

**U.S. Department of Commerce**  
**NOAA**



**Privacy Threshold Analysis**  
**for the**  
**National Fisheries Permit and Landings Reporting System**  
**(NFPLRS)**

**U.S. Department of Commerce Privacy Threshold Analysis**  
**National Marine Fisheries Service/National Fisheries Permit**  
**and Landings Reporting System**

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

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system and its purpose:**

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

The National Fishing Permit and Landings Reporting System (NFPLRS), designated as NOAA4011 is a major application with a moderate system security categorization. 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.

*b) System location*

NOAA4011 is a hosted application environment located in the Amazon Web Services (AWS) GovCloud and at ERT Office in Silver Spring, MD 20910.

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

The following systems have interconnections with NFPLRS, but are outside of the system boundary:

- The Payment Gateway (real-time processing of credit card transactions) at Pay.gov

- The National Marine Fisheries Service (NMFS) Northeast Fisheries Science Center (NEFSC) pulls data from the NFPLRS
- The NMFS pulls data from the NFPLRS
- The Atlantic Coastal Cooperative Statistics Program (ACCSP) pulls data from the NFPLRS
- NMFS pulls data from Commission for the Conservation of Antarctic Marine Living Resources (CCAMLR)
- The NMFS Southeast Regional Office (SERO) pushes data to NFPLRS.

*d) The purpose that the system is designed to serve*

NFPLRS a hosted application environment located in the Amazon Web Services (AWS) GovCloud and at ERT Office in Silver Spring, MD 20910. NOAA4011 provides a secure application and hosting environment for National Marine Fisheries Services (NMFS) applications, content, and utilities that are used to deliver content and applications to an audience made up of employees, contractors, partners, and the general public worldwide. The system supports the headquarters Sustainable Fisheries Division, Enforcement and Financial offices. Users include the general public, fish dealers, NMFS staff and customer service staff. The hosted applications provide real-time reports for monitoring of compliance with requisite laws and regulations.

*e) The way the system operates to achieve the purpose*

The hosted applications provide real-time reports for monitoring of compliance with requisite laws and regulations. The system host the following applications:

**1. National Fisheries Permit and Landings Reporting System (NFPLRS)**

The NFPLRS allows members of the recreational and commercial fishing communities to acquire permits for certain highly migratory species (HMS), renew those permits, report landings and/or catch, and access a library of related information (e.g., online brochures).

**2. Electronic Monitoring Data Storage and Processing (EM)**

EM Data Storage and Processing is a web-based application for reviewing videos and metadata captured from fishing vessels. The video footage only captures data related to fish caught/landed.

**3. Trade Monitoring System (TMS)**

The National Seafood Inspection Laboratory's (NSIL) Trade Monitoring Program is responsible for collecting, collating, editing, and entering all of the catch/trade documents for swordfish, frozen bigeye tuna, Atlantic, Pacific, and Southern Bluefin tuna.

**4. International Affairs Information Capture and Reporting System (IAICRS)**

The National Marine Fisheries Service, Office of International Affairs and Seafood Inspection Program (IASI) is responsible for implementing Congressionally mandated programs to strengthen leadership in international fisheries and protected species conservation and management.

### **5. Species Substitution Screening Tool**

The purpose of the Species Substitution Screening Tool application is to combat the current trend of seafood species substitution, the National Seafood Inspection Laboratory (NSIL) set out to develop a rapid and reliable software screening method for species identification.

*f) A general description of the type of information collected, maintained, use, or disseminated by the system*

NFPLRS collects the following information from users in the process of submitting a permit request

#### Vessel Information

- 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
- System Administrators Information
- Name

g) *Identify individuals who have access to information on the system*

NMFS employees, contractors, partners, and the general public worldwide.

h) *How information in the system is retrieved by the user*

NFPLRS web-based application applications allows access to the environment remotely via Hypertext Transfer Protocol Secure (HTTPS) over the Internet. Privilege user access servers requires administrators to first connecting through virtual private network VPN then SSH to specific servers. Additionally, privilege user access to manage of Amazon GovCloud services is done via HTTPS.

i) *How information is transmitted to and from the system.*

The information is transmitted to and from the system through the Internet using VPN, HTTPS, and SSH secure protocols.

Questionnaire:

1. What is the status of this information system?

- This is a new information system. *Continue to answer questions and complete certification.*
- This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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

This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

This is an existing information system in which changes do not create

new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).  
*Continue to answer questions and complete certification.*

Version Number: 01-2019

\_\_\_\_\_ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

\_\_\_\_\_  Yes. (Check all that apply.)

Activities			
Audio recordings		Building entry readers	
*Video surveillance	X	Electronic purchase transactions	
Other (specify):* Video footage of fishing activities aboard the vessel is recorded for later review for compliance monitoring.			

\_\_\_\_\_ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

\_\_\_\_\_  Yes, the IT system collects, maintains, or disseminates BII.

\_\_\_\_\_ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

\_\_\_\_\_  Yes, the IT system collects, maintains, or disseminates PII about:  
(Check all that apply.)

DOC employees  
 National Institute of Standards and Technology Associates

Version Number: 01-2019

Contractors working on behalf of DOC  
 Other Federal Government personnel  
 Members of the public

No, this IT system does not collect any PII.

*If the answer is "yes" to question 4a, please respond to the following questions.*

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

N/A
-----

N/A
-----

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

Version Number: 01-2019

***If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.***

# CERTIFICATION

Version Number: 01-2019

X I certify the criteria implied by one or more of the questions above **apply** to the **National Fishing Permit and Landings Reporting System (NFPLRS)** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

       I certify the criteria implied by the questions above **do not apply** to the **National Fishing Permit and Landings Reporting System (NFPLRS)** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

## Information System Security Officer (ISSO) or System Owner (SO):

Name:    Doug Brackett    Date:    5/5/2020   

Signature of ISSO or SO: \_\_\_\_\_

## Information Technology Security Officer (ITSO):

Name:    Catherine Amores    Date: \_\_\_\_\_

Signature of ITSO: \_\_\_\_\_

## Privacy Act Officer (PAO):

Name: \_\_\_\_\_ Date: \_\_\_\_\_

Signature of PAO: \_\_\_\_\_

**Co-Authorizing Official (AO):**

Version Number: 01-2019

Name: \_\_\_\_\_ Jenni Wallace \_\_\_\_\_ Date: \_\_\_\_\_

Signature of Co-AO: \_\_\_\_\_

**Co-Authorizing Official (AO):**

Name: \_\_\_\_\_ Roy Varghese \_\_\_\_\_ Date: \_\_\_\_\_

Signature of Co-AO: \_\_\_\_\_

**Bureau Chief Privacy Officer (BCPO):**

Name: \_\_\_\_\_ Mark Graff \_\_\_\_\_ Date: \_\_\_\_\_

Signature of Co-AO: \_\_\_\_\_