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

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

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

Tahira Murphy on behalf of Jennifer Goode 6/15/2022
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
NWS Enterprise Mission Enabling System (EMES)

Unique Project Identifier: NOAA8850

Introduction: System Description

Provide a brief description of the information system.

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.

The following application contains PII/BII in the operation and development systems. (NOAA8850 is responsible for the development side of MARS)

MARS is a web-based financial management and reporting system that was created to serve all financial and administrative components of the National Oceanic and Atmospheric Administration (NOAA). MARS is an automated system for collecting, storing, and retrieving information concerning the financial activities of the Financial Management Centers (FMC's) in NOAA, as well as the Workforce Management information. NOAA financial information is entered into the MARS system through various sources where it is processed and stored. Management and administrative personnel then retrieve this information in the form of reports for analysis. The MARS Development System is an OLAP/ETL development environment used for on-going design, development and testing of new reporting and querying modules, for eventual deployment to Pre-Production and Production in the MARS Reporting and Querying Module.

Address the following elements:

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

EMES is a General Support System (GSS)

(b) System location

EMES is located at 1325 East-West Hwy Silver Spring, MD 20910 (SSMC2)

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

EMES has interconnections with other NWS/NOAA FISMA IDs, including
NOAA0900 – Cloud App
NOAA1011-ITC
NOAA8100- CBITS
NOAA8106-UAOS
NOAA8107-AWIPS
NOAA8202-OWP
NOAA8203-N-PMS
NOAA8860-WCCIS
NOAA8872-MDLNet
NOAA0550-N WAVE
All of NWS Region Headquarters (Alaska Region – NOAA8880, Central Region – NOAA8881, Eastern Region – NOAA8882, Pacific Region – NOAA8883, Southern Region – NOAA8884, Western Region – NOAA8885)

PII data is only shared with NOAA1011-ITC

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

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)
The ECMO provides 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 provides performance metrics to support the administration priority performance areas of 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 Infrastructure, which consists of domain controllers, servers, desktop/workstation, laptops, printers and network infrastructure components and supports approximately 130 users and 380 network devices.

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".

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 that 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.

MYPS

The Multi Year Planning System (MYPS) now referred to as Enterprise Resource Integration Team (ERIT) is comprised of two General Services Systems (GSS) and includes 20 servers (CFO1 servers); the RIMS Labor Projection Model and the Management Analysis and Reporting System BI Maintenance Platform (MARS). The RIMS Labor Projection Model is an operational system and MARS BI Maintenance Platform is used only for maintenance efforts related to the production and pre-production MARS systems which are housed at the NOAA1011- Information Technology Center.

The Resource Information Management System (RIMS) 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. RIMS does not contain any PII/BII information.

The following application contains PII/BII in the operation and development systems. (NOAA8850 is responsible for the development side of MARS)

MARS is a web-based financial management and reporting system that was created to serve all financial and administrative components of the National Oceanic and Atmospheric Administration (NOAA). MARS is an automated system for collecting, storing, and retrieving information concerning the financial activities of the Financial Management Centers (FMC's) in NOAA, as well as the Workforce Management information. NOAA financial information is entered into the MARS system through various sources where it is processed and stored. Management and administrative personnel then retrieve this information in the form of reports for analysis. The MARS Development System is an OLAP/ETL development environment used for on-going design, development and testing of new reporting and querying modules, for eventual deployment to Pre-Production and Production in the MARS Reporting and Querying Module.

(e) How information in the system is retrieved by the user

The MARS Reporting & Querying module is available on the internet. Access to the MARS Data Entry module requires a connection to the NOAA VPN with a Government Furnished Equipment (GFE). Each Account is for the individual use of an identified employee or contractor of NOAA. Accounts remain valid for the duration the individual maintains the relevant status within their organization.

(f) How information is transmitted to and from the system

Information transmitted to and from the system is via the NOAA 0550 N-Wave\TICAP system. If a data transmission involves a privacy consideration, an EMES employee would use the DOC provided secure file transmission system. EMES employee personnel recommend the DOC secure file transfer method as standard practice to receive sensitive data into the system Data on laptops are encrypted at rest using AES-256. Sensitive Data, such as PII, is transmitted via Kiteworks using AES-256 encryption.

(g) Any information sharing conducted by the system

Federal employees and contractors with a NOAA CAC or NOAA email account have access to the information in the system.

EMES share PII information with NOAA1101- Information Technology Center.

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

Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.C. 3101, 3309.

Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and Federal Claim Collection Act of 1966.

5 U.S.C. 5701-09; 31 U.S.C. 951-953, 4 CFR 102.4, FPMR 101-7; Treasury Fiscal Requirements Manual.

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Order 9397 as amended by E.O.13478, E.O 9830, and E.O. 12107,

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

EMES is categorized as a Moderate system.

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):					

____ 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.

X This is an existing information system in which changes do not create new privacy risks, and there is 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.)*

Identifying Numbers (IN)					
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:					

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

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

Distinguishing Features/Biometrics (DFB)					
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):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	f. Queries Run	X	f. Contents of Files	

g. Other system administration/audit data (specify):

Other Information (specify)

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		Other Federal Agencies	
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/BII that is used for development is pulled directly from Production. 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 (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	
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	X
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)	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).

MARS information is used to support the administrative and financial management requirements of NOAA. The PII identified is for federal employees. BII is required for companies providing services to NOAA.

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.)

There is a possibility of insider threat. However, 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 Role Based Access. Data at rest is encrypted on all laptop computers. Privacy data is to be encrypted via Kiteworks before being transmitted. Protection of PII is part of the annual Security Awareness and Privacy Training.

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):NOAA	X		

	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	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: PII data is only shared with 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. Sensitive Data, such as PII, is transmitted via Kiteworks NOAA0900-Cloud App NOAA1011-ITC NOAA8100- CBITS NOAA8106-UAOS NOAA8107-AWIPS NOAA8202-OWP NOAA8203-N-PMS NOAA8860-WCCIS NOAA8872-MDLNet NOAA0550-N WAVE All of NWS Region Headquarters (Alaska Region – NOAA8880, Central Region – NOAA8881, Eastern Region – NOAA8882, Pacific Region – NOAA8883, Southern Region – NOAA8884, Western Region – NOAA8885)
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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.
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: https://www.weather.gov/privacy. .

	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: Federal workers sign a privacy release pursuant to the Privacy Act of 1974 during on-boarding with NOAA and the Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. 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: Federal workers sign a privacy release pursuant to the Privacy Act of 1974 during on-boarding with NOAA and the Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. MARS collects information solely for testing applications (no opt out).
	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.

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: 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.

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: Business objects security tool/report that tracks and monitors analytics and access.
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): 11/30/2021 □ 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.
X	Contracts with customers establish DOC 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).*

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).

MARS information is maintained in encrypted files and protected through Role Based Access Controls.

Section 9: Privacy Act

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

X 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. *(list all that apply)*: COMMERCE/DEPT-18, Employees Information Not Covered by Notices of Other Agencies; COMMERCE/DEPT-25, Access Control and Identity Management System, OPM/GOVT-1, General Personnel Records
	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 Records Schedule Series Chapter: 900 904-01Building Identification Credential Files NOAA Chapter 100: Enterprise-Wide Functions Electronic Records schedule: NARA General Records Schedule 4.1
	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		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.)*

	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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: An individual could be identified by the information collected and stored in this system and could lead to identify 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.
X	Data Field Sensitivity	Provide explanation: Information is restricted to MARs developers admins only
X	Context of Use	Provide explanation: MARS links some PII data using natural keys for SQL table joins which report users cannot see.
X	Obligation to Protect Confidentiality	Provide explanation: Information is restricted to MARs developers admins only
X	Access to and Location of PII	Provide explanation: Information is restricted to MARs developers admins only
	Other:	Provide explanation:

<u>Section 12</u>: 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.)

To eliminate any potential threats, the load of sensitive data was suspended: - Source tables that included PII or other sensitive data were truncated. - Target tables that included PII or other sensitive data were truncated. - Whenever the table was required for development, the PII field was loaded with a dummy variable instead (“-9999999”)

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.