

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



**Privacy Threshold Analysis  
for the  
NOAA5044  
Mission Support LAN (MSL)**

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

### NOAA/NESDIS/Mission Support LAN (MSL)

**Unique Project Identifier: NOAA5044**

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

#### **Description of the information system and its purpose:**

The Mission Support LAN (MSL) provides services in support of missions at various NESDIS sites that utilize applicable DOC, NOAA, and OSPO enterprise services. NOAA missions supported by the MSL include:

- Geostationary Operational Environmental Satellite (GOES)
- Polar-Orbiting Environmental Satellite (POES)
- Environmental Satellite Processing Center (ESPC)
- NOAA Jason Ground System (NJGS)
- Defense Meteorological Satellite Program (DMSP)
- GOES-R series (GOES-16), including Deep Space Climate Observatory (DSCOVR)
- Joint Polar Satellite System (JPSS)
- Comprehensive Large Array-data Stewardship System (CLASS)
- Radio Frequency Interference Monitoring System (RFIMS)

The MSL supports the OSPO mission by providing a protected location outside the isolated SCADA boundary for read-only copies of Satellite Health and Safety information for near-real-time and long-term analysis, various engineering tools, and the Change Management approval system.

The primary physical site of MSL is located at the NOAA Satellite Operations Facility (NSOF) in the Suitland Federal Center. The MSL is located logically and/or physically outside current NOAA/OSPO mission systems but for some information systems, support data might be required to be exported for analysis, continuous monitoring, or other functions. Security controls and authentication methods are implemented between the MSL and other NOAA/OSPO mission systems to ensure that all organizational security standards and requirements are met. The MSL utilizes the latest virtualization techniques where applicable, and provides users with dependable access methods to specific mission support data. The MSL provides a reliable and redundant capability to route mission support data to and from other external systems. The MSL is a General Support System (GSS) that is currently in the production environment.

The MSL also provides enterprise-level services including the enforcement of NOAA/OSPO policies and procedures across FISMA control families, management and oversight of Security

Awareness and Role-Based Training, Configuration Management, and Incident Management Programs. The MSL is the Common Control Provider for all NOAA/OSPO systems, under NIST Special Publication 800-53 Rev 4, para 2.4, for these enterprise services. The MSL FIPS-200 documentation provides details on specific controls offered, justifications, and requirements for inheritance linked with all NOAA/OSPO information systems.

The MSL consists of four major network segments:

- The Security/Boundary Segment isolates the public Internet from the MSL.
- The Network Infrastructure Segment consists of the architecture—equipment and connections—that makes up the MSL.
- The Domain Segment consists of all the services in the MSL.
- The Workstation Segment represents all workstations and their operating systems for the MSL.

The MSL connects to the NOAA Enterprise Network (N-Wave) (NOAA0550) for Internet connectivity. Currently, it utilizes Microsoft Windows Server 2019 Active Directory Domain structure called NESDISMS.NOAA. The MSL consists of file servers, web servers/intranet servers, and application servers that host applications for NOAA/OSPO information systems including Microsoft SQL Server, ECMT, ECMO Big/Fix Server, McAfee e-Policy Orchestrator Server, DOORS Server, and Websense Web Filter, SharePoint, etc. The MSL provides engineering and analysis tools for satellite operations and product processing. Data being processed, stored, and transmitted is restricted to sensitive – for official use.

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 Mission Support LAN (MSL) is a General Support System.

*b) System location*

The NOAA Mission Support LAN (MSL) is located in the following locations:

- NOAA Satellite Operations Facility (NSOF) in Suitland, MD (primary)
- NOAA Center for Weather and Climate Prediction (NCWCP) in College Park, MD
- NOAA SSMC1 in Silver Spring, MD

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

MSL interconnects with the following NOAA information system:

- NOAA0100, Cyber Security Center
- NOAA0550, NOAA Enterprise Network
- NOAA5003, Geostationary Operational Environmental Satellite Ground System
- NOAA5006, Headquarters Local Area Network
- NOAA5026, Polar Operational Environmental Satellite Ground System
- NOAA5040, Comprehensive Large Array-Data Stewardship System

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

The MSL utilizes the latest virtualization techniques where applicable, and provides users with dependable access methods to specific mission support data. The MSL provides a reliable and redundant capability to access Mission Support Data.

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

NOAA5044 provides services in support of missions at various NESDIS sites that utilize applicable OSPO enterprise services. The MSL supports the OSPO mission by providing a protected location outside the isolated SCADA boundary for read-only copies of Satellite Health and Safety information for near-real-time and long-term analysis, various engineering tools, and the Change Management approval system. NOAA5044 operates with network infrastructure, virtual server infrastructure, physical servers, workstations, and storage area networks, and printers to support staff in meeting the mission.

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

Mission Support LAN (MSL) collects and stores mission support data. COOP data is collected for contingency related activities. Additionally, MSL contains General Purpose Data (GPD) including name, maiden name, email, and telephone number, Work Related Data (WRD) including job title, work address, work telephone number, and work email address, and System Administrative / Audit Data (SAAD) including user ID, IP address, date/time of access, queries run, ID files access, and contents of files.

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

NOAA5044 users (federal employees and contractors) authenticate to the system using their CAC and have access to resources based on their role and responsibilities or need to know basis.

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

MSL users (federal employees and contractors) authenticate to the system using their CAC and have access to resources based on their role and responsibilities.

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

The MSL connects to the NOAA Science Network (N-Wave) (NOAA0550) for internet connectivity. The MSL is primarily a Microsoft Windows Network.

**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.*
- 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 01-2017). *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 01-2019 or later). *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.
- 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.

Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

Yes, the IT system collects, maintains, or disseminates BII.

No, this IT system does not collect any BII.

4. Personally, Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

- DOC employees
- Contractors working on behalf of DOC
- Other Federal Government personnel
- Members of the public

No, this IT system does not collect any PII.

*If the answer is "yes" to question 4a, please respond to the following questions.*

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
--

Provide the legal authority which permits the collection of SSNs, including truncated form.
---

No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

Yes, the IT system collects, maintains, or disseminates PII other than user ID.

No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact

level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

No, the context of use will not cause the assignment of a higher PII confidentiality impact level.


***If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP 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 NOAA5044 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.

<p><b>Information System Security Officer or System Owner</b>  Name: Brian Little  Office: DOC/NOAA/OSPO  Phone: 301-817-3899  Email: Brian.Little@noaa.gov</p> <p style="text-align: right;">Digitally signed by LITTLE.BRIAN.WILLIAM.1365841 230 Date: 2021.07.01 16:10:58 -04'00'</p> <p>Signature: <u>LITTLE.BRIAN.WILLIAM.1365841230</u></p> <p>Date signed: _____</p>	<p><b>Information Technology Security Officer</b>  Name: Rick Miner  Office: DOC/NOAA/NESDIS  Phone: 301-427-8822  Email: Rick.Miner@noaa.gov</p> <p style="text-align: right;">MINER.RICHARD.SCOTT.13 98604519 2021.07.07 08:47:01 -04'00'</p> <p>Signature: <u></u></p> <p>Date signed: _____</p>
<p><b>Privacy Act Officer</b>  Name: Adrienne Thomas  Office: NOAA OCIO  Phone: 240-577-2372  Email: Adrienne.Thomas@noaa.gov</p> <p style="text-align: right;">Digitally signed by THOMAS.ADRIENNE.M.1 365859600 Date: 2021.07.14 13:54:20 -05'00'</p> <p>Signature: <u>THOMAS.ADRIENNE.M.1365859600</u></p> <p>Date signed: <u>59600</u></p>	<p><b>Authorizing Official</b>  Name: Richard Gregory Marlow  Office: DOC/NOAA/OSPO  Phone: (301) 817-4105  Email: Richard.G.Marlow@noaa.gov</p> <p style="text-align: right;">Digitally signed by MARLOW.RICHARD.GREGORY.1522118490 Date: 2021.07.01 16:30:43 -04'00'</p> <p>Signature: <u>MARLOW.RICHARD.GREGORY.1522118490</u></p> <p>Date signed: <u>22118490</u></p>
<p><b>Bureau Chief Privacy Officer</b>  Name: Mark Graff  Office: NOAA OCIO  Phone: 301-628-5658  Email: Mark.Graff@noaa.gov</p> <p style="text-align: right;">Digitally signed by GRAFF.MARK.HYRUM.1 514447892 Date: 2021.07.20 13:43:50 -04'00'</p> <p>Signature: <u>GRAFF.MARK.HYRUM.1514447892</u></p> <p>Date signed: <u>447892</u></p>	