

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



**Privacy Threshold Analysis  
for the**

**NOAA4020 - Science and Technology (S&T) Silver Spring**

## **U.S. Department of Commerce Privacy Threshold Analysis**

### **NOAA4020 - Science and Technology (S&T) Silver Spring**

**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:** The NOAA4020 Science and Technology (S&T) system functions as a general data processing system for NOAA and NMFS headquarters located in Silver Spring, MD. It provides resources to support scientific operations and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs. The user base of this system reaches across different headquarter offices and across regions and science centers within NMFS. Many of these automated systems are built in support of the NOAA Fisheries mission.

#### **1) International Trade Data System (ITDS)**

ST6 International Trade Data System (ITDS) is used to support a number of NMFS offices/programs to monitor imports of fisheries products. Types of BII data collected are name of business, address, contact information, and product information. The data is collected by U.S. Customs and Border Protection (CBP) provided to NMFS via SFTP for inclusion in the ITDS database. Reasons for the NMFS database:

- (1) The ITDS is an inter-agency, distributed system that allows businesses to submit trade data to a single agency (CBP). CBP then makes these data available to participating ITDS agencies via secure, system integration.
- (2) The NMFS component of the ITDS is an import monitoring system designed to improve the efficiency and accuracy of NMFS trade monitoring programs by utilizing the data and services provided by CBP via the national ITDS architecture. NMFS trade monitoring programs supported by the NMFS ITDS include the Antarctic Marine Living Resources (AMLR) program, the Highly Migratory Species (HMS) program, the Seafood Import Monitoring Program (SIMP), and the Tuna Tracking Verification Program (TTVP). The NMFS ITDS is also integrated with the NMFS National Permit System (NPS) to provide international trade permit data to NMFS trade monitoring programs and to CBP.

## **2) Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL)**

The Marine Recreational Information Program (MRIP) Extract, Transform and Load (ETL) system is a tool to collect and process recreational saltwater fishing license and registration data from the Atlantic and Gulf of Mexico coastal states for inclusion in the National Saltwater Angler Registry (NSAR). Types of PII collected include fishing license information, name, address, driver's license number, phone, email, and date of birth.

This section was changed to improve the clarity and accuracy of the text. Nothing significant changed on any of these applications. This does not impact our overall privacy risk as far as being a moderate FISMA system.

## **3) National Saltwater Angler Registry - NSAR**

The National Saltwater Angler Registry (NSAR) system serves as a consolidated phone book of the nation's recreational saltwater anglers. NSAR data is used to furnish frames for the MRIP surveys. Types of PII collected include fishing license information, name, address, driver's license number, phone, email, and date of birth.

## **4) NOAA Fisheries Committee on Scientific Stature. This is not an outside advisory committee.**

The NOAA Fisheries Committee on Scientific Stature (NFCSS) is a national-level performance Management Advisory Committee (PMAC) established to review the contributions, impact and stature of NOAA Fisheries Band IV and V non-supervisory research scientists. The NFCSS evaluates scientists whose primary responsibility is to conduct research and develop scientific products for resource management advice, other scientific advice, publications, and reports that represent new or more comprehensive understanding of a subject. The NFCSS members are Band V scientists, who are subject matter experts, from the regional science centers appointed to three-year terms by the respective regional Science Director. There is a website and database to manage and record the results of NFCSS member reviews conducted for the purpose of evaluating a scientist's credentials and contributions to allow them to be assigned to a higher pay Band without being a supervisor and to produce a standard report for the committee chair (OST Science Director). In 2014, OST upgraded the NFCSS website and database to enable password protected, role-based secure storage and retrieval of review package documents. Access to the database is restricted to the OST Science Director, the six regional Deputy Science Directors, one Band V research scientist from each regional science center, the NOAA Fisheries HR Business Partner, and the NFCSS database administrator and is provided by the NFCSS database administrator only at the request of the NFCSS Chair. Information collected: name, work contact information, letters of reference and curricula vitae, performance plan, science director memoranda and name of immediate supervisor. The administrator uploads copies of a memorandum from the NFCSS Chair to the Science Center director of staff being reviewed. The data (name, email, documents) for staff being reviewed are entered by their Deputy Science Director. The review comments are entered by the NFCSS members.

**5) Protected Resources National Inventory of Marine Mammals (NIMM) System.**

The National Inventory of Marine Mammals (NIMM) system maintains current and past data (it replaces previous inventory databases maintained by NMFS since the 1970s) on marine mammals under NMFS’ jurisdiction (dolphins, porpoises, whales, seals, and sea lions) held in permanent captivity for public display. In addition, NIMM includes information on marine mammals held in permanent captivity for scientific research, enhancement, and national defense purposes. NIMM includes beached/stranded marine mammals only if they have been deemed non-releasable and cannot be returned to the wild. NIMM allows marine mammal Owners and Facilities to enter inventory data directly into the online system. NIMM will eventually provide the public with real-time access to the national inventory. Types of BII collected include institution name, address, email, phone, and fax.

**6) NOAA Emergency Contact List**

The Emergency Contact List stores store contact information for ST staff and staff emergency contacts to be used in case of emergency. This is PII data.

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).

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

The NOAA4020 Science and Technology (S&T) system is a general support system for NMFS headquarters.

*b) System location*

NOAA4020 NMFS headquarters located in SSMC3 Room 12244 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)*

NOAA4020 is a subsystem of NOAA4000.

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

NOAA4020 provides resources to support scientific operation and research, data and information management, fisheries surveys, statistical analysis, stock assessments, socio-economic analysis, ecosystem management, other national program database and applications development, and management decisions needs.

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

NOAA4020 provides application servers, database servers, proxy servers, file servers, sftp servers to achieve its purpose.

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

NOAA4020 hosts databases and flat files containing fishery-dependent (commercial and recreational landings and effort) and –independent data, marine mammal data, environmental and habitat data, scientific operation and research data and information, fisheries surveys, statistical analyses, stock assessment data, and socio-economic data. This information support of the NOAA Fisheries mission.

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

The user base of this system reaches across different NMFS headquarters offices and across regions and science centers within NMFS. Users outside of NMFS, including other agencies, state, regional, and tribal partners, stakeholders, and the public can access selected information.

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

NOAA users login to the web based application within NOAA. External users access the information via public-facing, web-accessible applications and web sites.

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

The information is transmitted within NMFS via Local and Wide area Networks using secure connections. Information is transmitted to external users through secure internet connections.

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.*

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.*
- 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.*
- 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		Electronic purchase transactions	
Other (specify):			

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

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 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.

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.

***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 approved PIA must be a part of the IT system’s Assessment and Authorization Package.***

