Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA4930
Southwest Fisheries Science Center (SWFSC) 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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.05.20 13:47:27 -04'00' 5/8/2024

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/ NMFS/ Southwest Fisheries Science Center (SWFSC) Network

Unique Project Identifier: NOAA4930

Introduction: System Description

The Southwest Fisheries Science Center (SWFSC), NOAA4930, is a General Support System (GSS) supporting approximately 300 users consisting of scientific, administrative, and support staff and provides multidisciplinary scientific and technical information to the West Coast Regional Office (WCRO) of NOAA Fisheries, other NOAA line offices, stakeholders and other constituents to inform decision and policy-making processes. The SWFSC Network is used to provide information technology support to all federal employees, contractors, affiliates and volunteers. The roles held include scientific, administrative, and support staff who are distributed among the California cities/communities of La Jolla, Monterey, and Santa Cruz. All personnel are subject to the same security clearance requirements regardless of status or role. The network provides access to essential NOAA services such as email, the Internet, shared printer/copiers, software applications and data. Information and data that are processed, analyzed and summarized include environmental, biological, chemical, technical, contract and procurement documentation and other administrative data that scientists, managers and administrators use to support the NOAA Fisheries mission-related research and management programmatic decision processes.

Address the following elements:

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

The NOAA4930 system is a General Support System.

(b) System location

The NOAA4930 system is comprised of the NOAA/NMFS Southwest Fisheries Science Center facilities located in the cities/communities of La Jolla, Santa Cruz and Monterey in the state of California.

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

The NOAA4930 system is interconnected with the following FISMA systems/entities:

- NMFS WAN (NOAA4000)
- NMFS OCIO - Office of Science and Technology (NOAA4000)
- NMFS NWFSC (NOAA4600)
- N-Wave (NOAA0550)
- University of California, Santa Cruz (UCSC) from the Santa Cruz Laboratory only.

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

The operational system functions that are provided include:

- Network File Storage, Sharing, and Printing
- Internet Access
- NMFS Wide Area Network Connectivity
- Administrative Support Systems
- Scientific Database Access
- Scientific Statistical Data Analyses
- Geographic Information Systems
- Web Based Information Dissemination
- Telecommunications

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

NOAA4930 information is retrieved via government furnished information technology (IT) equipment after verifying authentication and authorization levels.

Local data are stored on a Windows network fileshare. Access to data stored locally is restricted to authorized personnel only via Windows Active Directory (AD) group. Authorized users authenticate to access the data via two factor authentication (Common Access Card (CAC)). For authorized users who are in the process of obtaining a CAC, they access the system via username and strong password that meet the Department of Commerce (DOC) password requirements. The principle of least privilege and separation of duties is implemented by SWFSC to ensure that personnel with the need to know only have access to this information.

Authorized users who access the data from outside of the NOAA4930 boundary may only do so via NMFS Virtual Private Network (VPN) concentrators (East or West). The NMFS VPN connections are encrypted, the users must authenticate onto the VPN via two factor authentication, and the authorized user may only connect to the NMFS VPN with government furnished equipment (GFE) that is subject to all Federal Information Security Management Act (FISMA) system requirements.

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

NOAA4930 transmission is protected using defense in depth architecture. Particularly sensitive information is encrypted while in transmission.

(g) Any information sharing

The Southwest Highly Migratory Species database (SWHMS) contains database links to external database systems that contain BII. These external database systems, which are stored at the Pacific States Marine Fisheries Commission (PacFIN) – a private interstate commission that warehouses state data and provides access to authorized users like us – and the U.S. Coast Guard, are accessed through user accounts managed by the Commission. We do not distribute or share BII data from PacFIN and we retain control over who may access the SWHMS database. The information we retrieve from the SWHMS database is summarized to a non-confidential level and shared in non-confidential data products and reports as required by our reporting mandates.

Information collected and managed in the system is mandated under Magnuson-Stevens Fishery

Conservation and Management Act (MSA) re-authorization (H.R. 5946--109th Congress), Pacific Highly Migratory Species (HMS) Fisheries Management Plan (50 CFR Parts 223, 224 and 660) and international reporting obligations. As part of these reporting obligations, information in this system is shared case by case within NOAA, with state, local and tribal governments which provide us with logbook and landings data, and with foreign entities such as the Inter-American Tropical Tuna Commission, who in turn provide us with summaries of catch and effort data from member countries that fish for HMS in the Pacific. That is, we receive raw data from the state, local and tribal governments, and summarized data from foreign entities, and then we share the state, local and tribal summaries with the applicable foreign entities and the foreign entities' summaries with the state, local and tribal governments.

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

	Type of Information Collected (Introduction h.)	**Applicable SORNs (Section 9.2)**	**Programmatic Authorities (Introduction h.)**
1.	Fishermen's Statistical Data	NOAA-6	Fish and Wildlife Act as amended (16 U.S.C. 742 et seq.)
			Fishery Conservation and Management Act of 1976 as amended (16 U.S.C. 1852)
2.	Visitor Logs & Permits for Facilities	COMMERCE/DEPT-6	5 U.S.C. 301
			44 U.S.C. 3101
3.	Investigative and Security Records	COMMERCE/DEPT-13	5 U.S.C 301
			5 U.S.C. 7531-332
			28 U.S.C. 533-535
			Equal Employment Act of 1972
4.	Collection & Use of SSN	COMMERCE/DEPT-18	44 U.S.C. 3101
			Executive Order 12107
5.	Department Mailing Lists	COMMERCE/DEPT-19	Public Works and Economic Development Act of 1976, Pub.L. 94-487, Title II, 90 Stat. 2339
			42 U.S.C. 3121
6.	System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
			Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
			Electronic Signatures in Global and National Commerce Act, Public Law 106-229

			28 U.S.C. 533-535
7.	Public Health Emergency Info & Reasonable Accommodation	COMMERCE/DEPT-31	Rehabilitation Act, 29 U.S.C. 701 et. seq
			Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d)
			29 CFR parts 1602, 1630, 1904, 1910, and 1960
			29 USC chapter 15 (e.g., 29 U.S.C. 668)
			Executive Order 12196
			5 U.S.C. 7902
8.	Personnel Actions Including Training	OPM/GOVT-1	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 5379, 8347
			Executive Orders 9397, as amended by 13478, 9830, and 12107

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

The FIPS 199 impact level of this system is moderate.

Section 1: Status of the Information System

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

_____ This is a new information system.

_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): Removed the interconnection between NOAA4930 and the University of California, San Diego (UCSD) since it is now being maintained/managed by N-Wave (NOAA0550).					

____ 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	
b. Taxpayer ID	X	g. Passport	X	k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: The business need for collecting SSN data is within the Operations and Management division in NOAA4930. This information is required on forms for the processing of passport applications. This data is only stored until the passport application process has been completed at which point it is deleted.					

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

f. Race/Ethnicity	X	m. Education	X	t. Mother's Maiden Name	
g. Citizenship	X	n. Religion	X		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		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):					

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

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

Other Information (specify)
BII - Catch amounts and sales information including dates, buyers, sellers, amounts and prices.

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): *The phone-based communications arc for data Quality Assurance/Quality control (*QA/QC)* only; primary data collection is not conducted via phone. The notice for this data being collected is communicated to the fishermen in the permitting process via the permit application.					

Government Sources

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

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

Information is collected directly from the individual or entity for whom the information pertains to the maximum extent possible.

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. 0648-0009 Billfish Tagging Report
	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):			

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)		For web measurement and customization technologies (multi-session)	X
Other (specify): In compliance with federal and international mandates.			

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).

(a) The information collected under the authority of the HMS FMP and international treaty requirements is used to monitor compliance with federal mandates and international reporting requirements (civil enforcement). Contact information is used to contact the submitter when insufficient or erroneous data are submitted. Information is collected from members of the public.

(b) Under requirements of the Western and Central Pacific Commission (WCPF), vessel identifiers are required to be submitted with individual fishing set information. Logbook and landings information, collected from NMFS permit holders and from state, local and tribal entities, are required to be submitted under FMPs and international reporting obligations. This information is used to ensure that all vessel owners that catch or sell HMS have a valid permit and are in compliance with the requirements of that permit. Information is collected from members of the public.

(c) PII is collected for all personnel (federal employees, contractors, etc.) designated to

work at the SWFSC. This information is collected for administration and business functions within SWFSC. Photographs that are taken are used in internal communications (emails for personnel introductions to staff so that the new personnel can be recognized as being affiliated with the SWFSC), and for identification badges for short term or temporary personnel. PII data is also used for personnel management – human resources purposes. This information is required on forms for the onboarding of new hires.

(d) For contractual purposes, the SWFSC stores procurement and contract information, stored in a restricted area of the shared drive accessible only by authorized personnel.

(e) PII may be present on identification that is presented by visitors (public) at the time of check in for on-site visits. This information is collected via an ID card scanner. The data is stored on a dedicated server for this application. The data is used to establish the positive identification of a visitor for verification that they have been authorized by a staff member who is hosting them and also to maintain a record for who is in the facility in case there is an emergency. The data is only accessible to authorized administrative personnel who monitor visitor check in and check out, and IT system administration staff. The data is not disseminated.

(f) Video surveillance and door card readers are in use for maintaining the physical security of the SWFSC facilities. Signs are present informing all individuals that video surveillance is being conducted. The data is only accessible to authorized administrative personnel who monitor the physical security of the building and IT system administration staff. The data is not disseminated.

All information is stored on a restricted area of a shared drive or on dedicated devices that are accessible only by authorized personnel.

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.)

The main threat to the privacy data holding at the SWFSC is the accidental release or disclosure of data, and there is also the risk of insider threat. To mitigate the risk of this occurring there are a number of controls in place. All personnel are required annually to complete the NOAA Cybersecurity Awareness & Privacy Training Course and to read and accept the rules of behavior. By accepting the rules of behavior, the user has formally acknowledged that they are on notice for abiding by these agency rules which includes the proper handling of PII, BII, and CUI data. The data is stored with encryption enabled on the storage devices. If the device is in the possession of

the personnel who is responsible for the data, the device is stored in a secured location with access restricted to personnel who have a legitimate business need to access the data. The vast majority of the data is stored on a centrally maintained (by Center IT staff) Windows fileserver with encryption enabled for the data at rest. Access to each specific fileshare is restricted to a specific Windows AD group of which each member must have a legitimate business need to access the data. The fileserver device is located in a secured data center with physical access restricted to Information Technology Services (ITS) staff and limited facilities personnel only. Access to this space is controlled by a card reader system that maintains audit logs of individual personnel entries and timestamps. When any data storage device is taken out of service and excessed, its content is sanitized via a degausser for magnetic storage media or device is physically destroyed in an industrial shredder for solid state media.

Authorized users (NMFS employees and contractors) have access to the confidential logbook and landings information and access is controlled through database roles. All authorized users that access confidential information must sign a non-disclosure agreement that certifies that the user has read and understands NOAA Administrative Order on Confidentiality of Statistics (NAO 216-100). These non-disclosure agreement are maintained at SWFSC.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies	X		
Public			
Private sector			
Foreign governments			
Foreign entities	X		
Other (specify):			

*PII shared with law enforcement in the instance of a physical security threat.

	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?

	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.

X	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: NMFS Northwest Fisheries Science Center (NOAA4600), NMFS Office of Science and Technology and the NMFS WAN (NOAA4000). Network connection is via an encrypted wide area network, only authorized users who have signed NDA have access to the S&T system, authentication is via username and strong password that meets DOC password requirements. The system is administered by NMFS ST6 database administration staff at NOAA4000. The NOAA4930 system connects to N-Wave (NOAA0550) for NOAA wide area network and Internet access. The connection to NOAA0550 is physically through the University of California, San Diego and the University of California, Santa Cruz. These connections are administered and maintained by NOAA0550. The boundary between NOAA4930 and these external entities are protected by Cisco ASA firewall devices.
	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): Cooperative institute employees, students, and volunteers.			

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/west-coast/sustainable-fisheries/west-coast-highly-migratory-species-logbooks https://www.nmfs.noaa.gov/aboutus/privacy.html .

X	Yes, notice is provided by other means.	Specify how: Notice is provided by language in the logbooks, sent to the fishermen, stating that the information must be submitted in order to maintain a Federal permit, per cited regulations. Notice is given to SWFSC personnel (including federal employees, contractors, etc.) in writing. For responses to solicitations, notice is given on the request for information (RFI) or request for proposal (RFP). Written notice is visible in a conspicuous manner to all facility visitors in the reception area where they are checked in. Written notices stating that video surveillance is being conducted are posted around the exterior of the facility and at entry points.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals may decline to provide the information by not submitting the logbook, but in order to maintain a Federal fishing permit, it must be provided. Federal employees and contractors may decline to provide information in writing, but it may affect their job status and access to the facility. Responses to RFPs/RFIs are voluntary, based on the offeror's decision to respond. Visitors may choose which form of positive identification to present for checking in for an on-site visit. An individual may choose to not present their identification but they will not be allowed to enter the facility beyond the reception area.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Written notices stating that video surveillance is being conducted are present around the exterior of the facility and at entry points. If any individual wishes to not be recorded they may do so by not accessing the area within the facility. However, video surveillance and recording around the exterior of the facilities is conducted 24 hours a day, seven days per week, so an individual who is walking by could be recorded.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: The information collected is only used for the stated purposes of monitoring and reporting at the level required under federal and international requirements. Individuals provide consent by completing and submitting the logbook. Employees and users accessing the system are provided with the link to NOAA's privacy policy which states: "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." There is only one use for proposals in response to RFIs or RFPs. When visitors check in for an onsite visit, there is a written notice of the requirement of identification to be presented and the receptionist will ask the visitor for identification. Visitors consent to present identification is voluntary but it is required for entry to the facility. If they decline to present identification then the host may conduct their visit with the individual in the reception area. Written notices stating that video surveillance is being conducted are present around the exterior of the facility and at entry points. By entering the facility an individual consents the video surveillance.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: There is no opportunity for individuals to review or update the video surveillance images recorded for safety & security purposes.

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: Periodic renewal notices are sent to permit holders, which give them the opportunity to update their information collected. Vessel name changes and other updates can be provided on the permit renewal forms that are collected and maintained. Fishermen can also call the Permits Program Office to provide updates. All federal/contractor/affiliate user information is maintained within NOAA Staff Directory (NSD) database where users can review and update their contact information at https://nsd.rdc.noaa.gov Offerors will contact the office which issued the solicitation, with updated information. The visitor presents the identification of their choosing for the

		onsite visit check in process.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: There is no opportunity for individuals to review or update the video surveillance images recorded for safety & security purposes.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:** Access to data stored locally is restricted to authorized personnel only via Windows Active Directory (AD) group. Authorized users authenticate to access the data via two factor authentication (Common Access Card (CAC)). The principle of least privilege and separation of duties is implemented by SWFSC to ensure that personnel with the need to know only have access to this information.
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): 2/5/2024 ☐ 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).*

For the Highly Migratory Species (HMS) Fisheries Management Plan (FMP) data, the data reside within the boundaries of the NOAA4000 system. Only authorized personnel who have signed a NDA have access to the data. Access to the system from NOAA4930 is via an encrypted WAN connection.

Only authorized NOAA4930 personnel are granted access to the PacFIN database. All authorized

personnel are required to sign a data non-disclosure agreement as part of the conditions to access the data. The database is accessed through a data entry web application using HTTPS protocol.

Local data are stored on a Windows network fileshare. All disk partitions on the Windows fileserver are encrypted to protect the data at rest. Access to data stored locally is restricted to authorized personnel only via Windows AD group. Authorized users authenticate to access the data via two factor authentication (CAC card). For authorized users who are in the process of obtaining a CAC card, they access the system via username and strong password that meet the DOC password requirements. The principle of least privilege and separation of duties is implemented by SWFSC to ensure that personnel with the need to know only have access to this information.

Authorized users who access the data from outside of the NOAA4930 boundary may only do so via NMFS VPN concentrators (East or West). The NMFS VPN connections are encrypted, the users must authenticate onto the VPN via two factor authentication, and the authorized user may only connect to the NMFS VPN with government furnished equipment (GFE) that is subject to all FISMA system requirements.

All NMFS personnel and contractors are instructed on the confidential nature of this information. Through acknowledgement of the NOAA rules of behavior on an annual basis, account request agreements, etc. All users are instructed to abide by all statutory and regulatory data confidentiality requirements, and will only release the data to authorized users who have a business need to have access to the data.

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. *(list all that apply)*: NOAA-6, Fishermen's Statistical Data COMMERCE/DEPT-6, Visitor Logs and Permits for Facilities Under Department Control COMMERCE/DEPT-13, Investigative and Security Records COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-19, Department Mailing Lists COMMERCE/DEPT-25, Access Control and Identity Management System COMMERCE/DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations

	OPM/GOVT-1, General Personnel Records.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: 1. Chapter 901-03: Facility Security Management Operations Records 2. Chapter 1505-11: Catch Statistics Files 3. Chapter 1507-11: Statistical Data Files 4. Chapter 300: Personnel Management Files 5. Chapter 702: Procurement and FOIs Management Files
	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): * After approximately 30 days the video surveillance data is overwritten. When data storage devices are excessed at end of life, the disks are degaussed.			

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

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

X	Identifiability	Provide explanation: The vessel IDs can be used to identify a person or a business but the disclosure of this data would not be severe or catastrophic.
X	Quantity of PII	Provide explanation: PII is collected from SWFSC personnel (employees, contractors, etc.) and visitors who are checked in for on-site entry.
X	Data Field Sensitivity	Provide explanation: The BII data is limited to vessel identifiers, harvest amounts, dates and locations. The value of this information is considered low. Sensitive PII collected from employees exists on individual forms (ex. PDFs of in-processing forms). Sensitive PII collected from visitors consists of ID number from a given identification card source, name, address and date of birth.
X	Context of Use	Provide explanation: The BII data would only disclose previous fisheries harvest amounts for a given geographic location. Information collected is to granted system access and to maintain employee emergency notification lists. The PII data is used within the operations and management purposes including onboarding new hires and for establishing (verifying) identification of visitors for entrance to the facility.
X	Obligation to Protect Confidentiality	Provide explanation: The data is subject to the confidentiality protection of the Magnuson – Stevens Act, 16. U.S.C 1801, Section 402.
X	Access to and Location of PII	Provide explanation: Access to the SWHMS data is limited to fewer than 10 authorized personnel who have a business need to access the data. The PII data that is used for operations and management purposes is stored on servers that are physically secured in the NOAA4930 LAN room and has access to data restricted to authorized staff only via Windows AD domain group permissions. For data on the visitor check in system, the data is only accessible from a single workstation where the data input is completed. Access to this device requires two factor (CAC) authentication followed by restricted access to the application that is controlled by defined accounts for administrative personnel who are authorized to use the system.
	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 main threat to the privacy data holding at the SWFSC is the accidental release or disclosure of data. To mitigate the risk of this threat the following items are in place. Personnel are educated annually via the required NOAA Cybersecurity Awareness and Privacy Training on the policies for accessing and working with privacy data. Periodic inventories are conducted of the data holdings that contain PII and/or BII. During this process, meetings are conducted with the data owners to understand the need for the privacy data that is collected. If a determination is made with the stakeholders that any data holdings are not required for business needs, the data is eliminated via procedures described below. This is completed in an effort to manage the privacy data footprint to ensure the holdings only included what was needed to support the mission of the SWFSC. The data is stored with encryption enabled on the storage devices. The vast majority of the data is stored on a centrally maintained (by Center IT staff) Windows fileserver with encryption enabled for the data at rest. Access to each specific fileshare is restricted to a specific Windows AD group of which each member must have a legitimate business need to access the data. Data storage servers are located in a secured data center with physical access restricted to Information Technology Services staff and limited facilities personnel only. Access to this space is controlled by a card reader system that maintains audit logs of individual personnel entries and timestamps. When any data storage device is taken out of service and excessed its contents are sanitized via a degausser for magnetic storage media or the device is physically destroyed in an industrial shredder for solid state media.

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.