

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



**Privacy Threshold Analysis
for the
NOAA4000 – Fisheries WAN and Enterprise Services**

U.S. Department of Commerce Privacy Threshold Analysis
NMFS/NOAA4000 – Fisheries WAN and Enterprise Services

Unique Project Identifier:

A. 006480200001230000	SISP	Seafood Inspection Services Portal
B. 006000351102004802000200	EDMS	*Electronic Document Management System
C. 006000316800004801140200	VMS	National Vessel Monitoring System
D. 006000316800004801140200	TRIDENT	TRIDENT
E. 006480200001230000	NRDA	National Resources Damage Assessment Database
F. 006480200001230000	RCDB	Restoration and Conservation Database
G. 006480200001230000	eAOP	Electronic Annual Operating Plan
H. 006480200001230000	MMHSRP	Marine Mammal Health and Stranding Response Program
I. 006480200001230000	GCLD	General Counsel Litigation Database
J. 006480200001230000	NPS	National Permits System
K. 006480200001230000	FOIA	eDiscovery Application (FOIA)
L. 006480200001230000	TIPS	Traceability Information Program for Seafood
M. 006480200001230000	ECO	Environmental Consultation Organizer
N. 006480200001230000	FSD	Financial Services Division
O. 006480200001230000	FWS	NMFS Federal Website
P.	UAS	Unmanned Aircraft System - OLE Data

Introduction: System Description

This system hosts several applications that collect, store and/or disseminate information, mainly on members of the public, including foreign national guests, and in some cases, NOAA staff and/or contractors. This system is located in NMFS headquarters in Silver Spring, MD.

- A. SISP - The Seafood Inspection Services Portal** - is a web-based application that captures information pertaining to the scheduling, tracking, and fee collections for seafood inspection activities. The SISP allows Seafood Inspection Program participants (Seafood Companies, Seafood Inspection Personnel, System Administrative Staff,

NOAA Finance (Billing Data)) to create an account, to update company information including multiple locations, to request certificates, inspections and contracts, and to review and pay invoices. We collect the information under the authority of Agriculture and Marketing Act of 1946 and Fish & Wildlife Act of 1956. Name, work email address, work address, and financial transaction are collected. We share the information with the private sector for invoicing and bill payment. **This application collects PII and BII.**

- B. EDMS – The Electronic Document Management System** – is a Web-based content management application that serves as a secure repository to archive various artifacts throughout their development life cycle. Authorized NMFS users (employees and contractors) can easily query this content management database, which has improved workflow. This application is a central resource for Habitat Division supervisors and staff for ongoing performance appraisal activity, and to assist in completing required personnel related forms that contains names, job descriptions, and GS level. EDMS also contains various legal documents/case files that may include SSN/Tax ID numbers. Information in EDMS is housed behind the network firewall. The collection of such information is authorized by **5 U.S.C. 1302. This application collects PII and BII.**
- C. VMS - The National Vessel Monitoring System** - program provides near-real time fishing vessel monitoring, control and surveillance throughout the U.S. Exclusive Economic Zone (EEZ). Continuous 24/7/365 monitoring supports compliance with marine and fishing regulations regarding open and closed seasons, closed areas, international boundaries and obligations, and overfishing. The onboard-enhanced mobile transceiver units (EMTUs) send position location information to NMFS, which is stored in a database and displayed on an electronic surveillance software, which is currently vTrack. The information obtained through VMS is evidentiary in nature and used to prosecute violations of fishery regulations in administrative and civil proceedings. The overall authority for federal fishery management is the **Magnuson-Stevens Conservation and Management Act (16 U.S. Code 1801 et. Seq.)**. Names, home telephone numbers, home email addresses and addresses for vessel operators are collected. Fisheries share the information with the U.S. Coast Guard, many coastal states' marine enforcement offices, the Navy, Immigration and Customs Enforcement, NMFS science centers, and NMFS fishery managers. **This application collects PII/BII.**
- D. TRIDENT** - Trident is a cloud based, case management system which allows sworn law enforcement officers, special agents, and other staff seamless electronic collaboration with internal team members and external partners, and the development of case documentation by providing the ability to view/share incident data that documents enforcement activities such as patrols, investigations, compliance assistance and education and outreach.

The information is used to document and track patrols, investigations and other enforcement activities in which U.S. laws and regulations as well as violations of

international agreements. Enforcement personnel develop domestic and international investigative case files that support prosecuting alleged violations; data and information from these files and data collected refers to businesses and members of the public.

This information is collected under the authority of the **Magnuson-Stevens Fishery Conservation and Management Act (16 U.S. Code 1801 et. Seq.)** and other laws under the purview of NOAA.

The Trident solution is a FedRAMP platform as a service (PaaS), private cloud, web accessible development environment, enabling the use of MicroPact's infrastructure and middleware services. The production environment consists of Tomcat/Apache web application server. Entellitrak is the thin client that manages the business logic, data storage and interface presentation. Backend storage are Oracle and SQL Server. The system is integrated with the NOAA Office General Counsel system Justware. **This application collects PII and BII.**

- E. **NRDA - The Natural Resources Damage Assessment Database** - collects information about restoration projects suggested by the public in response to an incident, such as an oil spill. The public (which could include companies or other business entities) submits all restoration activity information. Statute authorizing programs to cover collections of information from the public in the form of contact information for receipt of data generated by programs, e.g. **15 U.S.C. 1151**, "to make the results of technological research and development more readily available to industry and business, and to the general public." Along with project information, the database collects individual contact information (name, organization, work email address, home address, and home phone number). Personal information is used internally and not disseminated. We disseminate organization names either publicly as the submitting organization or as project partners, along with research information. **This application collects PII.**
- F. **RCDB - The Restoration and Conservation Database** - collects information related to fisheries habitat restoration projects implemented by the NOAA Office of Habitat Conservation. The Restoration Center often works with private companies and members of the public to implement projects and collects but does not disseminate contact information for individuals who have worked on the projects. Contact information includes name, work phone number, work email address, work address and organization name. An authorizing statute is **15 U.S.C. 1151**. Company names can be disseminated publicly and listed as "project partners" or "funding recipients" depending on their relationship to the project. Research information is also available to the public. **This application collects PII.**
- G. **eAOP - Electronic Annual Operating Plan** - The application provides NMFS managers and employees with the ability to plan, monitor, and report on organizational and Program information. This includes planning and reporting of milestones and performance measures, arraying milestones by key subject areas, and assisting

Programs managers and staff in producing Program Annual Operating Plans. Contact names and phone numbers PII (contact information) are included in the milestone and performance measure information. Only NMFS employees with password access, granted by the Database Administrator, may retrieve information from the system. The organization uses the information internally for assembling annual operating plans and for reporting strategic progress to NOAA and Department of Commerce. **This application collects PII.**

- H. MMHSRP - Marine Mammal Health and Stranding Response Program** The Marine Mammal Health and Stranding Response Program system is a centralized database that is accessible via a restricted web that collects and disseminate reference (Level A) data (i.e, genus, species, common name, etc.) on stranded marine mammals and tracks the animal's rehabilitation disposition when deemed non-releasable. The system is for the purpose of scientific research. Our users are federal agencies, their non-federal partners, private organizations (i.e., aquariums), researchers, and educational institutions. **PII/BII is not collected.**
- I. GCLD - General Counsel Litigation Database** - This is an application to assist NOAA's legal counsel manage and respond to various inquiries on NMFS/NOAA litigation from Congress, the White House, Fisheries councils, government agencies. **PII/BII is not collected.**
- J. NPS - National Permits System** - 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. NMFS established the National Permits System (NPS) to accept and maintain all Sustainable Fisheries permit applications and related data. Some of the West Coast and Pacific Islands Regions permits information is housed in NPS, as well as Antarctic Marine Living Resources and High Seas permits; the rest is in other NMFS FISMA systems and is addressed in their PIAs. Authorities are the **Magnuson-Stevens Fishery Conservation and Management Act (16 USC 1801 et seq.)**, the **High Seas Fishing Compliance Act**, the **Tuna Conventions Act of 1950**, the **Antarctic Marine Living Resources Convention Act**, the **Western and Central Pacific Fisheries Convention Implementation Act (WCPFCIA; 16 U.S.C. 6901 et seq)**, 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**. **This application collects PII and BII.**
- K. eDiscovery Application** - The eDiscovery Platform system is a web-based application used to simplify agency response to Freedom of Information Act (FOIA) requests, aid in the processing Administrative Records (AR), and to a lesser extent, Congressional Inquiries and Legal Holds. The system serves as a single point for the collection, review, tagging, redaction and export of responsive records. NMFS offices shares the information in order to coordinate monitoring and management of sustainability of fisheries and protected resources, as well as with the applicable State or Regional Marine Fisheries Commissions and International Organizations. Sources of information

include the permit applicant/holder, other NMFS offices, the U.S. Coast Guard, and State or Regional Marine Fisheries Commissions. **This application collects PII and BII.**

- L. **TIPS - Traceability Information Program for Seafood** - The Traceability Information Program for Seafood (TIPS) is a public facing, web based application. The TIPS application is used to establish registration, reporting and recordkeeping requirements for U.S. aquaculture Version Number: 01-2017 producers of shrimp and abalone, two species subject to the Seafood Traceability Program, also known as the Seafood Import Monitoring Program (SIMP). Owners or operators of U.S. inland, coastal and marine commercial aquaculture facilities (“producers”) will be required to report information about production and entry into U.S. commerce of shrimp and abalone products. In addition, producers will be required to register with NMFS and retain records pertaining to the production of shrimp and abalone and entry of those products into U.S. commerce. This program serves as a domestic counterpart to the shrimp and abalone import requirements under SIMP, and will help NMFS verify that U.S. aquaculture shrimp and abalone were lawfully produced by providing information to trace each production event(s) to entry of the fish or fish products into U.S. commerce. **This application collects PII and BII.**
- M. **ECO - Environmental Consultation Organizer** - ECO is a web-based, case management application on Appian PaaS using AWS to support NMFS consultations under the **Endangered Species Act (ESA)** and under the **Magnuson-Stevens Fishery Conservation and Management Act sections 305(b)(2) & 305(b)(4) Essential Fish Habitat (EFH)**. This is the database for documenting and tracking consultation status and key internal process requirements throughout the consultation including quality assurance review and status in meeting statutory timelines. ECO collects project lead’s name and business telephone number. Some fields are for internal use while some fields are available to the public through the public interface on the application. **This application collects BII.**
- N. **FSD Loans - Financial Services Division** - The Financial Services Division collects information from applicants for the following programs and purposes: The Fisheries Finance Program (FFP), credit information, personal identification including social security number, and tax returns. The information collected verify applicants for fisheries loans. Capital Construction Fund (CCF), personal identification including social security numbers and tax returns. The information collect verify applicants for CCF accounts and projects. Fishermen's Contingency Fund (FCF), personal identification including social security numbers, and personal transaction information. The information is used to verify business losses and lost fishing gear for claims made by the fishermen. Information collected includes tax returns. Information collected: applicant’s name and address, the amount of financing applied for, the purpose of loans, an appraisal of the vessel or facility involved, financial information including the last 3 tax returns (these are not stored electronically), a list of creditors and buyers with relevant credit terms, identification of authorized representatives (accountant, attorney,

insurance agent), and legal history (status regarding bankruptcy, litigation, delinquency on and Federal debt, etc.). Annual financial statements are required of all borrowers. These statements update the financial statement information presented with the original application. The financial statements are used to monitor the borrower's financial condition and to trigger servicing actions if indicated. Loan applications are entered into the system from paper forms completed by the public, into an online application, which is managed by NMFS NOAA4000. Regional offices access the information in order to administer loans for applicants. The loan data is stored only in NOAA4000. **This application collects PII and BII.**

- O. FWS - NMFS Federal Web Site** - The National Marine Fisheries Service Federal Web Service (NMFS FWS) is a public facing responsive web service implemented with a Drupal 8 instance provisioned on an Acquia Drupal PaaS multi-tier medium environment fronted by Akamai Kona Site Defender web application firewall (WAF) and Akamai Content Delivery Network edge caching services. The Web Application Firewall is configured to mitigate DDOS events and perform network endpoint management services. Akamai Edge Cache consists of thousands of edge nodes backed by Akamai NetStorage which reverse proxies content managed in the Drupal instance. This consolidation improves information architecture, web content, and search functions, as well as providing a responsive design to accommodate increasing number of customers using mobile devices. **PII/BII is not collected.**
- P. UAS - Unmanned Aircraft System** is a standalone system used for civil and criminal enforcement activities and fisheries intelligence. The UAS collects pictures and videos of vehicles, vehicle tags, vessels vessel IDs and persons. The information in the system will be retrieved either by live feed to an external hard drive, directly to the computer, or to a flash drive. A camera is mounted on the unmanned aerial system, which broadcasts the information to the person(s) on the ground. Some UAS uses radio signals to transmit and receive the information. Some UAS has a multi-band wireless transmitter built in along with an antenna. Depending on the UAS, the receiver of the information signals can be either the remote control unit, a computer, tablet or smartphone device. Some UAS uses 4G / LTE network to transmit the information. This is comprised of a camera module, a data module and a 4G / LTE modem. The only information sharing conducted by the system will be with state and federal partners such as the US Coast Guard and JEA partners. We collect information under the authority of Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015). **This system collects PII/BII.**

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	X	g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access	X	h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): New Applications and Public Web Site associated with TIPS : ECO : FSD Loans : FWS Two applications were removed: TCTS : Rhythmx CMX					

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). *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. *Please describe the activities which may raise privacy concerns.*

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 about: *(Check all that apply.)*

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..."

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

DOC employees

Contractors working on behalf of DOC

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?

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.

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 the NOAA4000 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 [IT SYSTEM NAME] 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): Steven Freeman

Signature of ISSO or SO: FREEMAN.STEVEN.L Digitally signed by
FREEMAN.STEVEN.LEVERNE.105385154
8
Date: 2019.12.04 07:49:18 -05'00'
EVERNE.1053851548

Name of Information Technology Security Officer (ITSO): Rick Miner

Signature of ITSO:  MINER.RICHARD.SCOTT.1398604
519
2019.12.04 08:43:48 -05'00'

Name of Authorizing Official (AO): Roy Varghese

Signature of AO: VARGHESE.KOYICKAL.R Digitally signed by
VARGHESE.KOYICKAL.ROY.1400785496
Date: 2019.12.04 14:11:45 -05'00'
OY.1400785496

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

Signature of BCPO: INDIVIGLIO.FRANK.M.13 Digitally signed by
INDIVIGLIO.FRANK.M.1380923714
Date: 2020.01.13 14:18:08 -05'00'
80923714