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

Privacy Threshold Analysis
for the
NMFS Southeast Region Office Local Network
NOAA4300
U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NOAA4300

Unique Project Identifier: 006-48-01-14-02-3305-00

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: Provide a general description of the information system in a way that a non-technical person can understand.

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 Southeast Regional Office NOAA4300 system functions as the overall office automation support system for the NOAA/NMFS offices in St. Petersburg, Florida. It provides access to automated systems typically found in administrative offices within the federal government. It supports all offices within the Southeast Region (SER) which include the Regional Administrator's Office; Operations, Management & Information Services Office; State/Federal Liaison Office; Sustainable Fisheries Division; Protected Resources Division; and, Habitat Conservation Division. The system also supports non-SERO offices located in St. Petersburg including NOAA SE Office of General Counsel (GCSE), Damage Assessment Center (DAC), and NMFS SE Financial Services. The information for these offices is covered by the NOAA4000 and NOAA4020 Privacy Impact Assessments.

NOAA4300 collects and stores information that consists of basic identifying information about employees, contractors, volunteers, and partner agency staff who are facility occupants or system users. The information is maintained as a supplement to other records for purposes of human resource activities, Continuity of Operations (COOP) execution, and performing other related administrative tasks, e.g., training, travel, awards, facility management, and NOAA training requirements in support of individual job duties and requirements.

Information collected to manage security clearances may include: full name, home address, home phone number, e-mail address, educational background, SSN, and employment history. Information maintained for COOP and other administrative processes includes: full name, grade level and/or position within the organization, role/responsibility, home address, home phone number, and mobile phone number.

NOAA4300 also collects permit-related data. In order to manage U.S. fisheries, the NOAA National Marine Fisheries Service (NMFS) requires the use of permits or registrations by
participants in the United States. This information consists of contents of permit applications and related documents, such as permit transfers and percentage of ownership in a corporation. A typical transaction is an initial or renewal permit application: the permit holder or applicant completes an application downloaded from the applicable NMFS Web site or obtained through visiting the Permits office, submits it to the applicable office by mail or in person, along with any required supporting documentation and proof of payment (through pay.gov), and receives a new permit once approved by NMFS. For permit transfers within a family, marriage certificates, divorce decrees, and/or death certificates may be required. Tax Identification Numbers allow positive identification for cost recovery billing of IFQ holders.

In addition, information may be collected to facilitate public education, outreach, or collaboration with partners on research/conservation projects. For these activities, the name, address, e-mail address, telephone number, and other non-sensitive organizational information may be temporarily stored. These individuals, businesses or organizations may be workshop participants, business contacts, members of mailing lists, etc. In all cases the information is voluntarily submitted.

NOAA4300 employs contractors in a variety of roles in order to support its mission, primarily in the Habitat/Sustainable Fisheries/Protected Resources branches. All contractors undergo the same security clearance process as Federal Government employees. Contractors do not have access to sensitive PII.

Access to information collected and maintained within the system boundary of NOAA4300 is determined by the individual’s job duties and role in the organization. Any request involving the sharing of any sensitive data, whether internal or external, must be documented in a Memorandum of Understanding (MoU) or Interconnection Security Agreement (ISA), and approved by each system’s Authorizing Official. Information is shared within the Southeast Region in order to coordinate monitoring and management of sustainability of fisheries and protected resources. Information may also be shared at the state or interstate level for the purpose of determining an applicant’s eligibility when data collected by the state affects permit eligibility. Sources of information include the permit applicant/holder, other NMFS offices (Such as the Office of General Counsel and the Southeast Division of the NMFS Office of Law Enforcement), the U.S. Coast Guard and the Department of Justice.

NOAA4300 will have a data sharing agreement with the Atlantic Coastal Cooperative Statistics Program (ACCSP). The ACCSP requires a unique identifier for each for-hire SER Permit holder in order to validate landing reports. ACCSP will provide an algorithm to NMFS, who will run the algorithm for each applicable permit holder in order to generate the identifier, and then share the encrypted identifier with ACCSP. Although the identifier will be comprised of fragmentary PII (birthdate, email address, and phone number), there will be no exploitable data contained in

ACCSP was established through NOAA’s provision for Fishery Information Networks (FIN) to address data deficiencies that constrained the management of fisheries along the Atlantic coast. With the proposed implementation of the South Atlantic Fishery Management Council’s electronic logbook reporting for the for-hire sector by the National Marine Fisheries Service (NMFS), there is a need for efficient and cost-saving data collection. The implementation team
for the for-hire reporting investigated numerous options for data housing, with the decisive elements including 1) accessibility to NMFS staff and program patterns, 2) flexibility in database design, 3) integration with other agency programs (e.g., state programs, NMFS Mid-Atlantic, VMS), 4) staffing needs to develop and maintain the system, and 5) estimated initial and annual costs.

Data housing solutions were limited to those either run by the government or funded through the government, such as FIN, as these groups would be most experienced with confidential data requirements. The Implementation team reviewed the various options and settled on using ACCSP as the first line choice for a variety of factors, with top factors including costs, flexibility, and integration. ACCSP has an existing data warehouse structure and data collection system that will meet the needs of for-hire electronic logbook reporting, saving NMFS significant initial costs ($500 K to $1.5 M) and annual costs ($120K to $240K for software renewals and staffing). The ACCSP system is a flexible system that has the ability to integrate with various other NMFS and state agencies. Furthermore, ACCSP has a long-standing working relationship with NMFS and already is the first receiver of federal dealer data supplied by the Gulf and South Atlantic states. ACCSP has also been developing front-end user tools and interfaces that allow for a free mobile app to be available for any participant to use to enter the required data elements.

For this system to work effectively, ACCSP will need to link the data collected from electronic reports with data contained within NMFS permit system. In addition, the ACCSP would need to establish the linkage at the time of the creation of user accounts in ACCSP. The information needed to successfully link the two, in the absence of using a Tax ID Number (SSN or FEIN), would be a unique identifier generated from fragments of each permit holder's name, email address, birth date, and phone number. This unique identifier would be generated using an algorithm supplied by ACCSP. Without providing ACCSP access to this information, there is a high likelihood that NMFS will not be able to move forward with using the ACCSP as the data warehouse, which would significantly delay implementation of the reporting program as well as cost NMFS significant money.

The overall legal authority for collection of information addressed in this PIA is:
5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.


Permit and registration data are collected from individuals under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Atlantic Coastal Fisheries Cooperative Management Act, the Atlantic Tunas Convention Authorization Act, the Northern Pacific Halibut Act, international fisheries regulations regarding U.S. Vessels Fishing in Colombian Treaty Waters, the Marine Mammal Protection Act, the Endangered Species Act and the Fur Seal Act. The authority for the mandatory collection of the Tax Identification Number is 31 U.S.C. 7701.
NOAA4300 is a FIPS199 Moderate system.

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.

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

   ___ 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 or later). Continue to answer 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.

   ___ X___ Yes. Please describe the activities which may raise privacy concerns. There are readers for entrance to secure areas.

   ___ 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.)

__X__ DOC employees
__X__ 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 ___ I certify the criteria implied by one or more of the questions above apply to NOAA4300 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 NOAA4300 and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):
Eric Barton – ISSO, NOAA4300

Signature of ISSO or SO: BARTON.ERIC.H.136
5837321
Date: 10/9/2018

Name of Information Technology Security Officer (ITSO):

Signature of ITSO: AMORES.CATHERINE.S
OLEDAD.1541314390
Date: 10/9/2018

Name of Authorizing Official (AO):
Dr. Roy Crabtree – Regional Administrator, NMFS Southeast Region

Signature of AO: CRABTREE.ROY.E.DR.136
Date: 10/9/2018

Name of Bureau Chief Privacy Officer (BCPO):
Mark Graff

Signature of BCPO: GRAFF.MARK.HYRUM.151
4447892
Date: 10/9/2018