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/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 two components: Identity Credentialing Access Management (ICAM) and the Enhanced Security Administrative Environment (ESAE). 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.

- Identity Management (IDM): manages account attributes:
  - Provides identity synchronization, reconciliation, workflow, and self-service interfaces.
  - Identity sync with NEMS, 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 group and search and export LDAP entries for users/groups.
  - Manage about 47K objects for people and groups.

- Public Key Infrastructure (PKI): DoD
  - Provide X509 certificates using the DoD PKI. 2500 PKI requests in 2019: 1700 Server certs, 780 Alt Tokens.
  - Provide certificates validation service. Approximately 1 million queries per day
  - Operate NOAA VA Root for validation infrastructure
  - Validation infrastructure: 3 Responders: SSMC, Seattle, Denver and 4 Repeaters: SSMC, Seattle, Denver, Dallas
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.

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 two systems that compromise HAES are outlined in the table below:

<table>
<thead>
<tr>
<th>Address</th>
<th>HAES Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ICAM</td>
</tr>
<tr>
<td>Level 3 Communications (ICAM North), 1850 Pearl St. Denver CO 80203</td>
<td>X</td>
</tr>
<tr>
<td>Silver Spring Metro Center Building 3 (SSMC), 1315 East West Highway, Silver Spring, MD 20910</td>
<td>X</td>
</tr>
<tr>
<td>Level 3 Communications (ICAM South), 400 South Akard Street Dallas, TX 75202</td>
<td>X</td>
</tr>
<tr>
<td>ICAM West &amp; ESAE West, 7600 Sand Point Way, Seattle, WA 98115</td>
<td>X</td>
</tr>
<tr>
<td>ICAM Pacific, 1845 Wasp Boulevard, Honolulu, HI 96818</td>
<td>X</td>
</tr>
<tr>
<td>NOAA Environmental Security Computing Center (NESCC), 100 Galliher Drive, Fairmont, WV 26554</td>
<td>X</td>
</tr>
</tbody>
</table>

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 Enhanced Security Administrative Environment (ESAE) system.
3. Connection to the CorpServ (NOAA1200) Active Directory system
4. Database connection to NOAA Staff Directory (NSD) to push new accounts and update accounts status.
5. LDAP connection to NOAA Enterprise Active Directory (NEAD) to create, update and delete accounts.
6. A connection to Google Sync Service
7. 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.

ICAM-to-ICAM Ports:

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

- 8989 (DS replication)
- 4444 (DS only)
- 50389 (AM internal DS)
- Host-Local Ports

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

- 50389 (AM local data store)

ESAE end users and applications access the unified information via:

- IPSEC (UDP 500, TCP 50)

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.

e) The way the system operates to achieve the purpose

HAES primarily operates a set of Dell servers deployed across 5 geographically separated sites for ICAM and two sites for ESAE. 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 servers 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.

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

The ICAM system collects, maintains, and disseminates PII about DOC employees and contractors working on behalf of the DOC. ICAM collects and maintains several common attributes such as:

1. User Name
2. Last Name
3. Phone number
4. Street Address
5. Email Address

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

The DOC user community as well as external federal Government personnel.
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 system. Only approved personnel have access to ESAE.

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 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.*

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

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>d. Significant Merging</td>
</tr>
<tr>
<td>e. New Public Access</td>
</tr>
<tr>
<td>f. Commercial Sources</td>
</tr>
<tr>
<td>g. New Interagency Uses</td>
</tr>
<tr>
<td>h. Internal Flow or Collection</td>
</tr>
<tr>
<td>i. Alteration in Character of Data</td>
</tr>
<tr>
<td>j. Other changes that create new privacy risks (specify):</td>
</tr>
</tbody>
</table>

___  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 (version 01-2015 or 01-2017). *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 (version 01-2019 or later). *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.

___  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.)

<table>
<thead>
<tr>
<th>Activities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio recordings</td>
<td>Building entry readers</td>
</tr>
<tr>
<td>Video surveillance</td>
<td>Electronic purchase transactions</td>
</tr>
<tr>
<td>Other (specify):</td>
<td></td>
</tr>
</tbody>
</table>

___ 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.

___ 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

___ 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.

___ 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.

___ 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.

___ 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  I certify the criteria implied by one or more of the questions above apply to the High Availability Enterprise Services and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above do not apply to the High Availability Enterprise Services 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: Kevin Mitchell
Office: NOAA OCIO
Phone: 301-628-5952
Email: kevin.mitchell@noaa.gov

Information Technology Security Officer
Name: Charles Obenschain
Office: NOAA OCIO
Phone: 240-533-9555
Email: charles.obenschain@noaa.gov

Privacy Act Officer
Name: Adrienne Thomas
Office: NOAA OCIO
Phone: 828-257-3148
Email: Adrienne.Thomas@noaa.gov

Authorizing Official
Name: Doug Perry
Office: NOAA OCIO
Phone: 301-713-9600
Email: douglas.a.perry@noaa.gov

Bureau Chief Privacy Officer
Name: Mark Graff
Office: NOAA OCIO
Phone: 301-628-5658
Email: Mark.Graff@noaa.gov