Privacy Threshold Analysis
for the
National Fisheries Permit and Landings Reporting System
(NFPLRS)
U.S. Department of Commerce Privacy Threshold Analysis

National Fisheries Permit and Landing Reporting System (NFPLRS)

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 information technology (IT) system. This PTA is primarily based on 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:
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 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 NMFS Office of Management and Budget, 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 provide are:

- Allow constituents to apply for and renew permits for highly migratory species (HMS), swordfish, and 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
• 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 NFPLRS website application provides general information about permits and facilitates online applications for HMS, swordfish, and Atlantic tunas permits. 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 website application stores data in the NFPLRS Database.

EM Data Review Application
EM Data Review Application (DRA) 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. This allows NFPLRS to monitor fishing activities of Atlantic tunas longline permit holders. The data is stored in Amazon Web Services (AWS) GovCloud utilizing S3 and AWS RDS database services. Prior to uploading files to AWS, videos go through a data pre-processing system (DPS). The servers hosting the DPS are located at ERT Office at Suite 100A, 8380 Colesville Road, Silver Spring, MD 20910.

Database
The NFPLRS and EM DRA applications both store data in AWS GovCloud. The database management system used is Oracle 11g for Windows. The database consists of tables, stored procedures, and constraints. These database servers are virtual machines that are secured and managed by AWS’s Platform as a Service (PaaS) 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 manage 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).

Questionnaire:

1. What is the status of this information system?

   ____ This is a new information system. Continue to answer questions and complete certification.

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

   ____ This is an existing information system in which changes do not create new privacy risks. Note (Existing PTA requires that questions 2, 3 and 4 are reviewed and addressed for accuracy as well)

   Changes That Create New Privacy Risks (CTCNPR)

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

   ____ X This is an existing information system in which changes do not create new privacy risks. Note (Existing PTA requires that questions 2, 3 and 4 are reviewed and addressed for accuracy as well)

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. Please describe the activities which may raise privacy concerns.

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

   • Vessel Information
     • Owners Name
     • Owners Address
     • Owners Telephone Number
o Owner’s email address
o U.S. Coast Guard documentation number and/or state registration number for the vessel
o Vessel name
o Home port city & state
o Principal port city & state
o Length in feet
o Year built
o Crew size
o Construction (e.g., wood)
o Gross tonnage
o Propulsion (e.g., gasoline)
o Main engine horsepower
o Hold capacity in pounds (if applicable)

Video footage of fishing activities.

___ 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 about: (Check all that apply.)

___ X ___ □ Companies

___ □ Other business entities

___ □ No, this IT system does not collect any BII.
4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: “The term ‘personally identifiable information’ refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc...”

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

___ □ DOC employees
___ □ Contractors working on behalf of DOC
__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 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.

4c. 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, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.
CERTIFICATION

__X__ Yes □ No I certify the criteria implied by one or more of the questions above apply to the NFPLRS and as a consequence of this applicability, a NMFS Permits PIA which includes this system’s information has been submitted to DOC for review.

□ Yes __ No I certify the criteria implied by the questions above do not apply to the [IT SYSTEM NAME] 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: ________________________________

Signature of ISSO or SO: ________________________________ Date: __________

Information Technology Security Officer (ITSO):

Name: ________________________________

Signature of ITSO: ________________________________ Date: __________