Version Number: 01-2017

U.S. Department of Commerce
National Oceanic and Atmospheric Administration
(NOAA)

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

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

11/01/2019

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/MSL

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

Introduction: System Description

General Description - 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) at 4231 Suitland Rd, Suitland Federal Center, Suitland, MD 20746. 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 three major network segments:

- The Security 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 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.

The FIPS 199 classification for MSL (NOAA5044) is moderate.

Authority - Statutory or regulatory authorities for collection and maintenance of the information include:

• 15 USC 1512 (Powers and Duties of the Department of Commerce) 5 USC 2101 to 10210 (Government Organizations and Employees, Part III, Employees) 5 USC 301 (Departmental Regulations)

• 10 USC 8010 to 9448 (Armed Forces - Air Force - Organization, Personnel, and Training)

• 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

• E.O. 9397; E.O. 12931; 40 U.S.C. Sec. 501–502.

• 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended Version Number: 01-2015 3 by 13478, 9830, and 12107.

• 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107–347, Sec. 203), 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.) and 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.

• Sections 1104, 3321, 4305, and 5405 of Title 5, U.S. Code, and Executive Order 12107.

• Federal Acquisition Regulation (FAR) Subparts 4.11 and 52.204 and 2 CFR, Subtitle A, Chapter I, and Part 25, as well as 40 U.S.C. 121(c); FAR Subparts 9.4 and 28.2, Executive Order 12549 (February 18, 1986), Executive Order 12689 (August 16, 1989)

• E-Government Act of 2002 (Pub. L. 107–347) Section 204; Davis-Bacon and Related Acts: 40 U.S.C. 3141–3148 40 U.S.C. 276a; 29 CFR parts 1, 3, 5, 6 and 7; Section 5 of the Digital Accountability and Transparency Act (DATA Act), Public Law 113–101.

• Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

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

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.)*

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):					

_X___ This is an existing information system in which changes do not create new privacy risks, and there is an SAOP approved Privacy Impact Assessment.

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.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	X
b. Taxpayer ID		f. Driver's License	X**	j. Financial Account	X
c. Employer ID		g. Passport	X**	k. Financial Transaction	X**
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	X
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: Navy Performance and award forms require the individual's SSN. The Navy requires SSN in its performance evaluation guidance (document provided with PIA).					

**For CAC ***Contract information

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

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

Other Information (specify)
Offeror responses to RFIs and RFPs, confidential/proprietary

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

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

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

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?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	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	X
Video surveillance		Electronic purchase transactions	X
Other (specify):			

	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	X
For administrative matters	X	To promote information sharing initiatives	X
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)	X	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).

1) There is electronic personnel related information about NOAA employees and prospective employees maintained on the Mission Support LAN, containing information such as SSN, Passport, Credit Card, Vehicle identifier, Name, Maiden Name, Gender, Age, Date of Birth, Place of Birth, Home Address, Telephone Number, Email Address, Financial Information, Military Service, Occupation, Job Title, Work Address, Telephone Number, Work History. In addition, the system maintains onboarding forms, training forms (SF-182), resumes, and vehicle information for parking. The documents are usually completed by the individual or preparer (administrative person that prepares the document for an individual employee). The files are sent to an HR system via DOC KiteWorks, but copies are stored on the Mission Support LAN. This information is not shared with anyone beyond those that are required to process it within the respective bureau.

2) For contractual and budgetary purposes, the Mission Support LAN stores procurement and contract information, purchase requests, and accounting information which is stored locally or in restricted areas of the shared drive accessible only by authorized personnel.

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 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.

4) Environmental Satellite Processing Center (ESPC), NOAA5045, account management processes typically collect name, address, phone number, and email address from individuals or organizations wishing to access ESPC data via its 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 locally or into 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) Performance awards that contain full Social Security Numbers for military and civilians assigned to the Naval Ice Center are stored on the Mission Support LAN. Access to the folder is restricted to those that have a need to know.

5.2 Describe any potential threats to privacy 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.)

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	X	
DOC bureaus	X		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*With OPM if an employee is hired by another agency.

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

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

X	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: NOAA WFMO Recruitment Analysis Data System (RADS). NOAA5044 uploads data in specified formats to RADS. Mission support LAN has media protection controls in place as well as user procedures on how to protect this information.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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.	Specify how: a. Written notice is included on all personnel forms that employees complete. b. For DOC and DOD performance/award documents, employees are informed by their supervisors that the evaluations are in process. Employees have access to view the official documents. c. For Mission Support LAN COOP or emergency recall in the NOAA directory, employees are notified in writing when collecting the applicable information. d. For ESPC, information is voluntarily submitted when a user completes the account request form. 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. An individual may decline to provide PII when applying for a position, by not completing all required forms, but his or her employment status may be affected. b. For DOD and DOC personnel data, employees may opt not to provide PII – at the time of the request, and in writing to the personnel administration representative who is assisting them - but this information is needed for processing awards. Performance information is part of the official personnel record for DOD and DOC employees and information is added to the eOPF in conjunction with the employee mid-year and annual reviews. The performance record/information is required in order to conduct performance evaluations. c. 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. This information is not required.

		d. 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. Responses to RFPs/RFIs are voluntary, based on the offeror'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. There is only one use for information provided during employee onboarding. b. Consent is included on all personnel forms that employees complete, and consent to the uses explained on the forms is implied by completion of the forms. c. For DOD and DOC personnel data, employees may opt not to provide PII – at the time of the request, and in writing to the personnel administration representative who is assisting them, but this information is needed for processing awards. Performance information is part of the official personnel record for DOD and DOC employees and information is added to the eOPF in conjunction with the employee mid-year and annual reviews. The performance record/information is required in order to conduct performance evaluations. This is the only use. d. For Mission Support LAN COOP or emergency recall, there is only one use, and consent to that use is implied by the voluntary provision of the information for that intended use. e. For ESPC, the only use is to provide information as requested. 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. An employee may update information on personnel forms at any time by contacting their HR representative This is explained during employee orientation. b. For DOD personnel data, employees may update their PII by contacting their HR representative, as explained during orientation. Employees review information in the eOPF and notify HR of errors. c. b. For Emergency and COOP information, the employee may not review the information, because it contains other

		staff's PII unless there is need-to-know, but may request updates from the assigned administrative staff, as explained by that staff when requesting the information. d. For ESPC, information can be updated by contacting the ESPC help desk. – as stated on the Web page. Offerors 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: If someone who doesn't have access and attempts to access to a folder containing PII/BII, then a failed access log is created. Audit logs from each computer system are recorded and monitored with various tools including Tripwire, Solarwinds and ArcSight. NOAA5044 has local monitoring tools on the servers having PII, such as FireEye Agent and Tripwire Enterprise/Log Center. FireEye Agent is managed by NOAA to monitor any potential threats to the system and data. Tripwire Enterprise/Log Center provides real time monitoring and threat alerts. Folders containing PII are encrypted.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 12/15/18 ☐ 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 supporting 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 ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify): As stated in the Mission Support LAN (MSL) System Security Plan (SSP), 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 (internal or external) 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 PII/BII, 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 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. *(list all that apply)*: DEPT-13, *Investigative and Security Records* DEPT-18, *Employees Information Not Covered by Records of Other Agencies.* NOAA-11, *Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission*

	OPM/GOVT-1, *General Personnel Records* OPM/GOVT-2, *Employees Performance File Records* GSA-GOVT-6, *GSA SmartPay Purchase Charge Card Program* GSA-GOVT -7, *Federal Personal Identity Verification Identity Management System (PIV IDMS)* GSA-GOVT-9, *System for Award Management* GSA-GOVT-10, *Federal Acquisition Regulation (FAR) Data Collection System*
	Yes, a SORN has been submitted to the Department for approval on (date).
	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.)*

Disposal			
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 as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse

	effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – 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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individuals may be identified based on the PII stored.
X	Quantity of PII	Provide explanation: There is a large amount of PII in the system.
X	Data Field Sensitivity	Provide explanation: There are several types of sensitive PII/BII collected.
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access to PII is restricted to need to know. If someone that doesn't have access attempts to access a folder containing PII/BII, a failed access log is created. NOAA5044 also employs security monitoring tools that can detect PII in unauthorized locations.
	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.)

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.