Version Number: 01-2021

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

Privacy Threshold Analysis
for the
NOAA8850
Enterprise Mission Enabling System (EMES)

U.S. Department of Commerce Privacy Threshold Analysis

NWS Enterprise Mission Enabling System (EMES)

Unique Project Identifier: NOAA8850

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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.

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
NOAA1011-ITC
NOAA8100- CBITS
NOAA8106-UAOS
NOAA8107-AWIPS
NOAA8202-OWP
NOAA8203-N-PMS
NOAA8860-WCCIS
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)

d) The purpose that the system is designed to serve

EMES provide enterprise services and a reliable infrastructure throughout the NWS organization. Also, provides network infrastructure support, management, and connectivity services to the desktop and server customers within the NOAA8850 accreditation boundary, for administrative functions.

e) The way the system operates to achieve the purpose

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.

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.

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.

ERIT

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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

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.

g) Identify individuals who have access to information on the system

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

h) How information in the system is retrieved by the user

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.

i) How information is transmitted to and from the system

Information transmitted to and from the system is via the NOAA0550 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non- Anonymous		e New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): An enclave within NOAA8850 no longer collects PII/BII information.					

__X__ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

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

_X_ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when

combined with other information that is linked or linkable to a specific individual."

____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public

_X_ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

_X_ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

_X_ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ The criteria implied by one or more of the questions above **apply** to the **NOAA8850** and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_X_____ The criteria implied by the questions above **do not apply** to the **NOAA8850** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: De Shawn Lewis Office: NWS Phone: 301-427-6994 Email: Deshawn.lewis@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: LEWIS.DESHAWN.TYRELL.1510286541 Digitally signed by LEWIS.DESHAWN.TYRELL.1510286541 Date: 2023.04.20 13:26:44 -04'00' Date signed: _____	**Information Technology Security Officer** Name: Andrew Browne Office: NWS Phone: 301-427-9033 Email: Andrew.browne@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: BROWNE.ANDREW.PATRICK.1472149349 Digitally signed by BROWNE.ANDREW.PATRICK.1472149349 Date: 2023.04.20 14:23:00 -04'00' Date signed: _____
Privacy Act Officer Name: Robin Burress Office: NOAA OCIO Phone: 828-271-4695 Email: Robin.Burress@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.05.12 12:20:59 -04'00' Date signed: _____	**Authorizing Official** Name: Beckie Koonge Office: NWS Phone: 301-427-9020 Email:Beckie.koonge@noaa.gov I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: KOONGE.BECKIE.A.1408306880 Digitally signed by KOONGE.BECKIE.A.1408306880 Date: 2023.04.26 15:21:26 -04'00' Date signed: _____
Bureau Chief Privacy Officer Name: Robin Burress FOR Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: Mark.Graff@noaa.gov I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: BURRESS.ROBIN.SURRETT.1365847696 Digitally signed by BURRESS.ROBIN.SURRETT.1365847696 Date: 2023.05.12 12:38:38 -04'00' Date signed: _____	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.