right to consent to particular uses of their PII/BII, either to an intermediary entity such as ACCSP or to NOAA, yet failure to consent to all uses of the information negates their opportunities to legally fish. A written statement of consent to only particular uses, of those outlined on fishing or dealer applications, would be sent to the entity directly receiving the information. For employee onboarding and HR administration: Individuals have the right to consent to only particular uses of their PII, to their HR specialists or supervisors in writing, but failure to consent to all uses affects their employment status. Employee PII for system administration has only one use. eDiscovery Application: The BII/PII is collected via email as part of conducting business.
	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: Information may be reviewed/updated when completing or renewing a permit application or supporting document, or by calling (978) 281-9246 or emailing the applicable NMFS office at any time (contact information is on the permits and permit applications). Dealers may contact ACCSP by email at info@accsp.org to request that updates be made. Federal Employees/Contractors have the ability to review and update their PII through their HR Specialists. This information is provided as part of new employee orientation. eDiscovery Application: The BII/PII is collected via email as part of conducting business.
	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: Application accounts that are used to add and edit data into database tables that contain PII/BII are audited to a level in which we know who made the changes and what the changes were.
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>2/27/2023</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.
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).*

PII/BII for dealer /permit reporting is stored on a private network in a database with FISMA compliant access controls in place. Applications that interact with the database do so through encrypted channels. There is encryption at rest in the database.

PII used for supporting administrative functions is stored on an access controlled network share. The data at rest is stored in an encrypted state, with a minimum of 128 bit AES in a Microsoft office file.

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> NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries; COMMERCE/DEPT-18, Employees Information not covered by Records of other Agencies; COMMERCE/DEPT-2, Accounts Receivable; COMMERCE/DEPT-13, Investigative and Security Records, COMMERCE/DEPT-5, Freedom of Information Act and Privacy Act Request Records. COMMERCE/DEPT-14, Litigation, Claims, and Administrative Proceeding Records COMMERCE/DEPT-25, Access Control and Identity Management System. NOAA-5, Fisheries Law System. Enforcement Cases , NOAA-6, Fisherman Statistical Data. COMMERCE/DEPT-31 Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations
	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: 200-01 Administrative and Housekeeping Records, 1507 Fisheries Statistics and Marketing News Reporting Files, 2300-04 information Technology Operations and Maintenance Records
	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	
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: A significant amount of individuals could be identified from the PII stored
---	-----------------	--

X	Quantity of PII	Provide explanation: NOAA4100 collects as little PII as necessary to support business functions, but this includes PII from Permits data and from internal administrative functions.
X	Data Field Sensitivity	Provide explanation: Sensitive information including the Social Security Number is collected.
X	Context of Use	Provide explanation: The value of the data beyond its use at GARFO and other supporting missions is small.
X	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq.
X	Access to and Location of PII	Provide explanation: PII/BII for dealer and permit reporting is stored on a private network in a database with FISMA compliant access controls in place. Applications that interact with the database do so through encrypted channels. PII used for supporting administrative functions is stored on an access controlled network share. The data at rest is stored in an encrypted state, with a minimum of 128 bit AES in a Microsoft office file.
	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 GARFO 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 collected at 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.

There is a potential risk of the loss or compromise of ACCSP storage of Permit contact information that is not stored within the accreditation boundaries of NOAA4100.

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.