

U.S. Department of Commerce
NOAA



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

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/Mission Support LAN

Unique Project Identifier: 006-000351101 00-00-02-00-02-00

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:

The Mission Support LAN (MSL), formerly known as the NSOF Administrative LAN (NSOF Admin LAN), provides services in support of missions at various NESDIS systems that utilize applicable OSPO enterprise services, and connect to NESDIS Consolidated Administrative LAN in a secure and controlled manner.

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 the MSL is at the NOAA Satellite Operations Facility (NSOF) Suitland, MD. The MSL is located logically and/or physically outside current Mission systems, but for some Mission systems, support data might be required to be exported for analysis, or other functions. Security controls and authentication methods are implemented between the MSL and other systems to ensure that 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 to support Satellite Operation.

The MSL also provides enterprise-level services including Policies and Procedures across FISMA control families, management and oversight of Security Awareness and Role-Based Training, Configuration Management Program, and Incident Management Program. The MSL is a Common Control Provider to other 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.

The MSL consists of four major network segments:

- The Security/Boundary Segment isolates the MSL from the Internet.

- 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 consisting of all MSL workstations

The MSL connects to the NOAA Science Network (N-Wave) (NOAA0550) for connectivity. The MSL is primarily a Microsoft Windows network. Currently, it utilizes Microsoft Windows Active Directory Domain structure called NSOF.NESDIS.NOAA. The MSL consists of four Windows Server Domain Controllers, several file servers, web servers/intranet servers, and a few application servers that host applications including Microsoft SQL Server, ECMT, ECMO Big/Fix Server, McAfee e-Policy Orchestrator Server, DOORS Server, SharePoint, etc. The MSL provides engineering and analysis tools for satellite operations and product processing. Data being processed, stored, and transmitted is restricted to Controlled Unclassified Information.

The MSL network infrastructure is comprised of networking appliances, Firewalls and other security devices, which provide connectivity and redundancy.

Since the last PIA MSL underwent several changes that affected the types of information stored in the system. MSL transitioned from an administrative support system to a mission support system so fewer information types are stored on the system. The PII previously collected such as SSN, driver's license, passport etc. as related to background checks, HR actions, and travel, is no longer stored on MSL. This information is now stored on NOAA5006, which reduces the privacy risk for NOAA5044.

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

MSL users authenticate to the system using their CAC and have access to resources based on their role and responsibilities.

f) A general description of the type of information collected, maintained, use, 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 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

The information on NOAA5044 is retrieved through access rights to the data.

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

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

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		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). *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		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

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.

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 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 Mission Support LAN 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 Mission Support LAN 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): _____

Signature of ISSO or SO: _____ Date: _____

Name of Information Technology Security Officer (ITSO): _____

Signature of ITSO: _____ Date: _____

Name of Privacy Act Officer (PAO): _____

Signature of PAO: _____ Date: _____

Name of Authorizing Official (AO): _____

Signature of AO: Irene Parker _____ Date: _____

Name of Bureau Chief Privacy Officer (BCPO): _____

Signature of BCPO: _____ Date: _____