Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA4011
National Fisheries Permit and Landings Reporting System
(NFPLRS)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NMFS/NFPLRS

Unique Project Identifier: NOAA4011

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: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The National Fishing Permit and Landings Reporting System (NFPLRS) allows members of the recreational and commercial fishing communities to acquire and renew permits, and report landings data. The system supports the National Marine Fishery Services NMFS Sustainable Fisheries Division, Enforcement and Financial offices.

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 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.

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.

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:

- NOAA Greater Atlantic Regional Fisheries Office (NOAA4100) pulls data from the NFPLRS
- NMFS Office of Science & Technology (NOAA4020) Pulls data from NFPLRS
- NFPLRS pulls data from NOAA NMFS Vessel Monitoring System (NOAA4000)
- NOAA National Permit Services (NOAA4000) pulls data from the NFPLRS
- NOAA Southeast Regional Office (NOAA4300) pushes data to NFPLRS
- The Payment Gateway (real-time processing of credit card transactions) at Pay.gov
- 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)

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. Applications hosted in NFPLRS provide data for law enforcement actions, customer satisfaction activities, and to promote information sharing in support of permit and landing activities.

e) The way the system operates to achieve the purpose

NFPLRS a hosted application environment located in the Amazon Web Services (AWS) GovCloud and at ERT Office at Suite 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. 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. The Catch Shares Online System (CSOS)

The Catch Shares Online System (CSOS) supports NOAA Catch Share Programs by allowing flexible and accountable monitoring of fishing activates for meeting the national goal for rebuilding and sustaining our fishery resources. CSOS collects, stores, and designates PII and BII data to verify catch information.

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

NFPLRS collects the following information from the public (owner and operators of fishing vessels) in the process of submitting a permit request and reporting landings. Data collected is share within NOAA and with ACCSP. Data is transmitted via secure connection using VPN, HTTPs, and SSH

- Name
- Address
- Telephone Numbers
- Email address
- Vessel Registration Number
- Vessel Name
- Vessel Type and Characteristics (such as length, year built, crew size, etc.)
- Vessel Permit Number
- Fee and Payment
- Vessel Landing and Catch Information (such as date, location, weight, length, etc.)

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

Personnel that has access to the system are law enforcement, NOAA employees and contractors who operate the system such as customer service representatives, system administers, and data scientists. Additionally, public user have access to their individual data only.

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. Status of the Information System

1a. 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.*

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):					

____ 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.

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

X___ No. This is not a new information system.

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.

_X___ 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.)."

X___ 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."

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

_X_ DOC employees
_X_ Contractors working on behalf of DOC
____ Other Federal Government personnel
_X_ 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 collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

_X_ 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?

_X_ 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.

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

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 PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

X The criteria implied by one or more of the questions above **apply** to the NOAA4011 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the NOAAXXXX and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer Name: Wilbert Francis Office: NOAA4011 Phone: 202-427-6397 Email: Wilbert.Francis@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: FRANCIS.WILBERT.R.1463197551 Digitally signed by FRANCIS.WILBERT.R.1463197551 Date: 2022.07.04 14:08:45 -04'00' Date signed:	**Information Technology Security Officer** Name: Doug Brackett Office: NOAA/NMFS/OCIO Phone: 301-427-8815 Email: Doug.Brackett@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: Digitally signed by BRACKETT.DOUGLAS.HOWE.1365899564 Date: 2022.07.05 12:16:34 -04'00' Date signed:
Privacy Act Officer Name: Robin Burress Office: NOAA/OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2022.07.18 08:41:16 -04'00' Date signed:	**Authorizing Official** Name: Kelly Denit Office: NOAA/NMFS/Office of Sustainable Fisheries Phone: 301-427-8517 Email: Kelly.Denit@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system Signature: Digitally signed by DENIT.KELLY.L.1365842074 Date: 2022.07.05 09:25:25 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA/OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.07.19 07:46:08 -04'00' Date signed:	**Co-Authorizing Official** Name: Nancy Majower Office: NOAA/NMFS/OCIO Phone: 301-427-8811 Email: Nancy.Majower@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system Signature: REID MAJOWER.NANCY.1365836694 Digitally signed by REID MAJOWER.NANCY.1365836694 Date: 2022.07.15 13:27:41 -04'00' Date signed: