Template Version Number: 01-2021

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

Privacy Impact Assessment
for the

NOAA0700

High Availability Enterprise Services (HAES)

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CHARLES CUTSHALL
Digitally signed by CHARLES CUTSHALL
Date: 2024.05.28 17:02:22 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/OCIO/ High Availability Enterprise Services

Unique Project Identifier: NOAA0700

Introduction:

HAES is comprised of four components: Identity Credentialing Access Management (ICAM), Enhanced Security Administrative Environment (ESAE), NOAA Enterprise Active Directory (NEAD), and NOAA BigFix Services (NBFS).

The ICAM component will provide a centralized Enterprise service for the NOAA community. The only publicly accessible PII is via the active directory managed by ICAM. The ICAM team provides the following services:

- Single Sign On (SSO): Access Manager for authenticating users:
  - Supports all current web standards: Security Assertion Markup Language (SAML), Web Services Federation (WSFed), OpenID Connect (OIDC), Web Authentication (WebAuthn), Open Authorization (OAuth), Fast Identity Online 2/Universal 2nd Factor (FIDO2/U2F).
  - Capability to support legacy applications: proxy or agent.
  - DOC SAML Proxy for all the Bureaus.
  - SSO to Microsoft Azure Cloud Services Federation
  - NOAA identity synchronization to Microsoft Azure Services (M365) via AD Connect
  - SSO to Amazon Web Services (AWS) Commercial Cloud Services Federation

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

- Directory Lightweight Directory Access Protocols (LDAPS): datastore for accounts:
  - LDAPSv3 compliant service in multi-master replication.
  - Web application with ability to manage groups and search and export LDAPS entries for users/groups.
  - Manage about 47K objects for people and groups.

- Public Key Infrastructure (PKI):
  - Provide X509 certificates using the Department of Defense (DOD) PKI.
  - Provide certificates validation service. Approximately 1 million queries per day

  - Operate NOAA Validation Authority (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:

  - National Weather Service (NWS) National Centers for Environmental Prediction (NCEP)/Space Weather Prediction Center (SWPC)
  - NWS Office of Observations (OBS)/Radar Operations Center (ROC)
  - NWS NCEP/NCEP Central Operations (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 three 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.

NBFS is a multilayered platform that assists NOAA in managing computers running on different operating systems. The platform offers capabilities that assist the Bureau in further certifying data collected from NOAA endpoints and reinforcing the Bureau's management over its IT infrastructure.

Address the following elements:

(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 four systems that comprise HAES are outlined in the table below:

Locations	System			
	ICAM	**ESAE**	**NEAD**	**NBFS**
NOAA-OCIO-EDC Boulder, CO	**X**	**X**	**X**	**X**
Level 3 Communications (ICAM North) Denver, CO	**X**			
Silver Spring Metro Center Building 3 (SSMC) Silver Spring, MD	**X**			
ICAM West & ESAE West Seattle, WA	**X**	**X**	**X**	
NOAA Environmental Security Computing Center Fairmont, WV		**X**	**X**	**X**
Microsoft Azure Government, NOAA OCIO Tenant, Virginia Datacenter				**X**
NOAA EDC Data Center Ashburn, VA	**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. Electronic Data Interchange Personal Identifier (EDIPI), certificate, User Principal Name (UPN) and Common Name (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 Cybersecurity Awareness Training (CSAT) training status
7. Connection to N-Wave

The ESAE system resides on its own sub-network with its own limited IP range. This minimizes access 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, Boulder, 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 conducts the following for backchannel communication and replication:

- DS replication
- DS only
- Multi-node OpenAM installations

For ICAM, the following only need inter-process communication (IPC)/localhost access on this host itself:

- AM local data store
- AM JMX Session Queue
- AM and WhitePages only: Tomcat shutdown ports

ESAE end users and applications access the unified information via:

- Internet Protocol Security (IPSEC)

NEAD

- LDAPS connection to ICAM for identity sync
- Encrypted connection Azure Commercial via AD Connect for AD user sync

NBFS

- TCP/UDP Encrypted connection
- Encrypted connection to HCL for content retrieval from HCL vendor – outbound only

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

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

- IDM
- SSO
- SAML/OIDC
- LDAPS
- 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 three 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 plays 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 at three sites.

NBFS is a multilayered platform that assists NOAA in managing computers running on different operating systems. The platform offers capabilities that assist the Bureau in further certifying data collected from NOAA endpoints and reinforcing the Bureau's management over its IT infrastructure.

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

In regards to the ICAM system, only the directory is publicly accessible, through Government Furnished Equipment (GFE) and the Internet. There is no public access to the ESAE, NEAD, or NBFS systems. Only approved personnel have access to ESAE, NEAD, and NBFS.

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

The ICAM services all utilize secure protocols Hypertext Transfer Protocol Secure (HTTPS) and LDAPS for users. Administrators utilize secure protocol Secure Shell (SSH) to manage systems only through a Virtual Private Network (VPN). Access to ESAE and NEAD services and information are restricted to only ESAE Engineers and Line Office (LO) administrators, who use its services to access their specific networks. All access is done through a hardened Privileged Access Workstation, using 2-Factor Authentication (FA) and IPsec encryption. For NBFS, Azure Virtual desktop is used by users to access data and the system utilizes proprietary encrypted data transfer protocols. Scheduled reports are distributed by email using NOAA unified messaging services (UMS) email servers. The ESAE component provides a secure enterprise deployment of Active Directory for protecting privileged access to NOAA Active Directory instances. The only publicly available PII is Active Directory within ESAE.

(g) Any information sharing conducted 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. Middle Name
4. Last Name
5. Personal address
6. Work Phone number
7. Work Address
8. Work Email Address
9. Occupation
10. Job Title
11. Employee Type
12. Organizational data (bureau, line office, etc., manager; employee number; DOD ID)
13. Activity timestamps for password changes, logins and Security Awareness training
14. Personal Identification Verification (PIV)/Common Access Card (CAC) encryption public certificate(s)
15. Password
16. IP Address
17. Date/Time of access to the system
18. Queries/Actions
19. 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)

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

	Type of Information Collected (Introduction h.)	**Applicable SORNs (Section 9.2)**	**Programmatic Authorities (Introduction h.)**
1.	Badging & CAC Issuance	COMMERCE/DEPT-18	Electronic Signatures in Global and National Commerce Act, Public Law 106-229
			5 U.S.C. 301
		GSA/GOVT-7	5 U.S.C. 301
			Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
			Federal Information Security Management Act of 2002 (44 U.S.C. 3554)
			E-Government Act of 2002 (Pub. L. 107–347, Sec. 203)
2.	Info Collected Electronically in Connection w/ DOC Activities, Events & Programs	COMMERCE/DEPT-23	15 U.S.C. § 272
			15 U.S.C. § 1151
			15 U.S.C. § 1512
			15 U.S.C. § 1516
			E.O. 11625
3.	System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
			Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
			Electronic Signatures in Global and National Commerce Act, Public Law 106-229
			28 U.S.C. 533-535

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

The NOAA0700 overall Security Categorization (SC) is High.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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): New NOAA EDC Data Center located in Ashburn, VA, processes PII/BII. Connection to N-Wave is not new, simply overlooked on previous PIA.					

_____ 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.

_____ 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): DOD ID.					
*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		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Physical Characteristics	
f. Race/Ethnicity		m. Education		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		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): Job Title, Employee Type.					

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	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X

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

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)

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	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

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

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

NOAA0700 systems ensure that access to these systems and services is controlled through implementation of policy, procedures and security controls that mitigate the risk of unauthorized access to NOAA's information or information systems.

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	The IT system does not support 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	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify): ICAM runs a Single Sign On (SSO) service for NOAA personnel. The ESAE component provides a secure enterprise deployment of Active Directory on Dell servers for protecting privileged access to NOAA Active Directory instances. The ESAE component provides a secure enterprise deployment of Active Directory on Dell servers for protecting privileged access to NOAA Active Directory instances.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The NOAA0700 FISMA system (ICAM) collects all PII via web forms from various IT Service Desks throughout NOAA to provide Single Sign On (SSO) and Identity Management (IDM) services. These services cover only employees, contractors, and affiliates of NOAA. The only information collected via the web forms is work related and falls within the employee's/contractor's duties of employment. The ESAE, NEAD, and NBFS components of NOAA0700 do not collect, maintain, or disseminate PII/BII.

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.)

ICAM is secured against possible security threats by people, technology, and operational components of the system through the use of security-based design principles such as:

- Fail-safe defaults (set default access to none and require security privileges to be specifically granted).
- Separation of privilege (require multiple conditions to be met before granting

permission). See AC family of controls.
- Defense in depth (layered protections)
- Packet filtering router with gateway.
- Layered or device-specific Access Control Lists (ACLs) are implemented whenever possible to provide access control and protection of ICAM systems.
- By addressing these principles, ICAM is less likely to fall into an unprotected and vulnerable state. Through user training and awareness, policies and procedures, and the use of redundant operational protection measures, effective protection of the system is accomplished.
- ICAM system administrators rely on Ansible scripts for automated configuration management to ensure appropriate security controls are met prior to implementation.

ESAE is a legacy system and is secured against possible security threats by people, technology, and operational components of the system through the use of security-based design principles.

NEAD is secured against possible security threats by people, technology, and operational components of the system through the use of security-based design principles.

NBFS is secured against possible security threats by people, technology, and operational components of the system through the use of security-based design principles.

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		X	
Federal agencies			X
State, local, tribal gov't agencies			
Public			X*
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Public can only access the directory.

	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.
X	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	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: • LDAPS connection to DOD Global Directory Service (GDS) for obtaining NOAA user's CAC information e.g. EDIPI, certificate, UPN and CN. • Connection to the CorpServ (NOAA1200) Active Directory system • Database connection to NOAA Staff Directory (NSD) to push new accounts and update accounts status. • LDAPS connection to NOAA Enterprise Active Directory (NEAD) to create, update and delete accounts. • A connection to Google Sync Service • K2Share for CSAT training status • Connection to N-Wave 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. ESAE is under the NOAA0700 umbrella. NEAD has its own subnets in Fairmont, Seattle, and Boulder. 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 NBFS communicates with any system that has the agent installed, but does not process PII/BII.
	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	X*	Government Employees	X
Contractors	X		

Other (specify): *Public can only access the directory.

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://whitepages.noaa.gov/whitepages/#/privacy_act_statement. However the site is not publicly accessible. See the PAS at the end of this document; which is located on the web page.	
X	Yes, notice is provided by other means.	Specify how: Employees and contractors are provided notice on the applicable HR forms when onboarding.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: As detailed in the privacy policy outlined in Question 7.1

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: As detailed in the privacy policy outlined in Question 7.1

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Via accounts.noaa.gov, individuals can update their zip code, telephone, mobile number, and address.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

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: NOAA0700 maintains audit records which can be tracked, monitored, and recorded.
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): * May 30, 2023 ☐ 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).*

System Administration access to ICAM servers is through a VPN requiring 2- Factor Authentication (2-FA) using FIPS 140-2 validated SSL. ICAM personnel are issued an Admin token (DOD Alt Token) for login to servers. All data is encrypted during transmission using a FIPS validated module. Sensitive data at rest is encrypted at rest using a FIPS validated module. Only approved system administrators have access to the ESAE, NEAD, and NBFS systems.

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 Personnel Files Not Covered by Notices of Other Agencies. COMMERCE/DEPT-23: Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs. COMMERCE/DEPT-25: Access Control and Identity Management System. GSA/GOVT 7: HSPD-12 USAccess
	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: 201-01b2: Records Maintained by NOAA Line and Staff Offices. DAA-0370-2015-0006-0004 (03/04/16) 201-05: Information Technology Development Project Records. (Feasibility Studies) DAA-GRS-2013-0050007 (GRS 3.1, item 011) 2400-01: Systems and Data Security Records. DAA-GRS-2013-0006-0001 (GRS 3.2, item 010) 2400-02: Computer Security Incident Handling, Reporting and Follow-up Records. DAA-GRS-2013-0006-0002 (GRS 3.2, item 020) 2400-03: System Access Records. 2400-04a: Incremental backup files (System Backups and Tape Library Records). DAA-GRS-2013-0006-0005 (GRS 3.2, item 040) 2400-04b: Full backup files. (System Backups and Tape Library Records). DAA-GRS-2013-0006-0006 (GRS 3.2, item 041) 2400-06: PKI Administrative records.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing	X	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.)*

X	**Low** – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	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: minimal admin information for IT work identity.
X	Quantity of PII	Provide explanation: minimal work contact.
X	Data Field Sensitivity	Provide explanation: no sensitive data fields.
X	Context of Use	Provide explanation: minimal data for IT user identification.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: PII is located on the directory, which is the only part only part of the system that is publicly accessible
X	Continuity of Operations	Loss of system availability would have a severe adverse effect on the NOAA0700 subsystems services. Continuity of Operations is critical to this system; HAES would need to continue operations of all systems in the event of an outage.
X	Record Retention	The ESAE subsystem enhances security of the NOAA Active Directory production environment by limiting the exposure of privileged administrative credentials.
X	Help Desk Services	Help Desk Services are provided by the NOAA0700 ICAM subsystem at the Tier 3 level. Interconnected systems help desks require this level of escalation in the event an issue cannot be resolved at the Line Office (LO) or System Owner (SO) level.
X	System Maintenance	The NOAA0700 ICAM subsystem is responsible for the system maintenance of all systems that it hosts on behalf of the LO's and SO's. System Maintenance is provided as a service to its customers as part of a standard Service Level Agreement.
X	Information System Security	In providing NOAA with enterprise Identification & Authentication (I&A) for services such as email (ICAM) and enhanced security of the NOAA Active Directory production environment (ESAE), the NOAA0700 subsystems must also ensure that access to these systems and services is controlled through implementation of policy, procedures and security controls that mitigate the risk of unauthorized access to NOAA's information or information systems.
X	IT Infrastructure Maintenance	IT Infrastructure maintenance involves the planning, design, implementation, and maintenance of an IT infrastructure to effectively support automated needs.
X	System and Network Monitoring	The NOAA0700 subsystems provide monitoring of up/down status and alerting based on system availability and performance thresholds for devices and connections for its interconnected systems in real time.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

There are no additional potential threats to the privacy of the information collected by the system.

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.

Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations.

Purpose: The Department of Commerce (Department) is collecting this information to ensure that NOAA staff and contractors have the most current contact information available so that other staff may contact them when needed.

Routine Uses: The Department will use this information to maintain an accurate contact list for NOAA staff and contractors for daily work purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among Department staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent the individual from being contacted when needed in the context of work.