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

Privacy Threshold Analysis for the NOAA4000

Fisheries WAN and Enterprise Services

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/NMFS/Fisheries WAN and Enterprise Services

Unique Project Identifier: NOAA4000

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 NMFS Headquarters WAN and Enterprise Services System (NOAA4000) is a General Support System (GSS) comprising three cloud subsystems: Oracle Cloud Infrastructure (OCI), Google Cloud Platform (GCP), and the Appian Cloud Platform. The system hosts several applications that collect, store, and/or disseminate information on members of the public, including foreign national guests, and in some cases, NOAA staff and/or contractors. N0AA4000 has ingested the former NOAA4020 Science and Technology subsystem and all of its applications. Because NOAA4000 is a GSS system, the ingestion did not change or introduce any new support that NOAA4000 already provides.

Address the following elements:

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

The NMFS Headquarters WAN and Enterprise Services System (NOAA4000) is a General Support System (GSS) comprising three cloud subsystems: Oracle Cloud Infrastructure (OCI), Google Cloud Platform (GCP), and the Appian Cloud Platform. The system hosts several applications that collect, store, and/or disseminate information on members of the public, including foreign national guests, and in some cases, NOAA staff and/or contractors.

b) *System location*
This system has three geographical locations: Ashburn, VA; Seattle, WA; and 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)*

* There have been no changes to the interconnections since the last SAOP approved PIA. The updates to the PIA have been made to ensure that the Cyber Security Assessment and Management (CSAM) system and the PTA and PIA match.

The NMFS WAN NOAA4000 connects to the Seattle DR site via NWAVE NOAA0550 and has interconnections with the following entities:

1. U.S. Coast Guard
2. Pacific States Marine Fisheries Commission
3. U.S. Custom and Border Protection
4. Atlantic Coastal Fisheries Information Network (ACFIN)
5. Information Technology Center (ITC – NOAA1101)
6. 1901 NSOC
7. Department of Justice (DOJ)
8. Naval Research Lab MDA
9. Other NOAA NMFS Systems:
    a. NOAA0550 (NWAVE)
    b. NOAA4011 (NFPLRS)
    c. NOAA4100 (GARFO)
    d. NOAA4200 (NEFSC)
    e. NOAA4300 (SERO)
    f. NOAA4400 (SEFSC)
    g. NOAA4500 (WCR)
    h. NOAA4600 (NWFSC)
    i. NOAA4700 (AKRO)
    j. NOAA4800 (AKFSC)
    k. NOAA4920 (PIRO)
    l. NOAA4930 (SWFSC)
    m. NOAA4960 (PIFSC)

The interconnections between NOAA4000 and the entities listed above are established through encrypted interfaces (VPN) or the Verizon MPLS (which is internal NMFS). Authentication methods are in place to validate authorized users. Virus and malicious code prevention is employed to protect the integrity of the software and the data.

d) The purpose that the system is designed to serve

NOAA4000 provides the necessary infrastructure, data center colocation, and application support services that are instrumental to obtaining the objectives of the NMFS and its mission.

NOAA4000 GSS includes hardware, software, information, data, applications, communications, facilities, and people. NOAA4000 provides IT support by providing IT infrastructure for Fisheries applications, providing enterprise security services, network connectivity (WAN/LAN), enterprise resource access (local/remote), database management, and enterprise IT helpdesk support.

IT infrastructure consists of the hardware and software used within the environment to support the NMFS mission. The IT services component provides technology services to the NMFS organization and NMFS applications supported by the IT infrastructure. Below are the services NOAA4000 provides:

IT Infrastructure:

<u>Hardware</u>

End-user systems (Desktops/Laptops, Printers, Mobile devices, Desk phones)
Administrative Systems (Appliances, Servers, Networking devices, Storage)

<u>Software</u>

Operating Systems (Desktop, Mobile, Server, Network)
Applications (Utilities, Tools, Productivity, Database)
Telecommunications (Includes Voice, Data, and VTC Circuits)

IT Services:
Local Area Networking (LAN)
Wide Area Networking (WAN)
VoIP
File Shares/Print Service
Helpdesk
Internet Connectivity
Application Hosting and Development
Enterprise Active Directory Enterprise Storage
VPN
Web Services
IT Security Service
Database Management

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

NOAA4000 provides IT support by providing IT infrastructure for Fisheries applications, providing enterprise security services, network connectivity (WAN/LAN), enterprise resource access (local/remote), database management, and enterprise IT helpdesk support. The NMFS WAN services are through N-WAVE.

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

SISP - The Seafood Inspection Services Portal (SISP) 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, and NOAA Finance (billing data)) to: 1) create an account; 2) update company information including multiple locations; 3) request certificates, inspections and contracts; and 4) review and pay invoices. NOAA collects the information under the authority of the Agriculture and Marketing Act of 1946 and Fish & Wildlife Act of 1956. Name, work email address, work address, and financial transaction are collected. The information is shared with the private sector for invoicing and bill payment. This application collects PII and BII**.**

EDMS – The Electronic Document Management System (EDMS) 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 used to assist in completing required personnel-related forms that contain names, job descriptions, and General Schedule level. EDMS also contains various legal documents/case files that may include SSN and/or 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. Although EDMS has been decommissioned, residual data is still stored within NOAA4000 boundaries.

VMS - The National Vessel Monitoring System (VMS) 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 shares 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 BII.

TRIDENT - Trident has been officially decommissioned; however it remains active for historical records retention purposes. TRIDENT is a cloud-based case management system that allows sworn law enforcement officers, special agents, and other staff seamless electronic collaboration with internal team members and external partners. TRIDENT also aids in 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 accordance with U.S. laws and regulations and international agreements. Enforcement personnel develop domestic and international investigative case files that support prosecuting alleged violations. Data and information contained in these files relate 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 system is integrated with the NOAA Office of General Counsel system Justware. This application collects PII and BII.

NEIS - The NOAA Enforcement Information System (NEIS) is a cloud-based case management system to support Office of Law Enforcement (OLE) and General Council Enforcement Section (GCES) agent, officer, and attorney needs for the entry, case management, and reporting of law enforcement data and is the replacement application to the TRIDENT and JustWare systems. The authority for federal fishery management is the Magnuson-Stevens Conservation and Management Act (16 U.S. Code 101 et. Seq.). Vessel operator name, contact information and vessel ID are collected along with applicable law enforcement data such as case files and a list of seized property. The case files include, in addition to vessel operator name, contact information and vessel ID, information collected by authorized law enforcement officers or agents, such as approved fishing licenses, type of fishing gear being used, and information on the catch. The case files also contain substantiating evidence such as sworn witness accounts, photographs, documents, and voice recordings. The case files support the collection of fines and/or the prosecution of these cases. 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. This application collects PII and BII.

NRDA - The Natural Resources Damage Assessment (NRDA) 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. Statutes such as 15 U.S.C. 1151 authorize programs to collect information from the public in the form of contact information for receipt of data generated by programs "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. Data, including PII, is exported and shared with NRDA trustee agencies coordinating with NOAA in the development of restoration plans. Organizational names are publicly accessible as the submitting organization, as project partners, or in association with research information. This application collects PII.

RCDB - The Restoration and Conservation Database (RCDB) 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. This application collects PII.

eAOP – The Electronic Annual Operating Plan (eAOP) application provides NMFS managers and employees with the ability to plan, monitor, and report on organizational and program information. This includes the planning and reporting of milestones and performance measures, arraying milestones by key subject areas, and assisting program managers and staff in producing program annual operating plans. Contact names and phone numbers 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 the Department of Commerce. This application collects PII.

NPS – The National Permits System (NPS) accepts and maintains all Sustainable Fisheries permit applications and related data. Some of the West Coast and Pacific Islands Region permits information is housed in NPS, as well as Antarctic Marine Living Resources and High Seas permits. All other permit information is in other NMFS FISMA systems and is addressed in their PIAs. Authorities that apply to this application and its data are:

The Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 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.

ECO – The Environmental Consultation Organizer is a web-based case management application on Appian PaaS using Amazon Web Services (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 database is used 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 the 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 PII.

FishFinS - The FishFinS system is a major application that acts as the system of record for financial and customer data for multiple business lines (i.e., Fisheries Finance Program (FFP), Fishery Capacity Reduction Program (Buyback), Capital Construction Fund (CCF), and Fishermen's Contingency Fund (FCF)). The system is located in the Oracle Cloud Infrastructure (OCI) Cloud and will reside on the NMFS Oracle Multi-Tenancy Cloud Instance. FishFinS provides various types of information to the following groups:

- NOAA Internal - Provides financial/accounting information to another core accounting NOAA System (Commerce Business System (CBS)). Entries in CBS must match the FishFinS system.
- NOAA Senior Management - Provides reporting and financial portfolio management information to senior management, congressional delegates, and other special purpose groups regarding the status of loans and any additional questions for constituent/loan holder community.
- Department of Commerce (DOC) Management - Provides reporting and financial portfolio management information to senior management, other agencies, congressional delegates, and other special purpose groups.
- Congressional and Special Interest Groups - Provides metrics and business line data points to fulfill the approved inquiry. For example, the number of FFP loans by state.
- Stakeholders (Fisheries Finance Program (FFP), Buybacks, Fishermen's Contingency Fund (FCF), and Capital Construction Fund (CCF)) - Provides application paperwork, invoices, annual reports, and interest statements to borrowers, buyers, agreement holders, and claimants of the program. Each business line internally maintains data and reports and may provide information to senior NOAA management and the external constituent community.
- External Government Stakeholders - Provides annual reports to the IRS and can turn over default accounts to the U.S. Treasury Department. Some stakeholders provide reports and information to

other government agencies if and when asked. No formal connection exists between other government agency systems and FishFinS, nor the legacy systems. The connections may exist in the future if and when the second phase of development commences. The Buyback Program is part of the Magnuson-Stevens Fishery Conservation and Management Act that authorizes NMFS to conduct a fishing capacity reduction program. The Capital Construction Fund (CCF) is part of the Merchant Marine Act of 1936 as amended (46 U.S.C. 1177), United States tax code (26 U.S.C. Part 7518). The CCF is implemented by regulations under CFR Title 50, Part 259.

The Fishermen's Contingency Fund Regulation is (50 CFR part 296, 11/01/1982).

The Fisheries Finance Program (FFP) is part of the Merchant Marine Act and Magnuson-Stevens Act Provisions, Chapter 537 of Title 46 of the United States Code, 46 U.S.C. 53701, 46 U.S.C. 53702(b)(4)(B). This application collects PII and BII.

UAS – The Unmanned Aircraft System (UAS) is a standalone system used for civil and criminal enforcement activities and fisheries intelligence. The UAS collects pictures and videos of vehicles, vehicle tags, 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 use radio signals to transmit and receive the information. Some UAS have 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 use 4G / LTE networks to transmit the information. This consists 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 U.S. Coast Guard and Joint Enforcement Agreement (JEA) partners. NOAA collects 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.

GCLD – The General Counsel Litigation Database (GCLD) is an application to assist NOAA's legal counsel manage and respond to various inquiries on NOAA/NMFS litigation from Congress, the White House, Fisheries councils, and other government agencies. PII/BII is not collected.

MMHSRP – The Marine Mammal Health and Stranding Response Program (MMHSRP) system is a centralized database that is accessible via a restricted web connection that collects and disseminates 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. Users are federal agencies, their non-federal partners, private organizations (i.e., aquariums), researchers, and educational institutions. PII/BII is not collected.

FWS - 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. 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.

NATS – The NMFS Agreement Tracking System (NATS) was created to reduce the time and effort required to approve agreements by NMFS Financial Management Centers (FMCs) and Budget Execution Division (BEX) personnel. Additionally, NATS will reduce the number of physical folders and paperwork that need to be printed for routing and approval. This application collects BII.

GSDS - The primary purpose of the NMFS' Global Seafood Data System (GSDS) is to fulfill congressional directives to curtail the United States import and consumption of fisheries products that are a product of Illegal, Unreported, and Unregulated (IUU) fishing. Information derived from this system will be used to direct NMFS personnel in the monitoring, management, and enforcement of fisheries imports. The Seafood Import Monitoring Program (SIMP), will be the first of four NMFS trade monitoring programs that GSDS will focus on.

GSDS will utilize data analytics, machine learning, and artificial intelligence to process fisheries trade data from various sources to structure data and create reports. This information will be utilized to establish a more comprehensive approach to counter the flow of IUU fishing products into the U.S. It will help NMFS to establish management measures, within the scope of other U.S. fisheries trade management roles, to provide a well-informed awareness and understanding in support of the initiative to assure legitimate trade and combat IUU fishing.

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) and provided to NMFS via SFTP for inclusion in the ITDS database. The ITDS serves two primary purposes:

(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.

MRIP - 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. This data is entered 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.

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.

NFCSS - 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 pay 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 pay 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 (Office of Science and Technology (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 pay band V research scientist from each regional science center, the NOAA Fisheries Human Resources (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 include name, work contact information, letters of reference and curricula vitae, performance plans, 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.

Protected Resources National Inventory of Marine Mammals (NIMM) System - The National Inventory of Marine Mammals (NIMM) system maintains current and past data (it replaced 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.

NOAA Emergency Contact List - The Emergency Contact List (ECL) stores contact information for OST staff and staff emergency contacts to be used in case of emergency. This is PII data.

HawkEye 360 (HE360) Collection – Radio Frequency (RF) geo-location data buoy to be delivered/stored and shared with U.S. Coast Guard.

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

Authorized federal employees and contractors with a need-to-know have access to the information on the system. NOAA4000 also has publicly accessible data that is accessed by the public via the internet, but does not contain PII or BII nor do they have access to network resources. NOAA4000 also provides non-sensitive PII and BII to other state and federal agencies for law enforcement purposes. Additionally, NOAA4000 provides fishery information that does not include PII or BII to private organizations, researchers, and educational institutions.

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

There are two primary ways users can retrieve information from NOAA4000. The first is to be locally connected to the NOAA4000 network or via remote access through NMFS VPN, which is within the FISMA boundary of NOAA4000. The second way to retrieve data is via general internet, but this is limited based on the application or support being accessed.

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

NOAA4000 information is transmitted via Virtual Private Networks (VPNs), Internet, and dedicated network connections that makeup NMFS Verizon Multiprotocol Label Switching (MPLS) (WAN) network.

For Google Cloud Platform (GCP), all information is coming through the trusted internet connection (TIC) externally to NWave and then to GCP through a partner interconnect. The partner interconnect is controlled through a single Google Project, which is managed by the NMFS networking team. Those networking connections are then provided to the different partners within NMFS. Firewalls are managed through the same network connection described above. The default firewall configuration is to deny all, and allow through exception.

Firewall configurations are managed only by the networking team. Any communication ports that go through the firewall have to be opened by the firewall team, through an internal approval process.

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.*

_X__ 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): TRIDENT has been replaced with NEIS and FishFinS has replaced the Financial Services Division (FSD) Loans.					

_____ 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. *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): * UAS is used by law enforcement for area safety surveillance, detection, and avoidance while inspecting and marking remote crime scene areas and crime scene reporting. Use will follow the NOAA Unmanned Aircraft Systems policy in regard to PII and BII collection. HE360 RF geo-location data is being added.			

_____ 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
_X___ 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?

_X___ 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. The SSN is collected to verify applicant's eligibility for loans.
Provide the legal authority, which permits the collection of SSNs, including truncated form. From NOAA-12: The Marine Mammal Protection Act, 16 U.S.C. 1361 et seq.; the Fur Seal Act, 16 U.S.C. 1151 et seq.; and the Endangered Species Act, 16 U.S.C. 1531 et seq. [For collection of the Tax Identifying Number (Employer Identification Number or Social Security Number), 31 U.S.C. 7701.]

_____ 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 NOAA4000 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 or System Owner Name: Doug Brackett Office: 3609 Phone: 301-427-8815 Email: Doug.Brackett@noaa.gov Signature: Digitally signed by BRACKETT.DOUGLAS.HOWE.1365899564 Date: 2023.06.27 09:05:36 -04'00' Date signed:	**Information Technology Security Officer** Name: Catherine Amores Office: 3432 Phone: 301-427-8871 Email: Catherine.Amores@noaa.gov Signature: AMORES.CATHERINE.SOLEDAD.1541314390 Digitally signed by AMORES.CATHERINE.SOLEDAD.1541314390 Date: 2023.06.30 11:31:17 -04'00' Date signed:
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.06.30 12:53:36 -04'00' Date signed: 6/30/23	**Authorizing Official** Name: Nancy Majower Office: 3853 Phone: 301-427-8811 Email: Nancy.Majower@noaa.gov Signature: REID MAJOWER.NANCY.1365836694 Digitally signed by REID MAJOWER.NANCY.1365836694 Date: 2023.06.30 11:21:38 -04'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.07.03 09:44:06 -04'00' Date signed: 7/3/23	