Version Number: 01-2015

U.S. Department of Commerce
NOAA

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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2017.12.01 14:01:17 -05'00' 11/16/2017

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

U.S. Department of Commerce Privacy Impact Assessment
National Marine Fisheries Service
NOAA4930 - Southwest Fisheries Science Center (SWFSC) Network

Unique Project Identifier: 006-03-02-00-01-0511-00

Introduction: System Description

NOAA4930 SWFSC is a General Support System supporting approximately 375 users consisting of scientific, administrative, and support staff (federal employees and contractors) distributed among the California cities of La Jolla, Santa Cruz, and Monterey. There are a variety of hardware platforms and operating systems interconnected on this network system. The systems are designed and configured to support the staff in meeting the agency mission.

The primary functions provided include:

- Network File Storage, Sharing, and Printing
- Internet Access
- NMFS Wide Area Network Connectivity
- Administrative Support Systems
- Scientific Database Access – contains PII and BII.
- Scientific Statistical Data Analysis
- Geographic Information Systems
- Web Based Information Dissemination
- Telecommunications

As a requirement of the Highly Migratory Species (HMS) Fisheries Management Plan (FMP) implemented in 2005, participants (captains of permitted vessels) in HMS fisheries in the Pacific are required to submit logbook information on fishing activities. In addition, to monitor these fisheries and provide accurate catch estimates as required under the FMP and international obligations, landings information is collected and maintained. Biological and life history data are also collected and maintained to supplement stock assessment information used to assess and monitor fish stocks.

The logbook and landings data contain information that identifies fishery participants and contains information related to the business practices of those participants: Names, contact information including work and home e-mail and mailing addresses and phone numbers, vessel and processor identifiers and sales information including dates, buyers, sellers, amounts and prices.

This data is submitted to the Southwest Fisheries Science Center (SWFSC), where the information is entered into a centralized Oracle database, in an encrypted table space, that is located and maintained at the National Marine Fisheries Service (NMFS) Office of Science and Technology in Silver Spring, Maryland. The data is maintained by SWFSC staff and summarized for reporting. Summarization of the data follows established business rules for maintaining confidentiality of the summaries. Any information obtained from fewer than three persons is further aggregated and combined with other data.

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 agreements are maintained at SWFSC.

The categories of data inputted, stored and processed include administrative, scientific, statistical, economic, research and development, and technical.

The Southwest Highly Migratory Species database (SWHMS) contains database links to external systems that contain BII. These external database systems, including 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. We do not distribute or share this BII from our system. The information we receive from those databases is summarized to a non-confidential level and shared in non-confidential data products and reports.

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 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.

The SWFSC Operations and Management division maintains various type of PII and BII in support Center operations and the management of operational resources. The management information for the management of contracts and awards contains BII. The management of facility security that involves visitor access management, parking authorization and access control for Center personnel/staff, and general access to facilities, buildings and spaces include the maintaining of information that contains PII. The management of official government travel, both foreign and domestic, includes the maintenance of information that contains PII. Finally, the management of human resources, which includes emergency contact information, employee and labor relations/worker's compensation includes the maintenance of information that contains PII.

SWFSC also stores procurement and contract information, stored in a restricted area of the shared drive accessible only by authorized personnel.

Additional authorities:

From NOAA-6: Fish and Wildlife Act as amended (16 U.S.C. 742 et seq.) and Fishery Conservation and Management Act of 1976 as amended (16 U.S.C. 1852).

From Dept-6: 5 U.S.C. 301; 44 U.S.C. 3101.

From DEPT-13: Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

From DEPT-18: Includes the following, with all revisions and amendments: 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.

From DEPT-19: 5 U.S.C. 301; 15 U.S.C. 1512, 2205, 2208, and 44 U.S.C. 3101.

From OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

The 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.

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

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

__X__ This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	
c. Employer ID		g. Passport	X	k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify): BII: dealer identification, vessel and processor identifiers					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated					

form: SSNs are stored only in hard copy.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name		h. Place of Birth	X	n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

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

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		Hard Copy: Mail/Fax	X	Online	X
Telephone	X*	Email	X		
Other (specify): All of the information provided comes from the HMS permit.					

*The phone based communications are for data 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	X		
Other (specify					

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

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

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

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

Section 3: System Supported Activities

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

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): Driver license readers are used by facility security personnel to register visitors.			

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

Section 4: Purpose of the System

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

Purpose			
To determine eligibility		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	

For litigation	X	For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	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 both contractor and federal employee personnel designated to work with SWFSC. This information is collected for administration and business functions within SWFSC. Photographs that are taken are used specifically for identification badges for short term or temporary staff.

(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.

All information is stored on a restricted area of a shared drive accessible only by authorized personnel.

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):			

*In case of breach.

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

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

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NMFS Office of Science and Technology (NOAA4020). Network connection to S&T 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 NOAA4020.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.

X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.westcoast.fisheries.noaa.gov/fisheries/migratory_species/highly_migratory_species_logbooks.html http://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 federal employees and contractors, in writing. For responses to solicitations, notice is given on the request for information (RFI) or request for proposal (RFP).
	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.
	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: 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.
	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: 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 user information is maintained within NOAA Enterprise Messaging System (NEMS) database where users can review and update their contact information. Offerors will contact the office which issued the solicitation, with updated 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 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.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 9/11/2017 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

The data reside within the boundaries of the NOAA4020 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.

Local data is stored on a Windows network fileshare. 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, 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.

Section 9: Privacy Act

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

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/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 OPM/GOVT-1, General Personnel Records.
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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 schedule chapter 1505-11 and 1507-11
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

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

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

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

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
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 levels. *(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 employees and contractors.
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. There is no sensitive PII collected from employees or contractors.
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 only used within the operations and management purposes.
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. The PII data that is used for operations and management purposes is stored on a central fileserver that is physically secured in the NOAA4930 LAN room and has access to data restricted to authorized staff only via Windows AD domain group permissions.
	Other:	Provide explanation:

Section 12: Analysis

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

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

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

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