

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



**Privacy Impact Assessment
for the
NOAA0201
WOC Operation Center (WOC)**

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

GRAFF.MARK.HYRUM.151444
7892

Digitally signed by
GRAFF.MARK.HYRUM.1514447892
Date: 2024.11.25 10:07:47 -05'00'

25 Nov 24

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

Date

U.S. Department of Commerce Privacy Impact Assessment

NOAA/OCIO/Web Operation Center

Unique Project Identifier: NOAA0201 (006-48-02-00-01-3511-00)

Introduction: System Description

Provide a brief description of the information system.

As part of NOAA's Service Delivery Division (SDD), NOAA0201 WOC is a diverse information system providing a variety of cloud-based services to Line and Staff Offices within the NOAA Enterprise.

Services include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Domain Name Service (DNS) tailored to meet customer needs. WOC hosts and supports numerous (200+) websites that disseminate a wide variety of data and information to the scientific and meteorological communities and the public at large. This data and information is used for numerous purposes, including: the study of the ocean, atmosphere, and related ecosystems; natural disaster forecasting and monitoring; climatological analysis and climate change; biodiversity; weather prediction; and the preservation of life, limb, and property.

All WOC devices are provisioned in the Federal Risk and Authorization Management Program (FedRAMP)-Certified Amazon Web Services (AWS) Cloud, including US East-West (FedRAMP moderate impact) and GovCloud (FedRAMP high impact) computing environments. For the purposes of redundancy and availability, WOC customers with high security categorization requirements have access to AWS GovCloud (based in Northern Virginia (us-gov-east-1) and Northern California (us-gov-west-2)), and WOC customers with moderate security categorization requirements have access to AWS US East-West (based in Northern Virginia (us-east-1), Ohio (us-east-2), Northern California (us-west-1), and Oregon (us-west-2)).

Address the following elements:

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

NOAA0201 WOC is a General Support System (GSS).

(b) System location

AWS GovCloud: Northern Virginia (us-gov-east-1) and Northern California (us-govwest-2).

AWS US East-West: Northern Virginia (us-east-1), Ohio (us-east-2), Northern California (us-west-1), and Oregon (us-west-2).

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

NOAA0201 is not a standalone system and interconnects with the following NOAA information systems:

NOAA0550 – NOAA Enterprise Network

NOAA1101 - Information Technology Center

NOAA4100 – Greater Atlantic Regional Fisheries Office (GARFO; includes PII/BII)

NOAA4600 – Fishery Resource and Management (FRAM; includes PII/BII)

NOAA5006 - NESDIS Administrative Local Area Network (NESDIS Admin LAN)

NOAA5009 - National Climatic Data Center Local Area Network

NOAA5040 - Comprehensive Large Array-data Stewardship System

NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS)

NOAA8868 - Storm Prediction Center

NOAA8873 - National Data Buoy Center

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

NOAA0201 WOC provides data-dissemination business processes to distribute scientific and meteorological data, general information, and critical time sensitive life and property information to the public and meteorology community. This data is processed by other NOAA information systems and other federal agencies for use by the federal government and the public.

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

Only NOAA personnel (government employees and/or contractors) with valid user accounts and authentication may access information in the system. Access requires the use of Government Furnished Equipment (GFE). Remote access requires the use of a Virtual Private Network (VPN).

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

All data is encrypted in transit

(g) Any information sharing

NOAA0201 WOC provides data-dissemination business processes to distribute scientific and meteorological data and information gathered from a variety of sources across the globe. This data is processed by other NOAA information systems and other federal agencies for general use by the federal government and the public. In other words, NOAA0201 WOC provides the cloud-based infrastructure and platform (IaaS and PaaS) by which WOC customers gather, analyze, and disseminate scientific and meteorological data to the customer's various stakeholders (other NOAA systems, various federal and state agencies, and the general public).

In addition to the scientific and meteorological data, NOAA0201 contains PII in the form of contractor and federal employee contact information (name, phone number(s), email address(es), user ID) gathered from the employee(s) during the hiring process via phone, email, and in person. The information is vetted during the hiring and badging processes and used for administrative purposes only.

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

5 U.S.C. 301; 44 U.S.C. 3101; 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

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

The FIPS 199 Security Categorization for NOAA0201 WOC is High (CIA = H, H, H)

Section 1: Status of the Information System

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

_____ This is a new information system.

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

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

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

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

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*	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	X
e. File/Case ID	X				
n. Other identifying numbers (specify): Captain's license, State and Federal Dealer Numbers (if applicable), permit or license numbers for Federal or state permit/licenses issued and start and end dates and other permit status codes, vessel name and registration number. Per subsection (k): West Coast Groundfish Permits: check number, date and amount, for permit fees.					
*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 Individual Fishing Quote (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	X
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. West Coast Groundfish Observer Program (WCGOP) and Observer Logistics (OBSLOG): Observers' emergency contact information (whom to contact in case of observer emergency). Economic Data Collection (EDC): costs, revenue, ownership, and employment. West Coast Groundfish Permits: Permit applicant, permit holder, permit transferor/transferee, vessel owner, vessel operator, dealer applicant, dealer permit holder. Name of corporation, state and date of incorporation of business and articles of incorporation, marriage certificate, divorce decree, death certificate.					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
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): Vessel name, vessel length overall. Name of corporation, state and date of incorporation of business and articles of incorporation. WCGOP and OBSLOG: observer deployments, official observer statements (also called incident reports, affidavits). Sometimes when an observer witnesses a potential violation, Office of Law Enforcement (OLE) requests them to fill out a statement regarding the event; vessel length and type; vessel safety checklist, work related Performance (Training, Scores, Evaluations) EDC: costs, revenue, ownership, and employment West Coast Groundfish Permits: vessel name, vessel length overall OLE Vessel Monitoring System (VMS): vessel location, type of gear being used.					

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	X	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	d. 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). WCGOP and OBSLOG: vessel characteristics information (name, United States Coast Guard (USCG) #, # of crew, captain name), fishing effort information (fishing locations, gear used, depth, etc.), catch information (species caught, retained and discard, species compositions), biological data (otoliths, lengths, tissue samples) and protected species information (takes, injuries, sightings, samples, specimen collection) EDC: species catch information West Coast Groundfish Permits: 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	
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): State or Regional Marine Fisheries Commission's Data.					

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

The information pertains to DOC and contractor employees. The accuracy of the information is vetted during the hiring and security badging processes.

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.

WCGOP and OBSLOG: Data is entered by Observer personnel and is run through nearly 300 rigorous trip error checks to ensure the validity of the data. All data is also reviewed by Observer debriefing personnel to ensure the accuracy and validity of the data. EDC: Data is either entered directly by commercial fishermen or double key entered by EDC staff members to ensure accuracy. All data is reviewed during a quality control process by EDC staff, during which time EDC staff address potential inaccuracies by working directly with the commercial fishermen to confirm data entries.

West Coast Groundfish Permits Program: Historic data that was migrated into the PERMITS database managed by Northwest Fisheries Science Center (NWFSC), has been validated with the West Coast Region (WCR) Permits Office. With that said there are still a few outliers of historic data that was not migrated correctly. This information of historic permit records has not been deemed critical and due to the manual work involved to correct this data, it has not yet been corrected. Historic data records are or will be manually corrected. Since the NWFSC has managed this database, all data is validated by the WCR Permits Office. This includes creating new Permits for a new year and any permit ownership or vessel registration transfers and vessel ownership transfers.

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 0648-0212 0648-0593
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (Check all that apply.)

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

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

Section 3: System Supported Activities

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

Activities			
Audio recordings		Building entry readers	X*
Video surveillance	X*	Electronic purchase transactions	
Other (specify): * Video Surveillance and Building Entry Readers are in use by NOAA4600 FRAM. NOAA0201 now hosts this type of data for NOAA4600 FRAM.			
	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):			

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 (and transfers to the WOC) 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 U.S. Department of Agriculture), 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 Defense Enrollment Eligibility Reporting System and not retained).

2. For Establishing Employee IT system user accounts: Name, Office, Government phone number, email address, supervisor.

GARFO collects and maintains (and transfers to the WOC) 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 Atlantic Coastal Cooperative Statistics Program (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 publicly available through our website. We also allow other regions, centers and state organizations access to the publicly 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 National Marine Fisheries Service (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.

WCGOP and OBSLOG

1. WCGOP Database: Information collected from vessels is used in fisheries management and stock assessments. Information collected by observers, including statements of fact from vessels in the fishery may also be used by law enforcement to investigate and prosecute potential violations or criminal activity. Information collected is from members of the public.

2. OBSLOG: Information collected is used to determine eligibility of applicants wishing to be trained as a federal fishery observer. There are educational and other requirements specified in the federal register that must be met for a person to be eligible. OBSLOG also serves as the access point to OLE and USCG to view statements of fact and other incidents. Statements of fact are stored in the WCGOP database, but are viewable in OBSLOG via a database link. Information collected is from members of the public.

EDC

EDC requests data on costs, revenue, ownership, and employment and this information is used to study the economic impacts of the West Coast Trawl Groundfish Catch Share Program on affected harvesters, processors, and communities, as well as net benefits to the nation. Information is collected so that EDC economists may evaluate the Catch Share Program. Aggregated data and analyses are compiled into a report and presented to the Pacific Fishery Management Council. Additional economic analyses may be conducted by other NMSF staff. Information collected is from members of the public.

West Coast Groundfish Permits Program

This information will allow NMFS to identify owners and holders of permits and non-permit registrations and vessel owners and operators, evaluate permit applications, and document agency actions relating to the issuance, renewal, transfer, revocation, suspension or modification of a permit or registration. Tax Identification Numbers allow positive identification for cost recovery billing of IFQ holders.

OLE VMS

The declaration information is used to ensure compliance with regional and federal fishing regulations. The data is also utilized to analyze fishing activity in relation to whale and turtle entanglements on the West coast. The data is joined with other data sources with a goal of identifying methods for reducing whale and turtle entanglements off the West Coast.

- 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.)

Potential threats include the potential for unintentional disclosure of PII. This threat is countered by training all personnel with respect to cyber security, privacy, and awareness training annually. The information is retained in accordance with departmental policies.

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 (NDAs), 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.

Both external threats and insider threats pose a potential threat to privacy of the information stored. Additionally, any process or person that would disclose NOAA4600 data in an unauthorized or negligent manner are considered a threat. NOAA4600 implements various controls to protect the unauthorized disclosure of information including:

- Implementation of security standards on IT equipment which the data is stored
- Annual IT Security Training
- NDAs
- Enforcement of least privilege
- Utilization of encryption
- Sanitization of media

Additional threats also exist due to external sharing with the public for the purposes of law enforcement and/or litigation disclosure in discovery.

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*		X**
Private sector	X		X***
Foreign governments			
Foreign entities			
Other (specify):			

*Law Enforcement and/or litigation disclosure in discovery;

**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: NOAA0550 – NOAA Enterprise Network NOAA1101 - Information Technology Center NOAA4100 – Greater Atlantic Regional Fisheries Office (GARFO; includes PII/BII) NOAA4600 – Fishery Resource and Management (FRAM; includes PII/BII) NOAA5006 - NESDIS Administrative Local Area Network (NESDIS Admin LAN) NOAA5009 - National Climatic Data Center Local Area Network NOAA5040 - Comprehensive Large Array-data Stewardship System NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS) NOAA8868 - Storm Prediction Center NOAA8873 - National Data Buoy Center NOAA4200, Northeast Fisheries Science Center Network, NOAA4020, Science and Technology (S&T) Silver Spring, 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 Memoranda of Agreement/Service Level Agreement with NOAA4000 has with ACCSP. ACCSP is only receiving aggregate data.
---	---

	NOAA4000 - Fisheries Wide Area Network (WAN) and Enterprise Services NOAA4800 - Alaska Fisheries Science Center NOAA4930 - Southwest Fisheries Science Center NOAA4600 also has a connection with a non-FISMA system, the Monterey Bay Aquarium Research Institute All traffic is routed over an enterprise WAN connection and additional firewall access control levels limit the connection to specific resources and ports. Secure database connections (when a database connection is utilized) and appropriate access control levels on named database accounts are utilized.
	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	X	Government Employees	X
Contractors	X		
Other (specify): General Public who have a demonstrated need and have signed a NDA are granted access to data via the FRAM data warehouse. Data sharing agreements may also be used for valid collaborators for research purposes. EDC: Members of the General Public who have a demonstrated need and have signed an NDA are granted access to data via the FRAM data warehouse.			

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: 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 Vessel permit application: https://apps-garfo.fisheries.noaa.gov/fishtank/login/login Dealer permit application: https://apps-garfo.fisheries.noaa.gov/fishtank/login/ 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, COMMERCE/DEPT-25, Access Control and Identity Management System, NOAA-5, Fisheries Law System. Enforcement Cases, and 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 FOIA online. WCGOP https://nwcoa3.nwfsc.noaa.gov/obsprod/logon.display (Displays a pop-up that requires Internet Explorer or Firefox to access the app and statement) OBSLOG https://www.webapps.nwfsc.noaa.gov/apex/ifu/f?p=505:28 EDC https://www.webapps.nwfsc.noaa.gov/edc/PrivacyAct West Coast Groundfish IFQ https://www.webapps.nwfsc.noaa.gov/ifu (Scroll to the bottom and click "IFQ Privacy Act Statement to open the pop-up window. The Statement is also available when user clicks the "Log In" button) West Coast Groundfish Permits: https://www.webapps.nwfsc.noaa.gov/apex/ifu/f?p=112:88::POP:NO::: .	
X	Yes, notice is provided by other means.	Specify how: Notice is provided as part of employee enrollment, and on the staff directory warning banner. 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. WCGOP and OBSLOG Observation Information: Vessel captains/owners receive letters from the permit office explaining the requirements when they apply for permits or individual fishing quota accounts. OBSLOG Observer Application: Those submitting the information are informed on the observer provider company's application that it is a requirement for participating in the program. EDC: Notification is provided on the economic data survey instrument. West Coast Groundfish Permits: Notice is provided on the permit or related application. NOAA4600 System Maintenance Information: Information collected for employee/contractor emergency contact, and disaster recovery/continuity of operations is requested in writing. Information collected for account management is requested in writing or via email by the user's supervisor, at the time that the user requests an account on the information system.
	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: An individual may decline but would not have access to the NOAA IT network. 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. WCGOP and OBSLOG Observation Information: Vessel captains/owners may decline to provide PII/BII in writing to observers or observer program staff, but participation in a fishery requires consent to carry an observer when directed to by the agency and to provide information requested by the observer. If the individual declines, the vessel will be fishing out of compliance with the regulations and would be in violation. OBSLOG Observer Application: Observer applicants may decline to provide the information by not completing the application, but they would be denied entry into the program. Eligibility to perform the duties of a federal fishery observer cannot be determined without providing PII. EDC: The respondent may decline by not completing and submitting the required EDC form, but that may delay the completion of administrative actions such as permit renewal, vessel registration, license issuance, and quota transfers. Economic data collection is mandatory under the Catch Share Program, and thus participation in the EDC program is mandatory under the regulation 50 CFR 660.114. West Coast Groundfish Permits: The personal information is collected when the individual completes the appropriate application. On application, the individual is advised that providing the information is voluntary, but 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 or to consent to the particular use of their personal information at that time. NOAA4600 System Maintenance Information: Employees and staff may decline to provide PII /BII for emergency contact and disaster recovery by not filling in the PII/BII information. Employees and staff may decline to provide account information by not applying for an account, but this may be required for their job duties.
	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: There is only one use, which is explained during employee orientation. The employee may consent to this use of their data by continuing to move forward with receiving a badge and account access. 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. WCGOP and OBSLOG Observation Information: Vessel captains/owners may not consent to provide PII/BII (by not providing notification to observers of planned trips, or not allowing observers to board), but participation in a fishery requires consent to carry an observer when directed to by the agency and to provide information requested by the observer. Observer coverage of fisheries is required by regulation and to participate in the fishery, information must be collected for management uses, including stock assessments, and may also be used by law enforcement to investigate and prosecute potential violations or criminal activity. There are no other uses. OBSLOG Observer Application: Consent to the use of applicant information for determination of eligibility for employment is implied by completion of the application. EDC: Vessel owners or captains may decline to provide consent to the use of their data in economic analyses (this is the only use of the data) by not completing the form, but failure to comply may delay the completion of administrative actions such as permit renewal, vessel registration, license issuance, and quota transfers. West Coast Groundfish Permits: The individual may choose to decline to provide the required personal information or to consent to the particular use of their personal information at that time (see 7.2) NOAA4600 System Maintenance Information: Where specified in NOAA Office of Human Capital Services forms, employees have the opportunity to consent to particular use of their PII/BII.
---	---	---

		Employee and staff General Personal Data information is required for badging and emergency notifications but users may decline to provide COOP info. Employees and staff are informed of the use of their data, and these data are not used for any other purpose.
	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 view their info online and make a request for a change. Information may be reviewed/updated when completing or renewing a permit application or supporting document, or by calling (979) 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. WCGOP and OBSLOG Observation Information: Fisher information is collected from state or federal agencies where fishers submit the information in order to participate in the fishery. Fishers may contact WCGOP administration or permitting office by email or telephone to update their contact information. OBSLOG Observer Application: Observers are able to submit updates or requests to view the data, to their observer provider. EDC: Individuals may request their original submissions of PII/BII from the federal office staff. They may update any PII/BII via phone, fax, or mail. West Coast Groundfish Permits: When completing or renewing a permit application or supporting document, or by calling or emailing the applicable NMFS office at any time. Permits are completed online or by reviewing and updating a paper renewal application pre-filled by NMFS with their most recent information on the permit holder. NOAA4600 System Maintenance Information: Instructions for updating contact information fields are provided in the forms
---	---	--

		the customer fills out. NOAA Employees can update PII on an as needed basis through their supervisor for COOP and Emergency contact information.
	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 NDA.
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>August 27, 2024</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.
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).*

NOAA0201 uses audit logging and multi-factor authentication to protect the PII/BII in the system. Only NOAA personnel (government employees and/or contractors) with authenticated access would be able to change or delete information.
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.

NOAA4600 utilizes Data Resource Accounts, and Access Control Levels allow authorized staff to access NOAA4600 data, which may contain PII or BII. Computer account types include, but, are not limited to, Domain Accounts, Email/LDAP Accounts, Unix Accounts, Intranet Accounts, and Local System Accounts. Group memberships are used to assign Security Access Controls to authorized Data Resource Accounts. NOAA4600 applies Least Privilege and Least Functionality principles when providing security clearance. Access Enforcement Mechanisms (Encryption-at-Rest for offline media, Encryption-in-Transit, Distributed Directory Services) are implemented to prevent malicious or accidental access by unauthorized persons.

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."

Yes, this system is covered by an existing system of records notice (SORN).

Provide the SORN name, number, and link. *(list all that apply):*

[COMMERCE/DEPT-2](#), Accounts Receivable;

[COMMERCE/DEPT-5](#), Freedom of Information Act and Privacy Act Request Records.

[COMMERCE/DEPT-13](#), Investigative and Security Records,

[COMMERCE/DEPT-14](#), Litigation, Claims, and Administrative Proceeding Records

[COMMERCE/DEPT-18](#), Employees Personnel Files Not Covered by Notices of Other Agencies.

[COMMERCE/DEPT-25](#), Access Control and Identity Management

[COMMERCE/DEPT-31](#), Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations

[NOAA-5](#), Fisheries Law System Enforcement Cases;

[NOAA-6](#), Fisherman Statistical Data

[NOAA-15](#), Monitoring of National Marine Fisheries Service Observers

[NOAA-19](#), Permits and Registrations for United States Federally Regulated Fisheries;

[NOAA-23](#), Economic Data Collection (EDC) Program for West Coast Groundfish Trawl Catch Share Program off the coast of Washington, Oregon, and California

[OPM/GOVT-1](#): General Personnel Records

[OPM/GOVT-10](#): Employee Medical File System Records

	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: NOAA Records Disposition Handbook Chapter 200-12 200-01 Administrative and Housekeeping Records, 1507 Fisheries Statistics and Marketing News Reporting Files, 2300-04 information Technology Operations and Maintenance Records West Coast Groundfish Observer Program (WCGOP) and Observer Logistics (OBSLOG: 1502-02 Survey Operations Files; 1513-10 Observer Program Files EDC: 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. West Coast Groundfish Permits: NOAA 1504-11; NOAA 1514-01 NOAA4600 System Maintenance Information: GRS 2.1 Employee Acquisition Records GRS 2.2 Employee Management Records GRS 2.3 Employee Relations Records GRS 2.4 Employee Compensation & Benefits Records GRS 2.5 Employee Separation Records GRS 2.6 Employee Training Records GRS 2.7 Employee Health & Safety 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
	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: Minimal administrative information for IT work identity. A significant number of individuals could be identified from the PII stored.
X	Quantity of PII	Provide explanation: Minimal work contact information. NOAA4100 collects as little PII as necessary to support business functions, but this includes PII from Permits data and from internal administrative functions. The Information collects and maintains records which may be perceived as sensitive or potentially damaging for individuals or business related to the West Coast Observer Program, Economic Data Collection Program and West Coast Groundfish Permits Programs.
X	Data Field Sensitivity	Provide explanation: Sensitive information including the Social Security Number is collected. The IFQ and Permits applications contains moderately sensitive PII and BII, such as name, address, Tax ID number, and ownership interest. The IFQ system also maintains unique Vessel Account Identification numbers and manages Vessel Account balances and deficit tracking. This type of information is considered privileged, and unauthorized disclosure is prohibited

		by the Magnuson-Stevens Act, the Privacy Act, and laws prohibiting disclosure or unauthorized access.
X	Context of Use	Provide explanation: Minimal data for IT user identification. 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. Magnuson-Stevens Fishery Conservation & Management. Act, Sec. 402. ø16 U.S.C. 1881a; Information Collection.
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.)

The potential threats associated with the gathering of this information is thought to be minimal. The information collected from federal and contractor employees is for administrative purposes only, and is collected during hiring and badging processes. The information is retained in accordance with departmental policies and all staff are trained with respect to cyber security and privacy concerns on an annual basis.

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.

The system collects and maintains records that may be perceived as sensitive or potentially damaging for individuals or business related to the West Coast Observer Program, Economic Data Collection Program and West Coast Groundfish Permits Programs. Any process or person that would disclose this data in an unauthorized or negligent manner would be considered a threat. All collected information collected was deemed as important by the programs that manage the processes and is important for fisheries management.

NOAA4600 has put controls in place (i.e., encryption at rest and proper access controls) to ensure that the information is handled, maintained and disposed appropriately. Further, NOAA4600 follows DOC and NOAA mandates as well as trains applicable personnel to ensure everyone has a certain knowledge of proper security practices. This does not cause any new privacy risks.

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.