Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the

NOAA0700

High Availability Enterprise Services (HAES)

U.S. Department of Commerce Privacy Threshold Analysis

NOAA/OCIO/High Availability Enterprise Services

Unique Project Identifier: NOAA0700

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: HAES is comprised of three components: Identity Credentialing Access Management (ICAM), Enhanced Security Administrative Environment (ESAE), and the NOAA Enterprise Active Directory (NEAD). The ICAM component will provide a centralized Enterprise service for the NOAA community. The ICAM team provides the following services:

- Single Sign On (SSO): Access Manager for authenticating users:
  - Supports all current web standards: SAML, WSFed, OIDC, WebAuthn, OAuth, FIDO/U2F.
  - Capability to support legacy applications: proxy or agent.
  - DOC SAML Proxy for all the Bureaus.
  - Microsoft Azure Cloud Federation
  - SSO for NOAA users to Azure Commercial / Office 365 via AD connect

- Identity Management (IDM): manages account attributes:
  - Provides identity synchronization, reconciliation, workflow, and self-service interfaces.
  - Identity sync with NOAA Staff Directory (NSD), NOAA AD, GDS and Google.
  - Data consistency and standardization and policy enforcement.

- Directory (LDAP): datastore for accounts:
  - LDAPv3 compliant service in multi-master replication.
  - Web application with ability to manage groups and search and export LDAP entries for users/groups.
  - Manage about 47K objects for people and groups.

- Public Key Infrastructure (PKI):
  - Provide X509 certificates using the DoD PKI.
  - Provide certificates validation service. Approximately 1 million queries per day
  - Operate NOAA VA Root for validation infrastructure

  - Validation infrastructure: 3 Responders and 4 Repeaters

- Mail Transfer Agent (MTA): Provide mail relay service for three NOAA internal offices:
  - NWS NCEP/SWPC
  - NWS OBS/ROC
  - NWS NCEP/NCO

- Google Sync:
  - Synchronize identity data to NOAA's Collaboration suite provided by Google.

The ESAE component provides a secure enterprise deployment of Active Directory for protecting privileged access to NOAA Active Directory instances. ESAE is deployed to two sites and provides the following for the NOAA community:

- Secure, encrypted, administrative bastion forest separate from production forest
- Protects Enterprise and Domain level credentials from compromise and ensures quick recovery of Forest / Domains in event of compromise.
- Provides secure, Privileged Access Workstations (PAW) from which Enterprise and Domain level admin duties are completed.

NEAD provides support for SSO services to Azure Commercial / Office 365

- A separate domain (NEAD) is used to receive identities from ICAM and then, via AD connect, sync those identities to Azure AD in Azure Commercial / Office 365
- The domain NOAA.GOV is federated with Azure Commercial in order to enable the use of smart cards (NOAA CAC) when using Azure services in Azure Commercial.
- This setup leverages ICAM for SSO to Azure Services.

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).

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

HAES (NOAA0700) is a General Support System (GSS).

b) System location

The three systems that comprise HAES are outlined in the table below:

Address	System		
	ICAM	**ESAE**	**NEAD**
Level 3 Communications (ICAM North) 1850 Pearl St. Denver CO 80203	**X**		
Silver Spring Metro Center Building 3 (SSMC), 1315 East West Highway, Silver Spring, MD 20910	**X**		
ICAM West & ESAE West, 7600 Sand Point Way, Seattle, WA 98115	**X**	**X**	**X**
ICAM Pacific, 1845 Wasp Boulevard, Honolulu, HI 96818	**X**		
NOAA Environmental Security Computing Center (NESCC), 100 Galliher Drive, Fairmont, WV 26554		**X**	**X**

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

The ICAM system uses the following connections:

1. LDAPS connection to DOD Global Directory Service (GDS) for obtaining NOAA user's CAC information e.g. EDIPI, certificate, UPN and CN.
2. Connection to the CorpServ (NOAA1200) Active Directory system
3. Database connection to NOAA Staff Directory (NSD) to push new accounts and update accounts status.
4. LDAPS connection to NOAA Enterprise Active Directory (NEAD) to create, update and delete accounts.
5. A connection to Google Sync Service
6. K2Share for CSAT training status

The ESAE system resides on its own sub-network with its own limited IP range. This minimizes accessibility to system components and limits it to only those persons who have specifically provided access capabilities by way of access lists.

Where internal system connections are appropriate, HAES defines classes of components to be authorized, authorizes these, and defines the interface characteristics, the security requirements, and the nature of the information communicated.

NEAD has its own subnets in Fairmont and Seattle. NEAD currently has the following connections:

1. LDAPS connection to ICAM for account sync
2. Connection to Azure Commercial via AD Connect
3. Connection to ESAE for monitoring

ICAM-to-ICAM Ports:

The following ports only need access to and from other ICAM hosts. This is for backchannel communication, replication:

- 8989 (Open DJ replication)
- 4444 (DJ only)
- 50389 (ONLY in multi-node OpenAM installations. For single-node OpenAM, it can be host only.)

The following ports only need IPC / localhost access on this host itself:

- 50389 (AM local data store)
- 1689 (OpenAM JMX Session Queue - see note above.)
- 8005 (OpenAM and WhitePages only: Tomcat shutdown ports)

ESAE end users and applications access the unified information via:

- IPSEC (UDP 500, TCP 50)

NEAD

- 636 (LDAPS connection to ICAM for identity sync)
- 443 (Encrypted connection Azure Commercial via AD Connect for AD user sync)

d) The purpose that the system is designed to serve

The Homeland Security Presidential Directive (HSPD)-12 PKI infrastructure was built for all Line Offices and system owners to implement 2-Factor Authentication (2FA) on their Microsoft domains. The ICAM team employed an architecture to unify the identity stores and correlate all enrollment processes in NOAA and DOD. ICAM provides Identify Management Services and Systems (IDMS) and Single Sign-On (SSO) solutions to Line Offices and System Owners. The ICAM system operates a set of servers to manage and serve information that assists in the implementation of the HSPD-12 mandates for NOAA.

The Enhanced Security Administrative Environment (ESAE) is designed to enhance security of the NOAA Active Directory production environment by limiting the exposure of privileged administrative credentials. NOAA believes this implementation will improve the likelihood of avoiding significant financial, reputation, and operational impacts of potential future security breaches. The business impact from a successful malicious compromise of an organization's information systems can vary greatly from organization to organization and may encompass a wide spectrum of negative outcomes. Some of the impacts that have been experienced by organizations suffering from modern cyber-attacks include:

- Loss of reputation
- Significant cost of recovery and remediation
- Reduction in revenue
- Loss of competitive advantage
- Unauthorized reproduction of proprietary designs or other intellectual Property

ESAE is designed to thwart cyber-attackers business impact by mitigating credential theft techniques as well as several other known attack techniques. NOAA believes this will improve the likelihood of avoiding significant financial, reputation, and operational impacts of potential future security breaches.

NEAD is currently a Windows AD based resource forest that is used to facilitate the syncing of NOAA identities that originate from ICAM which are, in turn, synced to Azure Commercial via an AD Connect Agent. This syncing of identities allows a modification to occur so the use of SSO in Azure Commercial with ICAM is possible. NEAD places a pivotal role in allowing NOAA users in Azure Commercial to be able to use their NOAA issued CAC credentials as a multi-factor token so they can securely access cloud-based services like Microsoft 365, Dynamics 365, SharePoint Online, Power Bi and other Microsoft Cloud offerings.

e) The way the system operates to achieve the purpose

ICAM primarily operates a set of Dell servers deployed across 4 geographically separated sites for ICAM, and two sites for ESAE and NEAD. The ICAM component will provide a centralized enterprise service provides the following for the NOAA community:

- Identity Management (IDM)
- Single Sign On (SSO)
- Federation (SAML/OIDC)
- Directory (LDAP)
- Public Key Infrastructure (PKI)

The ESAE component provides a secure enterprise deployment of Active Directory on Dell servers for protecting privileged access to NOAA Active Directory instances. ESAE is deployed to two sites and provides the following for the NOAA community:

- Secure, encrypted, administrative bastion forest separate from production forest
- Protects Enterprise and Domain level credentials from compromise and ensures quick recovery of Forest / Domains in event of compromise.
- Provides secure, Privileged Access Workstations (PAW) from which Enterprise and Domain level admin duties are completed.

NOAA Enterprise Active Directory (NEAD) is currently a Windows AD based resource forest that is used to facilitate the syncing of NOAA identities that originate from ICAM which are, in turn, synced to Azure Commercial via an AD Connect Agent. This syncing of identities allows a modification to occur so the use of SSO in Azure Commercial with ICAM is possible. NEAD places a pivotal role in allowing NOAA users in Azure Commercial to be able to use their NOAA issued CAC credentials as a multi-factor token so they can securely access cloud-based services like Microsoft 365, Dynamics 365, SharePoint Online, Power Bi and other Microsoft Cloud offerings. NEAD is currently deployed in data centers in Fairmont, WV and Seattle, WA.

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

ICAM is a set of tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources. The ICAM system collects, maintains, and disseminates PII about DOC employees and contractors working on behalf of the

DOC. ICAM is available for use to any approved, government CAC holder. ICAM collects, maintains, and disseminates information such as:

1. User ID
2. First Name
3. Last Name
4. Personal address
5. Work Phone number
6. Work Street Address
7. Work Email Address
8. Occupation
9. Job Title
10. IP Address
11. Date/Time of Access to the system
12. Queries
13. Other system administration and data collected by NOAA0700 are:

System	Audit Records
SSO.noaa.gov	● User Login ● User Login failures ● User Account lock
whitepages.noaa.gov	● Binds ● Query ● Modification of objects
Accounts.noaa.gov	● Account actions (Create, Update, Delete)

The ESAE component maintains a secure enterprise Active Directory forest for protecting privileged access to NOAA Active Directory instances.

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

ICAM is available to the DOC user community as well as external federal government personnel. The systems are available for use to any approved, government CAC holder. ICAM servers provide information for the NOAA community in the NOAA Whitepages, which is NOAA's directory service. ICAM is a datastore for accounts and provides a web application with the ability to manage groups, search, and export LDAP or user entries for users/groups. There is no public access to the ESAE or NEAD systems. Only approved personnel have access to ESAE and NEAD.

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

Access to the ICAM system is publically accessible and may be done through Government Furnished Equipment (GFE) and the Internet. There is no public access to the ESAE or NEAD systems. Only approved personnel have access to ESAE or NEAD.

i) How information is transmitted to and from the system

The ICAM services all utilize secure protocols HTTPS and LDAPS for users. Administrators utilize secure protocol SSH to manage systems only through VPN. Access to ESAE services are restricted to only ESAE Engineers and Line Office (LO) administrators who use its services in order to access their specific networks. All access is done through a hardened Privileged Access Workstation using 2-Factor Authentication (FA) and IPsec 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.*

_X_ 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	X
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. *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."

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

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

____ 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?

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

____ 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

__X__ The criteria implied by one or more of the questions above apply to the NOAA0700 and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

_____ The criteria implied by the questions above **do not apply** to the NOAAXXXX 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: Jung Lee Office: NOAA OCIO Phone: 301-233-1202 Email: jung.lee@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: Jung Lee Date: 2022.01.20 16:39:48 -05'00' Date signed: 01/20/2022	**Information Technology Security Officer** Name: Ansaruddin Hasan Office: NOAA OCIO Phone: 202-964-0871 Email: ansaruddin.hasan@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: HASAN.ANSARUDDIN.ISA.13768162 Digitally signed by HASAN.ANSARUDDIN.ISA.1376816210 Date: 2022.01.24 08:00:34 -05'00' Date signed: 10
Privacy Act Officer Name: Adrienne Thomas Office: NOAA OCIO Phone: 828-257-3148 Email: Adrienne.Thomas@noaa.gov I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2022.02.02 11:50:31 -06'00' Date signed: 600	**Authorizing Official** Name: Doug Perry Office: NOAA OCIO Phone: 301-713-9600 Email: douglas.a.perry@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: PERRY.DOUGLAS.A.1365847270 Digitally signed by PERRY.DOUGLAS.A.1365847270 Date: 2022.02.01 14:54:51 -05'00' Date signed: 270
Bureau Chief Privacy Officer Name: 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: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2022.02.03 11:26:19 -05'00' Date signed: 447892	