Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA2220

Fleet Support System (FSS)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/OMAO/Fleet Support System (FSS)

Unique Project Identifier: NOAA2220 Fleet Support System

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 on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *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 NOAA2220 Fleet Support System (FSS) comprises of sensors, computers, and networked devices that are located on NOAA Office of Marine and Aviation Operations' (OMAO) ships, aircraft, uncrewed platforms and at NOAA's Marine and Aircraft Operations Centers that help facilitate OMAO's mission of remote data collection. The NOAA2220 Fleet Support System provides remotely deployable networks, computer systems, and sensors to support and facilitate all aspects of the collection of Oceanographic, Meteorological, Atmospheric, and Topographical data and transmits the data to other NOAA Line Offices for processing and distribution.

Address the following elements:

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

The NOAA2220 Fleet Support System (FSS) is identified as a general support system known for collecting scientific data.

b) *System location*

The NOAA2220 System is located throughout the United States. NOAA2220 is aboard ships that are homeported in San Diego, CA; Newport, OR; Honolulu, HI; Pascagoula, MS; Charleston, SC; Norfolk, VA; and Davisville, RI. Along with the ships are three Marine Operations Centers located in Newport, OR; Honolulu, HI; and Norfolk, VA. There are four support facilities that are located in San Diego, CA; Pascagoula, MS; Charleston, SC; and Newport, RI. NOAA2220 also has systems on aircraft that are stationed at the Aircraft Operations Center in Lakeland, FL. The NOAA2220 Headquarters is located in Silver Spring, MD. NOAA2220 has a FedRAMP approved

cloud presence that is hosted on servers that are located in the United States.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

The NOAA2220 Fleet Support System is a standalone system. It does not interconnect with any other systems for the purposes of processing or handling PII/BII. Where applicable, and when available, NOAA2220 interconnects with the NOAA0550 NOC/N-Wave which provides a trusted pathway between NOAA research vessels, aircraft, and other NOAA2220 cloud and land based facilities nationwide. NOAA2220 does not share or process PII/BII with the NOAA0550.

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

Though the original purpose of the NOAA2220 was to facilitate the remote collection and distribution of scientific raw data, over the years its role has expanded to support many aspects of mission operations.

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

The NOAA2220 system utilizes a variety of sensors, computers, ancillary devices and human input to collect the raw data that is the mission of the ships and aircraft.

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

The NOAA2220 system is a general purpose system that collects raw data (oceanographic, meteorologic, atmospheric, and topographical) from sensors, antennas, and human input. The system also supports administrative functions. Data (administrative, medical) is collected on employees to maintain good health and welfare as well as pay information. The collected science information is distributed to persons that have an interest including the public. The administrative information is not distributed outside of NOAA. Only authorized personnel (federal employees and contractors) with a need to know have access to the administrative information. Uncrewed Aerial Systems (UAS) collect video and photographic imagery. Any incidental capture of PII is immediately deleted. Video and images from the shipboard video safety system and security camera video monitoring secured spaced onboard ships is also collected.

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

Science data is available to all interested personnel through public-private partnerships. The administrative data is restricted to the executive officer, the administrative officer, and medical personnel. The system is maintained by System Administrators and Chief Electronics Technicians that can gain access to science and administrative information to perform IT functions on an as

needed basis.

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

Users are able to retrieve information from the system by accessing files from NOAA2220 computers, laptops, and portable USB devices.

i) How information is transmitted to and from the system

At its core, the purpose of the NOAA2220 Fleet Support System is to collect scientific and position data for maritime and airborne assets in the locations of interest. However, as described above the purpose of the NOAA2220 system has expanded over time to meet OMAO mission needs. As it pertains to sensitive business and personal information transmitted within the IT General Support Enclave sub-functions, data is transferred to and from the system via computers, USB portable drives, network connections, scanners, and video cameras. The IT R&D Science Enclave sub-function can ingest information from video cameras to the system and this information is transmitted from this Enclave via computers, USB portable drives, and network connections.

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.*

____ 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.*

_X_ 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):			

____ 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. *Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: OMAO CPC applications may collect and maintain SSN, EmployerID, EmployeeID, Driver's License, Passport, and Health Records for Human Resource functions like hiring, payroll, proof of residency, proof of identity for marine and aircraft facility locations, clearance to travel, fitness for duty requirements associated with both aircrew and ship's crew, treatment of medical emergencies onboard vessels at sea. NOAA Medical Providers responsible for the medical care of employees working throughout NOAA may disclose employee HIPAA and other protected information such as a SSN to facilitate medical care in the best interest of the employee.
Provide the legal authority which permits the collection of SSNs, including truncated form. COMMERCE/NOAA-1 - Applicants For The NOAA Corps. COMMERCE/NOAA-3 - NOAA Corps Officer Official Personnel Folders. COMMERCE/NOAA-21 - Financial Services Division. COMMERCE/DEPT-1 - Attendance, Leave, and Payroll Records of Employees and Certain Other Persons.

____ 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 NOAA2220 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 [IT SYSTEM NAME] 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: Thomas Grigsby Office: NOAA OMAO Phone: 301-628-5720 Email: thomas.grigsby@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: GRIGSBY.THOMAS.W.1049202896 Digitally signed by GRIGSBY.THOMAS.W.1049202896 Date: 2023.01.18 10:15:44 -05'00' Date signed:	**Information Technology Security Officer** Name: Sean McMillan Office: NOAA OMAO Phone: 863-296-8270 Email: sean.t.mcmillan@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: MCMILLAN.SEAN.T.1185814382 Digitally signed by MCMILLAN.SEAN.T.1185814382 Date: 2023.01.18 09:22:11 -05'00' Date signed:
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828 271-4695 Email: robin.burress@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.01.25 09:42:50 -05'00' Date signed: 01/25/2023	**Authorizing Official** Name: Luther Young Office: NOAA OMAO Phone: 202-731-7740 Email: luther.young@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: YOUNG.LUTHER.NMN.1063906677 Digitally signed by YOUNG.LUTHER.NMN.1063906677 Date: 2023.01.19 16:55:07 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2023.03.07 08:14:14 -05'00' Date signed: 7 March 2023	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.