

U.S. Department of Commerce
NOAA



Privacy Threshold Analysis
for the
[NOAA2220 Fleet Support System (FSS)]

U.S. Department of Commerce Privacy Threshold Analysis

[NOAA / Fleet Support System (FSS)]

Unique Project Identifier: [006-48-01-15-02-3601-00]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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, unmanned 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, Meteorologic, Atmospheric, and Topographical data and transmits the data to other NOAA Line Offices for processing and distribution.

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 NOAA2220 Fleet Support System (FSS) is identified as a general support system of computers, sensors, and networked devices most known for collecting scientific data. However, in support of OMAO operations, potential privacy and business sensitive information can exist within some of the functions of the General Support Enclave and Research and Development (R&D) Science Enclave. See figure 1 below.

b) System location

Systems are primarily located onboard NOAA OMAO ships, aircraft, unmanned vehicles, and in the cloud (Azure). However there is a very small number of support systems located at OMAO's Marine and Aircraft Operations Centers in Norfolk, Virginia; Honolulu, Hawaii; and Newport, Oregon. Additional

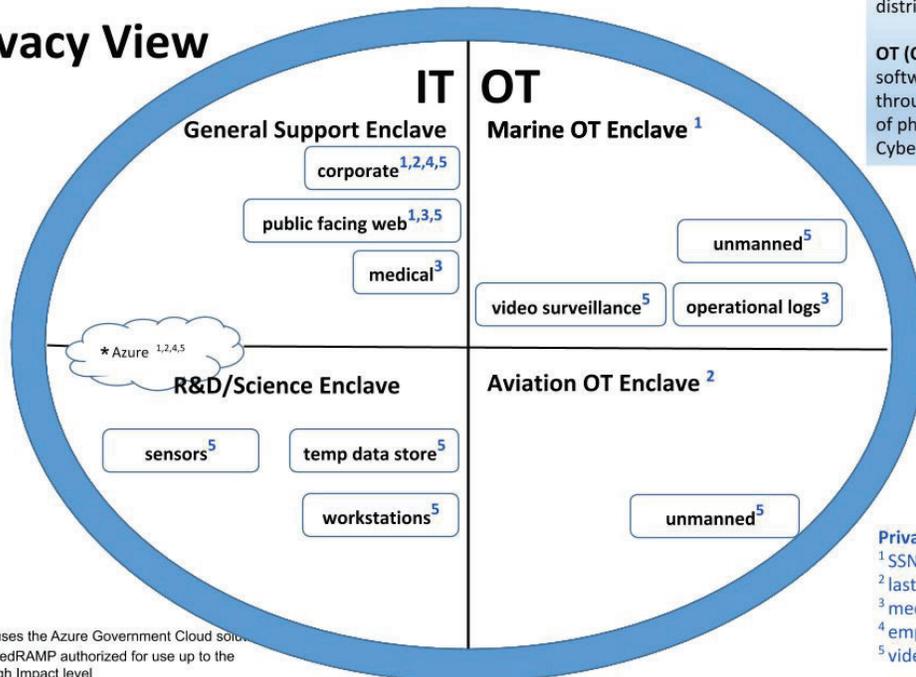
ship-specific support is provided through port office facilities in Woods Hole, Massachusetts; Davisville, Rhode Island; Charleston, South Carolina; Pascagoula, Mississippi; and Ford Island, Hawaii. Limited pier-side support is also provided to ships in Newport, Rhode Island and Kodiak, Alaska, though there is no IT equipment located at these locations.

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

The NOAA2220 system is designed to operate in a stand-alone environment and does not require any connections to perform its core requirements. However, during optimal operations, NOAA2220 interconnects with the NOAA NOC/NWAVE for trusted interconnection pathways to the NOAA2220 cloud environment and cyber, marine, and aircraft operations centers. This remotely deployed system is broken down into enclaves that facilitate all aspects of OMAO’s mission operations (see figure 1, privacy view of enclaves and data, next page). There are four main enclaves. Two that cover Operational Technology (OT) and two that cover Information Technology (IT). The OT enclaves are Marine Operational Technology (MOT) and Aviation Operational Technology (AOT). The MOT and AOT enclaves largely consist of navigation, mechanical, propulsion, as well as unmanned command and control systems and present very limited privacy risk in the form of video surveillance and video and photographic imagery from the unmanned functions.

There are two Information Technology (IT) enclaves: the General Support and the R&D Science. The General Support enclave privacy concerns exist within the corporate, medical and public facing web functions. The R&D Science enclave has a very limited privacy risk in the form of video and photographic imagery in the sensors, temp data store, and workstation functions.

NOAA 2220 Enclave Privacy View



IT (Information Technology): Hardware and software used for the processing and distribution of data. - Cyber Security

OT (Operational Technology): Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events. - Cyber Safety

Note:

* OMAO uses the Azure Government Cloud solution, which is FedRAMP authorized for use up to the FISMA High Impact level

Privacy Notes:

- ¹ SSN.
- ² last name, first name, address, phone, dob,
- ³ medical history
- ⁴ employee performance record
- ⁵ video imagery and or photos

Figure 1

d) The purpose that the system is designed to serve

The NOAA2220 Fleet Support System supports and facilitates all aspects of the collection of scientific data that OMAO is tasked with.

e) The way the system operates to achieve the purpose

In order to achieve OMAO's requirements, NOAA2220 Fleet Support Systems are deployed aboard NOAA's aircraft, ships, unmanned platforms as well as at the cyber, marine, and aircraft operations centers, and in the cloud (Azure).

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

NOAA2220 systems are primarily deployed to collect oceanographic, meteorologic, atmospheric, and topographical data for delivery to other NOAA line offices and customers. Some of these systems are also used to control and monitor the Operational Technology (OT) i.e. SCADA, support systems that help to position the operational platforms and it's personnel in the scientific target area. Potential privacy and business sensitive information can exist within NOAA2220 within the Enclave sub-functions, see figure 1. At its core, the purpose of NOAA2220 Fleet Support System is to collect scientific data, which is transferred from the R&D / Science enclave suite of sensors, telemetry, computers, to OMAO customers like other Line Offices. Further NOAA2220 Operational Technology (OT) i.e. SCADA systems are used to control, navigate and monitor marine, aircraft, and unmanned platforms. OT systems are stand-alone systems and receive data via sensors, servo loops, telemetry as well as other air-gapped computer systems. Within the MOT and AOT Operational Technology enclaves there is a limited privacy risk in the form of video surveillance and video and photographic imagery from the unmanned functions. Within the Information Technology (IT) enclaves: the General Support and the R&D Science. The General Support enclave privacy concerns exist within the corporate, medical and public facing web functions. The R&D Science enclave has a very limited privacy risk in the form of video and photographic imagery in the sensors, temp data store, and workstation functions.

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

These systems are designed, configured, operated, and maintained by authorized NOAA Corps, NOAA federal and OMAO contractor personnel. Science information is accessible by NOAA, OMAO, federal, contractor, university and public personnel. Privacy information is only accessible by authorized NOAA OMAO federal and contractor personnel and the subject individual of the information. Business sensitive information is only accessible by authorized NOAA OMAO federal and contractor personnel and the

subject vendor if applicable.

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

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

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

For cases where the transmission of sensitive privacy or business information is applicable (i.e., within the IT General Support Enclave sub-functions), data are 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. 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	X	f. Commercial Sources		i. Alteration in Character of Data
j. Other changes that create new privacy risks (specify): Potential sensitive video can exist within the IT R&D Science enclave under the Sensors, Data and Display functions due to the potential to capture personal imagery through unmanned aerial systems. COMMERCE/DEPT-29				

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	X	Electronic purchase transactions	
Other (specify): Electronic Health Records and Electronic Human Resources records, Potential video imagery and aerial photos associated with Unmanned Aerial System (UAS) and externally mounted cameras on research aircraft as well as video and images from shipboard video safety system and security camera video monitoring secured spaces onboard ships.			

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.

- Electronic Health Records
- Electronic Human Resources Records

Provide the legal authority which permits the collection of SSNs, including truncated form. NOAA2220 cites the following legal authority to collect SSN:

SORN's - OPM Government-1, COMMERCE/NOAA-1, COMMERCE/DEPT-1

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.

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 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 NOAA2220 Fleet Support System (FSS) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of Information System Security Officer (ISSO) or System Owner (SO): John W. Hill

Signature of ISSO or SO: **HILL.JOHN.W** Digitally signed by
.1201162790 HILL.JOHN.W.1201162790 Date: 8 June 2020
Date: 2020.06.08 12:34:12
-04'00'

Name of Information Technology Security Officer (ITSO): Sean T. McMillan

Signature of ITSO: **MCMILLAN.SEA** Digitally signed by
N.T.1185814382 MCMILLAN.SEAN.T.1185814382 Date: 8 June 2020
Date: 2020.06.08 11:50:32 -04'00'

Name of Privacy Act Officer (PAO): Adrienne Thomas

Signature of PAO: **THOMAS.ADRIEN** Digitally signed by
NE.M.1365859600 THOMAS.ADRIENNE.M.1365859600 Date:
Date: 2020.06.16 12:29:23 -04'00'

Name of Authorizing Official (AO): Shantrell Collier

Signature of AO: **COLLIER.SHANTRELL** Digitally signed by
NICOLE.1062371540 COLLIER.SHANTRELL.NICOLE.1062371540 Date: 8 June 2020
Date: 2020.06.08 18:39:01 -04'00'

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

Signature of BCPO: **GRAFF.MARK.HYRUM.151** Digitally signed by
4447892 GRAFF.MARK.HYRUM.1514447892 Date:
Date: 2020.09.08 09:29:43 -04'00'