

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



**Privacy Impact Assessment  
for the  
NOAA5044  
Mission Support LAN (MSL)**

Reviewed by: Mark H. Graff, Bureau Chief Privacy Officer

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer  
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

*Jennifer Goode*

10/06/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

## **U.S. Department of Commerce Privacy Impact Assessment NOAA/NESDIS/Mission Support LAN (MSL)**

**Unique Project Identifier: NOAA5044**

### **Introduction: System Description**

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.

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

NOAA5044 (MSL) is a General Support System (GSS).

*(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 way the system operates to achieve the purpose(s) identified in Section 4*

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.

*(e) 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.

*(f) 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.

*(g) Any information sharing conducted by the system*

Emergency Contact Information is shared for COOP purposes only. A limited subset of information (names, telephone numbers, and email addresses) is shared with Management.

*(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

5 USC 301, 1104, 1302, 2101 to 1210, 2951, 3301, 3321, 3372, 4118, 4305, 5379, 5405, 7531-332, and 8347  
10 USC 8010 to 9448 (Armed Forces Air Force - Organization, Personnel, and Training)  
15 USC 1501 et seq  
15 USC 1512 (Powers and Duties of the Department of Commerce)  
28 USC 533-535  
40 USC 121(c), 501-502  
41 USC 433(d)  
44 USC. 3101  
44 USC 3554, Federal Information Security Management Act of 2002

Executive Orders 9397 as amended Version Number: 01-2015 3 by 13478, 9830, and 12107; 10450, 11478,

12065, 12549, 12564, 12656, 12689, 12931, 13164,

Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204

FAR Subparts 9.4 and 28.2

2 CFR, Subtitle A, Chapter I, and Part 25

5 CFR Part 537

29 CFR parts I, 3, 5, 6 and 7

DAO 202-957

DAO 210 110

Public Law 100-71, dated July 11, 1987.

Federal Preparedness Circular (FPC) 65, July 26, 1999

E- Government Act of 2002 (Pub. L. 107- 347, Sec. 203-204), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283)

Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.)

Government Paperwork Elimination Act (Pub. L. 105 277, 44 U.S.C. 3504 note)

Homeland Security Presidential Directive 12 (HSPD- 12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

Davis-Bacon and Related Acts: 40 U.S .C. 3141 – 3148; 40 U.S.C. 276a;;

Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113 - 101.

Equal Employment Act of 1972.

Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)

*(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

The FIPS 199 Classification for Mission Support LAN(MSL)-NOAA5044 is Moderate.

**Section 1: Status of the Information System**

1.1 Indicate whether the information system is a new or existing system.

This is a new information system.

This is an existing information system with changes that create new privacy risks.

*(Check all that apply.)*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
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.

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).

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).

**Section 2: Information in the System**

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

<b>Identifying Numbers (IN)</b>					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

<b>General Personal Data (GPD)</b>					
a. Name	X	h. Date of Birth		o. Financial Information	

b. Maiden Name	X	i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

<b>Work-Related Data (WRD)</b>					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	X
c. Work Address	X	g. Work History		k. Procurement/contracting records	X
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

<b>System Administration/Audit Data (SAAD)</b>					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

<b>Other Information (specify)</b> Offerer responses to RFIs and RFPs, confidential/proprietary					
--	--	--	--	--	--

2.2 Indicate sources of the PII/BII in the system. (Check all that apply.)

<b>Directly from Individual about Whom the Information Pertains</b>					
In Person	X	Hard Copy: Mail/Fax		Online	X
Telephone		Email	X		
Other (specify):					

<b>Government Sources</b>					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

<b>Non-government Sources</b>					
Public Organizations	<input type="checkbox"/>	Private Sector	<input checked="" type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The Data Custodian of the information is responsible for ensuring the accuracy of the information. Access controls are in place to allow/disallow access to the information. Only those who have a need to know are granted access to PII/BII. PII/BII folders are encrypted. Data is provided directly by the data owners, who validates the validity of the data.

2.4 Is the information covered by the Paperwork Reduction Act?

<input type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
<input checked="" type="checkbox"/>	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. (Check all that apply.)

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</b>			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	--



**Section 3: System Supported Activities**

- 3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.
---	--

**Section 4: Purpose of the System**

- 4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

**Section 5: Use of the Information**

- 5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

- |  |
|--|
| <p>1) There is electronic personnel related information about NOAA employees maintained on the Mission Support LAN, containing information such as Name, Maiden Name, Home Address, Email Address, Job Title, Work Address, Phone Number.</p> <p>2) For contractual purposes, the Mission Support LAN stores contract information, which is stored on a restricted area of the secure shared drive accessible only by authorized personnel.</p> <p>3) The system's audit logs collect user ID, IP Address, Date/Time of Access, Queries Run, and ID Files accessed on the network and stored locally or into restricted areas of the server that are only accessible</p> |
|--|

by authorized personnel. The NOAA Directory collects PII in the form of name, email and contact number for Continuity Of Operations Plan (COOP). This information is stored on the Mission Support LAN and is accessible by authorized personnel only.

4) Environmental Satellite Processing Center (ESPC), NOAA5045, account management processes typically collect name, address, phone number, and email address from NOAA federal employees/contractors or other NOAA offices wishing to access ESPC data via IT distribution mechanisms, or to supply data as may be appropriate. This information is voluntarily submitted through the use of forms or email and is stored on restricted areas of the shared drive only accessible by authorized personnel. The information is collected to ensure the user receives the correct products in line with their request, or to allow an ESPC program manager to validate that a proposed supplier is a legitimate organization able to supply the information being proposed. The information may also be used to notify users and suppliers in the event of an outage or other type of service disruption.

- 5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau’s/operating unit’s use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

All federal employees and contractors with access to privacy data undergo annual training on handling PII. All access to the privacy data is monitored and logged. Insider threats would be a threat to the system, but safe guards are in place to mitigate the threat, such as Least privileges and the need to know, and annual IT Security training which is mandated by all employees.

Data handling and retention security controls are in place that ensure the information is handled, retained, and disposed of properly.

**Section 6: Information Sharing and Access**

- 6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. (Check all that apply.)

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus			
Federal agencies			
State, local, tribal gov’t agencies			
Public			
Private sector			

Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.
--	---

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>MSL has implemented the following controls for preventing and managing PII/BII leakage:</p> <p>NOAA5044 enforces information flow within the system and between interconnected systems using network firewalls.</p> <p>NOAA5044 only allows login access for authorized users, and uses the DOC secure file transfer system, Kiteworks, for sharing sensitive information.</p> <p>NOAA5044 firewalls use a deny-all, permit-by-exception policy for allowing any internal NOAA5044 component to connect to external information systems.</p> <p>NOAA5044 uses Windows Group Policy to manage Data Loss Prevention (DLP) for the NOAA5044/MSL system and its interconnections.</p> <p>NOAA5044 boundaries are protected by firewalls (providing stateful filtering), Intrusion Prevention Systems (IPSs), and packet-filtering Cisco Layer 3 switches that route all incoming and outgoing traffic.</p> <p>NOAA5044 limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.</p> <p>All network traffic is denied unless explicitly allowed through the use of access control list. IPS further looks for and alerts the security group on any abnormal traffic.</p>
---	--

	<p>NOAA5044 utilizes tools such as Intrusion Prevention Systems (IPS), SolarWinds, NetFlow, WebSense, and Firewalls configured to monitor all inbound and outbound traffic for abnormalities that would signal a threat to the MSL.</p> <p>MSL interconnects with the following NOAA information system:</p> <ul style="list-style-type: none"> <li>- NOAA0100, Cyber Security Center</li> <li>- NOAA0550, NOAA Enterprise Network</li> <li>- NOAA5003, Geostationary Operational Environmental Satellite Ground System</li> <li>- NOAA5006, Headquarters Local Area Network</li> <li>- NOAA5026, Polar Operational Environmental Satellite Ground System</li> <li>- NOAA5040, Comprehensive Large Array-Data Stewardship System</li> </ul>
	<p>No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.</p>

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

**Section 7: Notice and Consent**

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: .	
X	Yes, notice is provided by other means.	<p>Specify how:</p> <p>a. For Mission Support LAN COOP or emergency recall in the NOAA directory, employees are notified in writing when collecting the applicable information.</p> <p>b. For ESPC, information is voluntarily submitted when a user completes the account request form.</p>

		c. For responses to solicitations, notice is given on the request for information (RFI) or request for proposal (RFP).
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: a. For Mission Support LAN COOP or emergency recall in the NOAA directory, employees are asked permission in writing by their supervisors when collecting the applicable information, and may decline at that time.  b. For ESPC, information is voluntarily submitted through email and is stored locally. An individual may choose not to provide the information, by not answering the questions, but then will not have access to requested information.  c. Responses to RFPs/RFIs are voluntary, based on the offerer's decision to respond.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: a. For Emergency and COOP information, the employee has the opportunity to consent to particular uses as the COOP related information is created or updated annually.  b. For ESPC, users can consent to particular uses of their PII by contacting the ESPC help desk as stated on the Web page  c. For contract offerers, there is only one use of the BII information provided and acceptance of that use is implied by proposal submission.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: a. For Emergency and COOP information, the employee has the opportunity to annually review or update COOP related information.  b. For ESPC, information can be updated at any time by the
---	---	--

		individual providing PII/BII by contacting the ESPC help desk as stated on the Web page.  c. Offerers will contact the office with updated BII information.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

## **Section 8: Administrative and Technological Controls**

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Logging is in place to record each attempted access attempt to PII/BII.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): <u>12/15/2020</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): As stated in the Mission Support LAN System Security Plan, all employees and contractors undergo a national agency check with inquiries (NACI) security check when employed or contracted. This involves a check of Federal and local law enforcement records to help ensure the trustworthiness of the employee.  The user signs the Mission Support LAN Rules of Behavior (ROB) indicating that they have read and understand the ROB.

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. (*Include data encryption in transit and/or at rest, if applicable.*)

PII/BII is protected through a combination of measures, including operational safeguards, privacy specific safeguards, and security controls. Policies and awareness training are provided annually. The minimum amount of PII necessary to meet the mission is collected. Security controls are in place, such as access controls limiting access to PII/BII. This information has restricted access limited to authorized NOAA staff. Further, if someone that doesn't have access attempts to access to a folder

containing PIUBII, then a failed access log is created. The Mission support LAN has a dedicated drive with user access restrictions for those that store PII/BII.

The Mission Support LAN has NIST 800-53 Rev 4 security controls in place, including, but not limited to: the Access Control family, limiting access to allow only the necessary functions for users to operate within the Mission Support LAN. Account privileges are tied directly to job function and designed to enable the user to accomplish only what the job requires and no more. The Audit and Accountability family utilizes tools such as Tripwire to record, store and manage logs for auditable events. For the Identification and Authentication family, NOAA5044 utilizes two factor to identify and authenticate users. The Media Protection family to monitor access to stored data and the approved sanitation methods for all media.

NOAA5044 uses approved DOD sanitization software to ensure no data remains on NOAA5044 media. NOAA5044 is monitored using various tools including SolarWinds, Nessus, McAfee, and Cisco IPS. Also, NOAA5044 has enterprise monitoring tools, such as FireEye. FireEye is managed by NOAA and provides real time monitoring of potential threats to the system and data.

**Section 9: Privacy Act**

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

Yes, the PII/BII is searchable by a personal identifier.

No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i>  <a href="#">DEPT-18</a> , Employees Information Not Covered by Records of Other Agencies <a href="#">DEPT-25</a> , Access Control and Identity Management System <a href="#">GSA-GOVT-7</a> , Federal Personal Identity Verification Identity Management System (PIV IDMS) <a href="#">GSA-GOVT-9</a> , System for Award Management <a href="#">GSA-GOVT-10</a> , Federal Acquisition Regulation (FAR) Data Collection System
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, this system is not a system of records and a SORN is not applicable.

**Section 10: Retention of Information**

10.1 Indicate whether these records are covered by an approved records control schedule and

monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule:  NOAA Chapter 100 - General NOAA Chapter 200 - Administrative and Housekeeping Records NOAA Chapter 300 - Personnel.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

<b>Disposal</b>			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

### **Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level**

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	<b>Low</b> – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	<b>Moderate</b> – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	<b>High</b> – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals are identifiable by the information collected.
X	Quantity of PII	Provide explanation: Limited PII stored on NOAA5044
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields. Confidential/proprietary information is provided during the procurement process, but access is restricted.
X	Context of Use	Provide explanation: Ability to Perform COOP related activities based on PII provided



	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Physical and logical access controls are in place to restrict access to PII
	Other:	Provide explanation:

## **Section 12: Analysis**

- 12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The information collected for COOP purposes has been deemed the minimum necessary information to adequately support Continuity of Operations for NOAA5044. Insider threats would be a threat to the system, but safeguards are in place to mitigate the threat, such as least privileges and the need to know, and annual IT Security Training, which is mandatory for all employees. NOAA5044 collects less PII/BII since the scope of the system has been reduced to supporting only mission operation systems.

- 12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

- 12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.