

**U.S. Department of Commerce  
National Oceanic and Atmospheric Administration  
National Weather Service**



**Privacy Impact Assessment  
for the  
NWS Enterprise Mission Enabling System (EMES)  
NOAA8850**

Reviewed by: Mark 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

for Dr. Catrina D. Purvis

**LISA MARTIN**

Digitally signed by LISA MARTIN  
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of  
the Secretary, cn=LISA MARTIN, o.9.2342.19200300.100.1.1=13001000105292  
Date: 2018.12.07 15:34:32 -05'00'

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

11/27/2018

Date

## **U.S. Department of Commerce Privacy Impact Assessment NOAA8850**

**Unique Project Identifier:** NOAA8850

### **Introduction: System Description**

#### **NOAA8850**

The NWS Enterprise Mission Enabling System (EMES) is defined as a group of complementary enterprise services that provide a secure and reliable infrastructure throughout the NWS organization. EMES consists of Microsoft Active Directory (AD), McAfee ePolicy Orchestrator (ePO), Centralized Certificate Authority (CCA), and Enterprise Cybersecurity Monitoring and Operations (ECMO). Each of these separate products work together to provide authentication, security, reliability, inventory and an overall continuity of enterprise service for NWS staff. These tools ensure that only properly identified network devices connect to the NWS Network; run the latest software; run in a secure environment; and only properly identified and authorized NWS staff gain network access. The system employs redundancy to ensure reliability and availability while reducing latency and bandwidth.

NOAA8850 provides network infrastructure support, management, and connectivity services to the desktop and server customers within the NOAA8850 accreditation boundary, for administrative functions to include:

- Service Desk support,
- Active Directory (AD) services,
- File and print services
- File backup and restoration,
- Network Attached Storage (NAS)
- Dynamic Host Configuration Protocol (DHCP) and IP address space allocation
- Windows Internet Name Services (WINS)
- Domain Name Service (DNS),
- Application distribution and patch management,
- Backup and disaster recovery

In addition, it provides system-level support for servers, desktop computers/workstations, and laptops; and a test lab for systems and network engineers to develop and test new technologies, and to pre-configure new equipment for deployment. Lastly, the NOAA8850 AD user base receives electronic mail and calendar services from the NOAA Messaging Operations Center.

### **Microsoft Active Directory**

Microsoft Active Directory is a special purpose database that authenticates and authorizes all users and computers in a Windows domain network. It is responsible for assigning and enforcing security policies for all computers. Active Directory checks the submitted password and authorizes user access to the system. Multiple Domain Controllers maintain copies of the AD Database and provide redundancy if another Domain Controller is unavailable. Domain Controllers are located in regional offices and key field offices to provide user access and reduce bandwidth.

### **McAfee ePolicy Orchestrator (ePO)**

McAfee ePolicy Orchestrator is an integrated security software program designed to integrate the numerous security programs and to provide real time monitoring of security programs through a single console. McAfee EPO provides end-to-end visibility with a unified view of your security posture, simplified security operations, real-time security status, and an open architecture enabling faster response times.

### **Enterprise Cybersecurity Monitoring and Operations (ECMO)**

U.S. Office of Management and Budget (OMB) memoranda M-10-15 and M-10-19 require all Federal agencies to continuously monitor security-related information from across the enterprise and present this information to the various levels of agency-wide management to enable timely decision making. The ECMO initiative will fulfill this requirement, providing essential, near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness. ECMO will also provide performance metrics to support the administration priority performance areas for continuous monitoring, automated asset management, automated configuration management, and automated vulnerability management.

### **Centralized Certificate Authority (CCA)**

Centralized Certificate Authority issues certificates for day-to-day encryption needs, for encrypting local files and file systems, encrypting the communications between client workstation and servers, as well as server-to-server communication encryption. NOAA8850 utilizes 9 separate types of encryption for protecting information in transit and at rest. The nature of the encryption varies depending on the user need for access to the data, the sensitivity of the data, and the nature of the data being encrypted.

NOAA8850 also includes the National Weather Service Headquarters Local Area Network (NWSHQNet) Infrastructure, which consists of domain controllers, servers, desktop/workstation, laptops, printers and network infrastructure components. The Infrastructure is located within the Silver Spring Metro Complex Building 2 (SSMC-2) and supports approximately 130 users and 380 network devices.

The network infrastructure team provides the support, management and connectivity services for administrative functions to include: Service Desk support, Active Directory, file and print, file backup and restoration, storage, Dynamic Host Configuration Protocol, Windows Internet Name Services, Domain Name Service, IP address space allocation, application distribution and patch management, backup and disaster recovery to the desktop and server customers within the

accreditation boundary. In addition, it provides system-level support for servers, desktops/workstations, and laptops and a test lab mimicking the production environment for systems and network engineers to develop and test new technologies. *All servers are located in the Silver Spring Metro Campus in Maryland.*

### **Multi Year Planning System (MYPS)**

The Multi Year Planning System (MYPS) is comprised of three General Services Systems (GSS) and includes 20 servers (CFO1 servers). The GSS are the MYPS Labor Projection Model, Management Analysis and Reporting System BI Maintenance Platform (MARS), and the General Forecaster Vacancy System. The Labor Projection Model and the General Forecaster Vacancy System are operational production systems. MARS BI Maintenance Platform is used only for maintenance efforts related to the production and pre-production MARS systems which are housed at the NOAA Information Technology Center.

The MYPS Labor Projection Model is a tool used to compute the multi-year total NWS labor five year model using a detailed site-by-site, bottom-up cost approach. It calculates labor costs by site by position with the impact of changes in staffing levels. The model applies a labor lapse, calculates FTE, benefits, premium pay (shift differential), overtime, locality pay, COLA, special IT pay, awards, and annual pay raises. Costs are calculated using OPM-published salary and rates tables. All costs are categorized by ACCS, cost category, funding source, and portfolio. In addition, the model is used in “what-if” analyses to answer questions about proposed changes in labor such as lapse, labor rates, inflation, and table of organization changes. The resulting five year answer sets are used to answer detailed questions about labor planning for NWS, NOAA, DOC, OMB, and Congressional requests. The labor data contained in the model’s database is the master authorized (funded) position data for NWS. The model has its own user logon system and is accessed by its sole user and its maintenance support staff via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network.

MARS is a NOAA enterprise system that provides a common BI platform to all NOAA Line Offices for financial reporting and querying, budget planning and commitment tracking. It consists of two modules, Reporting and Querying and Data Entry. The Data Entry module is not supported by MYPS. The MARS Reporting and Querying module is a business intelligence maintenance environment used for on-going design, creation and testing of new reports; new extract, transform and load (ETL) jobs; and software patches and upgrades for eventual deployment to the Reporting and Querying module of MARS. MARS BI Maintenance Platform is accessible only via the NOAA Silver Spring Metro Campus (SSMC) trusted campus network.

The General Forecaster Vacancy System is a notification system that is used by regional workforce managers to make regional Met Interns aware of upcoming general forecaster vacancies at NWS WFOs, per an agreement between NWS management and the National Weather Service Employees Organization (NWSEO). The system contains a database of all the employees and federal Met Interns in the regions with names, email addresses and GS level (for federal employees). The data base is maintained by the regional workforce managers using a web application which is accessed using LDAP authentication. Prior to posting a vacancy for a general forecaster (meteorologist) at a WFO, the workforce manager in the region uses the system too automatically send an email to all the met interns listed in the database. An intern

who is interested in the listed vacancy clicks on an HTML hyperlink imbedded in the email to express their interest. The system counts the responses and a determination is made at the regional level, based on the number of responses, whether the vacancy will be advertised to status candidates only or to all hiring sources (USAJOBS, etc.). The web portal uses session cookies to time-out any open workforce manager sessions within five minutes to maintain security of the process. PII includes names, email addresses and GS level.

### **The Radar Product Improvement System (RPI)**

The Radar Product Improvement System (RPI) is defined as a testing and development platform for new functionality within Radar Product Generator (RPG), Supplemental Product Generator (SPG) and Advanced Weather Interactive Processing System (AWIPS). Its mission is to aide in the evolution of NOAA's NWS as an agile agency supporting emergency managers, first responders, government officials, businesses, and the public. The strategy is to improve the accuracy and usefulness of forecasts. To do so, RPI provides live radar data feeds from the Air Route Surveillance Radar System (ARSR-4) located in Guantanamo Bay, Cuba, and maintained by the Federal Aviation Administration (FAA). The ARSR-4 for RPI purposes, provides weather processing capabilities levied by RPI to generate Radar products for AWIPS testing. RPI ingests Level 2 radar data from ARSR-4 and generates Level 3 radar products. All data is categorized by FIPS 199 as "Environmental Monitoring and Forecasting".

RPI interfaces with the NWS Enterprise Mission Enabling System (NOAA8850) through the user access switch UA-SW-07103-0701 located at SSMC2, Room 7103. All RPI equipment is government owned and also located at SSMC2, Silver Spring MD.

### **The National AWIPS Program Office (NAPO)**

The National AWIPS Program Office (NAPO) mission is to support activities related to the development of the Advanced Weather Interactive Processing System (AWIPS). Build Servers compile code and ingest live data to assist in the AWIPS process. As a development environment, NAPO provides: build machines for fabricating test Redhat Package Manager (RPMS) and a Network Attached Server (NAS) for backup storage and shared storage.

NAPO features the implementation of live data feeds which support a wide variety of development projects and configurations. The NAPO systems makes available to its developers a live NOAAport SBN feed and a feed from the Ground Segment, over which live weather satellites, GOES16 and GOES17, GOES rebroadcast (GBR) space packets are received.

Authorities from DEPT-13: 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](#); Equal Employment Act of 1972; and all existing, applicable Department policies, and regulations.

Authorities from DEPT-18: 5 U.S.C. 301; 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.

Authorities from DEPT-25: 5 U.S.C. 301; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

Authorities from GSA/GOVT-7: [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); 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.

Authorities from OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

**Information sharing:** Information is shared outside the bureau only if there has been a security breach.

NOAA8850 has a FIPS 199 moderate level rating.

## **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.

  x   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	X*	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):					

**\*NOAA8205 integrated into this system.**

\_\_\_\_\_ 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.

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

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

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

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints		i. Photographs		g. DNA Profiles	
b. Palm Prints		j. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		k. Vascular Scan		i. Dental Profile	
j. 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	
b. IP Address	x	d. Queries Run	X	f. Contents of Files	
l. Other system administration/audit data (specify):					

<b>Other Information (specify)</b>					

- 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		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

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

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

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

MARS PII that is used for development is pulled directly from Production. PII from Forecaster Vacancy is entered by the user. No additional validation is required.
---

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 (TUCBPNPD)			
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	
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*	X
For web measurement and customization technologies (single-session )	X	For web measurement and customization technologies (multi-session )	
Other (specify):			

\*The Forecaster Vacancy System provides employees with available job openings.

### **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).

The MYPS system retains user name, job title and budgeted salary information for the purposes of budget forecast models.

The Forecaster Vacancy system retains name and email only for federal employees and Met interns and GS level for federal employees.

The MARS system retains sample PII for testing purposes only and discards after each testing cycle (destruction of disc after each test).

- 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.)

Privacy is protected both physically and logically. Physically, systems are in a protected environment not accessible to the public. Logically, access to systems is protected via Roble Base Access. Data at rest is encrypted on all laptop computers. Privacy data is to be encrypted via Accellion before being transmitted. Protection of PII is part of the annual Security Awareness and Privacy Training. Potential threats to privacy exist from insiders.

**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 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:  System ID NOAA1101; PII is protected physically through the implementation of badged access to the information system and logically through Role Based Access Controls. Data on laptops is encrypted at rest using AES-256. Sensitive Data, such as PII, is transmitted via Accellion using AES-256 encryption.
	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.
---	--

X	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: internal login pages for MYPS.	
	Yes, notice is provided by other means.	Specify how:
	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: The information collected for Forecaster Vacancy System is provided only if the service is desired.  The information collected by MYPS is solely for budget purposes (no opt out) and MARS collects information solely for testing applications (no opt out).
	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: There is only one use for each of these: MYPS (budget) and MARS (testing).  Forecaster Vacancy is voluntary for job openings and solely consists of user name and email address. There is only one use of the information.
	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: Users are informed in person or in writing by their supervisors at time of onboarding, that they can update PII/information via NOAA LDAP or NOAA Locator. <a href="https://nsd.rdc.noaa.gov/">https://nsd.rdc.noaa.gov/</a>  Forecaster Vacancy user name, email address and MYPS information updates are not applicable for the individual. However, updates may be implemented by HQ and FMC administrators at an individual's request in writing to one or the other.  Employees have access to their information; however, MARS PII is used solely for testing and thus the individual does not need to review/update PII/BII pertaining to them.
---	---	--

	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.*)

	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: MARS has built-in auditor for who accessed what report and when.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): November 14, 2017. <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 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.
x	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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.*)

<p>User name, Office location, and Telephone Number of NOAA employees and contractors are collected and maintained in NOAA8850 Active Directory and LDAP. NOAA8850 Administrators can access or alter this information; the Active Directory is not publicly accessible and has internal boundary controls in place to include firewall and Access Control Lists (ACLs).</p> <p>The MYPS and MARS information is maintained in encrypted files and protected through Role Based Access Controls.</p>
--

## **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. <i>(list all that apply):</i> Provide the SORN name and number <i>(list all that apply):</i> <a href="#">DEPT-13</a> , Investigative and Security Records, <a href="#">DEPT-18</a> , Employees Information Not Covered by Notices of Other Agencies; <a href="#">DEPT-25</a> , Access Control and Identity Management System, <a href="#">GSA/GOVT-7</a> , Personal Identity Verification Identity Management System. <a href="#">OPM/GOVT-1</a> , General Personnel Records
	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 Records Schedule Series Chapter: 900 904-01 Building Identification Credential Files  NOAA Chapter 100: Enterprise-Wide Functions Electronic Records schedule: NARA General Records Schedule 20, Electronic Records
	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		Deleting	x
Other (specify): Destruction of MARS disc after testing completed.			

## **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.
x	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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: The loss of confidentiality could lead to identity theft for individuals affected.
x	Quantity of PII	Provide explanation: All PII collected is done so with the scope minimized to only what data is required to perform the official function.
	Data Field Sensitivity	Provide explanation:
x	Context of Use	Provide explanation: MARS links some PII data using natural keys for SQL table joins which report users cannot see.
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	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.)

<p>To eliminate any potential threats, the load of sensitive data was suspended:</p> <ul style="list-style-type: none"> <li>- Source tables that included PII or other sensitive data were truncated.</li> <li>- Target tables that included PII or other sensitive data were truncated.</li> <li>- Whenever the table was required for development, the PII field was loaded with a dummy variable instead (“-9999999”)</li> </ul>
---

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.

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