Version Number: 01-2017

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Fisheries Permit and Landings Reporting System

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
Date: 2019.09.23 18:08:08 -04'00' 9/19/2019

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

U.S. Department of Commerce Privacy Impact Assessment
National Fishing Permit and Landings Reporting System

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

- The National Fishing Permit and Landings Reporting System (NFPLRS) allows members of the recreational and commercial fishing communities to acquire permits for certain species of fish, renew those permits, report catch/landings, and access a library of related information (e.g., online brochures). The system also provides an information source to NMFS through real-time reports accessible via web browsers.

- The secondary function in the system is Electronic Monitoring (EM). EM consists of monitoring catch/landings via video footage. The EM services support catch/landings data retrieval, catch/landings data analysis/review, and on-land data storage in order to support a program for approximately 135 vessels.

The system is part of the Office of Sustainable Fisheries and we coordinate as needed with the Office of Law Enforcement, and the Office of Financial Services, which calculates applicable permit fees.

- Users include the general public, NMFS staff and customer service staff.
- Supported applications include excel spreadsheets, PDF files, database development and management, electronic mail, and web server applications.

The major functions the system provides are:

- Allow constituents to apply for and renew permits for Highly Migratory Species, Swordfish, and/or Atlantic tunas
- Accept reports of bluefin tuna, swordfish, and billfish landings
- Provide the public timely information regarding fisheries regulations
- Provide the public documents and forms related to fisheries activities and permitting
- Provide NMFS staff and customer service staff administrative access to permits
- Provide NMFS staff access to update information on the NFPLRS website.
- Provide Enforcement agents access to permit status
- Provide NMFS staff with statistical reports on permit holdings and landings
- Support dealer reporting Fax functionality
- Provide users access to EM catch/landing footage and data
- Support fee collection

Major Functions/Applications
The NFPLRS integrates three functional mission applications.

Web Application
The NMFS Permit Web Site application provides general information about permits as well as a means to apply for HMS, Swordfish, and/or Atlantic tunas permits online. In addition, the system

provides general documentation and guidance. The system also accepts information regarding HMS catch/landings. The web site is accessible from Internet and was developed using JAVA. The NMFS Permit Web Site application stores data in the NFPLRS Database.

EM Data Review Application

EM Data Review Application (DRA) is web-based application for reviewing videos and metadata captured from fishing vessels. The video footage captures only data related to fish caught/landed. This allows NOAA4011 to monitor fishing activities of Atlantic Tunas Longline permit holders. The data is stored in Amazon Web Services (AWS) GovCloud S3 and AWS RDS database. Prior to uploading files to AWS, the videos go through a Data Pre-processing System (DPS). DPS is located at ERT Office at Suite 100A, 8380 Colesville Road, Silver Spring, MD 20910.

Database

The NMFS Permit Web Site application stores Permit and Catch/Landings data in the NFPLRS Database. The NMFS EM application stores catch/landings monitoring data in the AWS GovCloud as well. The database management system used is Oracle 11g for Windows. The NFPLRS Database subsystem consists of the COTS DBMS (Oracle) as well as the tables, stored procedures, and constraints that make up the database application. These Database servers are virtual machines are secured and managed by AWS's Platform as a Service (PaaS) cloud service offering.

Permit data is shared internally with NOAA NMFS/ Southeast Regional Office (SERO)/ Northeast Regional Office (NERO) and externally with Atlantic Coastal Cooperative Statistics Program (ACCSP). This system uses permit data to validate trip level reports.

Authorities: This data allows NMFS to manages living marine resources under U.S. jurisdiction under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the Marine Mammal Protection Act, Atlantic Tunas Convention Act (ATCA), the Endangered Species Act (ESA), and the Highly Migratory Species Fishery Management Plan, as well as be compliant with international obligations pursuant to the International Commission for the Commission of Atlantic Tunas (ICCAT).

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, and there is not 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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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): Information is captured about the vessel and landings. Data includes all information is listed below:

- Owner's Name
- Owner's Address
- Owner's Telephone Number
- Owner's Email Address
- U.S. Coast Guard documentation number and/or state registration number for the vessel
- Vessel name
- home port city & state
- principal port city & state
- length in feet
- year built
- crew size
- construction (e.g., wood)
- gross tonnage
- propulsion (e.g., gasoline)
- main engine horsepower
- hold capacity in pounds (if applicable)
- Fees collected
- Dealer name
- Atlantic Tunas Dealer Permit Number issued by Greater Atlantic Region
- Permit category to which landing is assigned
- Record ID
- Date fish was landed
- Type of gear used to catch fish
- Length of fish measured in inches
- Round weight (w/ head, fins & guts) in lbs,
- Dressed weight (head, fins, and guts removed) in lbs
- Unique tag number of each fish
- City and State where fish were landed
- Area where fish was caught
- Total amount of fish caught
- Price per pound for both round and dressed weight
- Paid under consignment or on dockside basis
- Grade for freshness , fat, color, shape
- Destination of fish
- Date landing report submitted

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	X	c. Date/Time of Access	X	e. ID Files Accessed	

b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify): Error message					

Other Information (specify)

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		Online	X
Telephone	X	Email			
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application X*					
Other (specify): * Permits site is hosted by a NOAA contractor: https://hmspermits.noaa.gov/					

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

Data is enter into system be primary permit holder or the authorized representative. Information can be updated by contacting customer service. The yearly renewal process includes an option for the primary permit holder or the authorized representative to update some permit holders data (eg. address, telephone number).

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. 0648-0327 and 0648-0328
	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): Data files are used in an Oracle database (AWS RDS) and videos files of fish are stored on a file server (AWS S3).			

	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	X	Electronic purchase transactions	
Other (specify):			

	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	
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	X	For employee or customer satisfaction	X

For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): The system was developed to make it easier for vessels to apply for and obtain permits and to report landings.			

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).

The permit and catch reporting data are used to comply with MSA.
The electronic monitoring videos are used to meet the needs of the observer program.
This information is collected from members of the public.

5.2 Describe any potential threats to privacy 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.)

Accidental or intentional discloser of data
An authorized user may intentionally or unintentional disclose data to unauthorized persons. To mitigate this threat, annual security awareness training and job function is a mandatory requirement. Additionally user activity is monitored for abnormal behavior.

Unauthorized access to data
A perpetrator may breach supporting applications to gain access to the network and data. To mitigate this threat, a continuous monitoring program is place. The program includes vulnerability management activities such as code reviews and vulnerability scanning, compliance audits and risk management.

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

*For criminal law enforcement.

	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. Connected system have restricted access to only the data authorized. The required data is extracted and placed in a different secure container for each connected system. The secure container is restricted by IP address and requires authentication. The data extract process is automated and run on a schedule.
	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	X*	Government Employees	X
Contractors	X		
Other (specify):			

*Permits Web site only.

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: _____.	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the permit application. SAAD: A supervisor provides written notice of employee account set-up, explaining the purpose for providing the PII.
	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: Applicants can choose to not complete an application and thereby forgo fishing privileges requiring the permit. The permit application states that the information is required for review of the application. SAAD: An employee can respond in writing to the supervisor that he/she declines to provide the PII, but this would affect employment, as an account is needed to perform the work.
	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 data that is being collected is used and analyzed for management purposes. There is only one purpose for this data collection, as stated on the application. Thus, if not consenting to the stated purpose, the applicant would not complete the application. SAAD: an employee could respond to the supervisor in writing that he/she does not consent to the use of the information provided for account set-up, but there is only the one use.
	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: If users want to know what data is being stored, they can request it via the online Feedback Entry form at http://hmspermits.noaa.gov/feedback. Users also have the ability to update their own information via the website, per

		website instructions. Employees can provide their supervisor or the system administrator with changes to their PII.
	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.
	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:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): September 17, 2018 ☐ 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 supporting 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 ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Contract with Web Master includes FAR Part 24, regarding PII collected its ownership.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

PII is stored in an Oracle database hosted in Amazon GovCloud Web Service (AWS). Access to the database is restricted to the Permits application webserver and via AWS administrative console. Database connection is open only to the internal network. Access to the AWS console is restricted to only system administrators and requires multifactor authentication (password and PIN). Webserver access utilizes SSL certificates using TLS protocol and strong cipher suites. All access to shared read-only data is restricted by source IP address and requires public/private key pairs. As part of our continuous monitoring activities, access to data is logged and reviewed periodically. Additionally, scans are executed to check vulnerabilities and weakness in the system.

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). This information collection is included in a comprehensive NMFS Permits and Registrations System of Records Notice (SORN), COMMERCE/NOAA-19, Permits and Registrations for United States Federally Regulated Fisheries.
	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. 1504 Fishery Management and Coordination Files. These files relate to programs to coordinate plans and research of the Federal Government in the area of fisheries management with those of the states; to obtain maximum uniformity of regulations; to institutionalize cooperation; to issue permits to foreign and domestic fishing vessels; and award related grants
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

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

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same 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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals are not easily identifiable.
X	Quantity of PII	Provide explanation: There is a significant quantity in that each permit application contains some PII; however, the PII in these records does not easily identify individuals.
X	Data Field Sensitivity	Provide explanation: As per NIST 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories", the highest level based on the information types captured is Moderate. The information collected and stored in NOAA4011 system is non-sensitive PII related to vessel and owner information. The information includes: • Owner Name • Address • Email Address • Telephone Number • Vessel Name • Vessel ID Video footage of fishing activities (not showing individuals) are also collected and stored for audit and enforcement purposes.
	Context of Use	Provide explanation:

	Obligation to Protect Confidentiality	Provide explanation: Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801, Section 402b.
	Access to and Location of PII	Provide explanation:
	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 data collected has been reduced and the stored data has only limited non-sensitive PII. The data is needed to support NOAA4011 mission. PII data in encrypted in-storage and in-transit.

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.