U.S. Department of Commerce
NOAA

Privacy Impact Assessment
For the
NOAA4930 System
National Marine Fisheries Service (NMFS) – Southwest Fisheries Science Center

Reviewed by: Mark Graff, Bureau Privacy Officer or Designee

Approved by: Catrina D. Purvis, DOC Chief Privacy Officer

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2016.02.04 10:03:41 -05'00'

Date approved:

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

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

NOAA4930 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. These data are 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 are 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 impact level of this system is moderate.

Section 1: Information in the System

1.1 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. Alien Registration		i. Financial Account	
b. Taxpayer ID		f. Driver's License		j. Financial Transaction	
c. Employee ID		g. Passport		k. Vehicle Identifier	
d. File/Case ID		h. Credit Card		l. Employer ID Number	
m. Other identifying numbers (specify): Vessel identifier, processor identifier					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	

f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Business sales information including dates, buyers, sellers, amounts, and prices.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		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		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

1.2 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):					

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		Public Media, Internet		Private Sector	X
Commercial Data Brokers					
Other (specify):					

Section 2: Purpose of the System

2.1 Indicate why the PII/BII in the system is being collected, maintained, or disseminated. Check all that apply.

Purpose			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities	X	For intelligence activities	
Other (specify): In compliance with federal and international mandates	X		

Section 3: Use of the System

3.1 Provide an explanation of how the bureau will use the PII/BII to accomplish the checked purpose(s), e.g., to verify existing data. Describe why the PII/BII that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and further the mission of the bureau and/or the Department. Indicate if the PII/BII identified in Section 1.1 of this document is in reference to a federal employee/contractor, member of public, foreign national, visitor or other (specify).

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.

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. Information is collected from members of the public.

Section 4: Information Sharing

4.1 Indicate with whom the bureau intends to share the PII/BII in the system and how the PII/BII will be shared.

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

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

Section 5: Notice and Consent

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

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 6.	
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.
	No, notice is not provided.	Specify why not:

5.2 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.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

5.3 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.

	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

5.4 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.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 6: Administrative and Technological Controls

6.1 Indicate the administrative and technological controls for the system. Check all that apply.

X	All users signed a confidentiality agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff received training on privacy and confidentiality policies and practices.
X	Access to PII/BII is restricted to authorized personnel only.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization: 8/26/2015
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST 800-122 recommended security 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.
	Other (specify):

Section 7: Privacy Act

7.1 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. Provide the system name and number: Fishermen's Statistical Data--COMMERCE/NOAA-6.

	Yes, a system of records notice has been submitted to the Department for approval on (date).
	No, a system of records is not being created.

Section 8: Retention of Information

8.1 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:

Appendix A

In the first column, please complete as "in place," "POAM ID # ____," "N/A," or "RA (Risk Accepted."

In Place	**Access Enforcement (AC-3)**. Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
In Place	**Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII.
In Place	**Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
In Place	**Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII.
N/A	**User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.
In Place	**Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).
In Place	**Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
In Place	**Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
In Place	**Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.
In Place	**Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm).
In Place	**Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled.
In Place	**Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
In Place	**Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas.
In Place	**Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.
In Place	**Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII.
In Place	**Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape.
In Place	**Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events.

This page is a supplement for item 6.1. Upon final approval, this page must be removed prior to publication of the PIA.

Points of Contact and Signatures

Information Technology Security Officer
Name: Bill Stearn
Office: NOAA/NMFS OCIO
Phone: 301-427-8813
Email: bill.stearn@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.

Signature: Digitally signed by STEARN.WILLIAM.IVAN.1384494222 Reason: As the NMFS IT Security Program Manager, I have reviewed this document.

Date signed: Date: 2015.10.23 07:09:19 -04'00'

System Owner
Name: Samer Tominna
Office: NOAA Southwest Fisheries Science Center
Phone: 858-546-7055
Email: samer.tominna@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.

Signature: TOMINNA.SAMER.FAWZI.1231763593 Digitally signed by TOMINNA.SAMER.FAWZI.1231763593 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=TOMINNA.SAMER.FAWZI.1231763593 Date: 2015.10.22 17:26:13 -07'00'

Date signed:

Information System Security Officer
Name: Rich Cosgrove
Office: NOAA Southwest Fisheries Science Center
Phone: 858-546-7057
Email: rich.cosgrove@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.

Signature: COSGROVE.RICHARD.E.III.1365890672 Digitally signed by COSGROVE.RICHARD.E.III.1365890672 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=COSGROVE.RICHARD.E.III.1365890672 Date: 2015.10.13 13:06:47 -07'00'

Date signed: 10/13/2015

Data Owner
Name: John Childers
Office: NOAA Southwest Fisheries Science Center
Phone: 858-546-7192
Email: john.childers@noaa.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.

Signature: John Childers Digitally signed by John Childers DN: cn=John Childers, o=Southwest Fisheries Science Center, ou=SWFSC, email=john.childers@noaa.gov, c=US Date: 2015.10.13 13:13:20 -07'00'

Date signed: 10/13/2015

NOAA Privacy Officer or Designee
Name: Sarah Brabson
Office: NOAA Office of the Chief Information Officer
Phone: 301-628-5751
Email: sarah.brabson@noaa.gov

I certify that the PII/BII processed in this system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2015.10.26 11:17:35 -04'00'

Date signed:

DOC Chief Privacy Officer
Name: Catrina Purvis
Office: Office of Privacy and Open Government
Phone: 202-482-1190
Email: CPurvis@doc.gov

I certify that I have reviewed this PIA for compliance with DOC policy to protect privacy and authorize for this PIA to be published on DOC websites.

Signature: Catrina D. Purvis Digitally signed by Catrina D. Purvis DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US Date: 2016.02.04 10:03:06 -05'00'

Date signed:

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.