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

Privacy Impact Assessment for the
NOAA0520
NOAA Enterprise Data Centers (EDC)

Reviewed by: Mark H. Graff, Bureau Chief Privacy Officer

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2025.05.06 11:24:25 -04'00'

DOC Chief Privacy Officer
Senior Agency Official for Privacy

Date

U.S. Department of Commerce Privacy Impact Assessment
NOAA0520 NOAA Enterprise Data Centers (EDC)

Unique Project Identifier: NOAA0520

Introduction: System Description

Provide a brief description of the information system.

The NOAA Enterprise Data Centers information system, identified as NOAA0520, is managed by the NOAA Office of the Chief Information Officer's Service Delivery Division, specifically the Critical Infrastructure Management Services (CIMS) group. The primary purpose of this system is to provide a secure platform for monitoring, operating, and managing critical infrastructure essential to NOAA's mission. This infrastructure includes Supervisory Control and Acquisition Data (SCADA) systems, Physical Access Control systems, Video Surveillance systems, fire alarm systems, Building Management Systems (BMS), Building Automation Systems (BAS), and related Information Technology (IT) systems that support facilities-based functions across NOAA. The NOAA0520 EDC FISMA System is critical to the agency. It provides foundational security controls that can be inherited by other NOAA systems, enhancing the overall security posture of the organization.

The NOAA0520 EDC FISMA System consists of servers and applications, including Data Center Infrastructure Management (DCIM) software (Nlyte), Physical Access Control System (PACS) software (CCure 9000 by SoftwareHouse), Video Surveillance Software (Milestone), Electrical Power Monitoring System (Schneider Electric), and Building Management Systems (Johnson Controls Metasys and Tridium N4).

Address the following elements:

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

The NOAA0520 EDC FISMA System is a general support system.

(b) System location

Physically, the scope or boundary of the NOAA0520 system is considered to include all of the following data center locations and locations that inherit physical security controls:

Data Centers

- Fairmont, WV
- Boulder, CO
- Silver Spring, MD

- Ashburn, VA
- Seattle, WA

Physical Security Services

- College Park, MD
- Norfolk, VA
- Narragansett, RI
- Milford, CT
- Falmouth, MA
- Woods Hole, MA
- Highlands, NJ
- Fairmont, WV
- Silver Spring, MD
- Boulder, CO
- Ashburn, VA
- Seattle, WA
- Suitland, MD

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

- Interconnected with NOAA0100 Cyber Security Center
  for Security Operations Center (SOC) Continuous Monitoring activities.

- Interconnected with NOAA0550 N-Wave
  for transport services between NOAA0520 locations.

- Interconnected with NOAA0700 High Availability Enterprise Services
  for Active Directory Federation Services for domain administration.

- Interconnected with NOAA1200 Corporate Services
  for laptop distribution and network accounts.

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

NOAA0520 facilitates the operation, maintenance, and secure monitoring of NOAA facilities and physical spaces using technical solutions to track all operations across the NOAA enterprise.

NOAA0520 deploys sensors and monitoring hardware in facilities to trach operating conditions in the facility, and in some cases, to control operations of the facility.

NOAA0520 also implements an Enterprise Physical Access Control System (ePACS) across various

NOAA sites to secure facility access. This system is FICAM compliant and uses the CAC/PIV to provide access to NOAA secured spaces. NOAA0520 provides the ePACS service for other NOAA sites and provides operating instructions for its use. Individual sites dictate how access for their facility is assigned.

NOAA0520 gathers telemetry and sensor data for facilities based systems for logging and analysis purposes. This data is consolidated in the DCIM, EMPS, BMS, ePACS, and eVSS systems to provide a convenient interface for end users.

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

End users of the NOAA0520 information system are only able to access NOAA0520 resources while on a known NOAA network. Systems accessible to end users include DCIM, eVSS, ePACS, and Tridium.

- **Data Center Infrastructure Monitoring (DCIM)**
  The DCIM system is accessible from a known NOAA network. Users login to the system through a web browser using the secure HTTPS protocol. Access is granted to those with a valid CAC/PIV and that have been given access to the system. Users, based on role based privileges, are able to see data about their data center space(s) in the web interface.

- **Enterprise Video Surveillance System (eVSS)**
  The eVSS is only accessible from a known NOAA network. Users login to the system through a web browser using the secure HTTPS protocol. Access is granted to those with a valid CAC/PIV and that have been given access to the system. Users, based on role based privileges, are able to view video feeds from the system for areas that they are permitted to view and have a security responsibility for.

- **Enterprise Physical Access Control System (ePACS)**
  The ePACS is only accessible from a known NOAA network. Users login to the system through a thick client installed on their workstation. Communications from the client to the server are encrypted. Access is granted to those with a valid CAC/PIV and that have been given access to the system. Users are able to view/edit/add information to the ePACS systems for areas that they are permitted to view and have a security responsibility for.

- **Tridium Building Controls System**
  The Tridium Building Controls System is only accessible from a known NOAA network. Users login to the system through a web browser using the secure HTTPS protocol. Access is granted to those with a valid CAC/PIV and that have been given access to the system. Users, based on role based privileges are able to view/edit/add information to the ePACS systems for areas that they are permitted to view and have a security responsibility for.

- **Electrical Power Management System (EPMS)**
  The Schneider EPMS is only accessible from a known NOAA network. Users login to the system through a web browser using the secure HTTPS protocol. Access is granted to those with a valid account and that have been given access to the system. Users, based on role based privileges are able to view information to the EPMS systems for areas that they are permitted to view and have a facility support responsibility for.

- **Metasys Building Management System (BMS)**
  The Metasys BMS is only accessible from a known NOAA network. Users login to the system through a web browser using the secure HTTPS protocol. Access is granted to those with a valid account and that have been given access to the system. Users, based on role based privileges are able to view information to the BMS systems for areas that they are permitted to view and have a facility support responsibility for.

Administrators provide system administration support only through the use of a VPN connection that requires CAC/PIV authentication. Administrators manage and maintain the systems supporting the NOAA0520 applications by connecting to devices, servers, and systems using secure connections.

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

Log data is securely transmitted to the NOAA0100 information system for analysis. These connections are made through a secure channel and permitted explicitly through the firewall. Data transmitted is gathered by a single device within the NOAA0520 system and sent to the NOAA0100 system.

System data is exchanged with the NOAA0700 information system for Active Directory system and user management. These connections are done over a secure channel.

No system information is actually transmitted to the NOAA0550 information system. The NOAA0550 information system (NWAVE) provides Layer 2 and Layer 3 connectivity and transport services between NOAA0520 sites.

The NOAA1200 information system provides end user workstations (laptops and desktops) for NOAA0520 system administrators to use. These devices are what are used to manage, maintain, and support general operations of the NOAA0520 systems and system infrastructure.

(g) Any information sharing

The NOAA0520 uses the following PII/BII that have been previously provided to authoritative sources:

- **General Personal Data**: Name
- **Work-Related Data:** Work email address, job title
- **Distinguishing Features/Biometrics (DFB):** Video Recording, Photographs

- **Information collected via CAC/PIV**: CAC Number (4-digit), Agency, System Credential Series/Individual Credential Issue (CS/CI), CAC Personal ID, Organization ID (NOAA), Organization Category (Federal Government Agency)
- **System Administration/Audit Data (SAAD):** UserID, IP Address, Date/Time of Access, Queries Run, ID Files Accessed and Content of Files

(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. Security Investigations (Security Clearance actions) / Breach Investigations	COMMERCE/DEPT-13	Executive Orders 10450, 11478 5 U.S.C. 7531-332 28 U.S.C. 533-535 Equal Employment Act of 1972 Privacy Act of 1974, 5 U.S.C. 552a(e)(10) Federal Information Security Modernization Act of 2014 (FISMA 2014) OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
2. Badging & CAC Issuance	COMMERCE/DEPT-18 & GSA/GOVT-7	Electronic Signatures in Global and National Commerce Act, Public Law 106-229 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)
3. Building Entry/Access & Surveillance Log Data / 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

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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					
All of the documented "interconnections" with other NOAA FISMA Systems enhance our security posture to allow for additional security monitoring or secure configuration compliance. The newly added site in Seattle, WA extends the NOAA0520 service offering to a new location managed similarly to the other data center spaces. Some of the applications provided by the NOAA0520 information system are operating at this facility and extend their capability and reach to this site.					

____ 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.

[THIS SPACE INTENTIONALLY BLANK]

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	X	i. Credit Card		m Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
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		e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	

d. Video Recording	X	i. Height		n. Retina/Iris Scans	
e. Photographs	X	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	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

Information collected via CAC:

- Credential Number (4-digit)
- Agency
- System Credential Series/Individual Credential Issue (CS/CI)
- CAC Personal ID
- Organization ID (NOAA)
- Organization Category (Federal Government Agency)
- Portrait
- Certificates

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	X		
Other (specify): Direct read from an individual's CAC/PIV.					

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.

CAC/PIV data accuracy ensured via input validation against DOD certificate servers, user validation, and encryption. Sensor and telemetry data is read-only as received by transmitting devices and cannot be altered based on integrity checks and timestamps.

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.

[THIS SPACE INTENTIONALLY BLANK]

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	X
Video surveillance*	X	Electronic purchase transactions	
Other (specify): *GSA Building			

	There are not any IT system supported activities which raise privacy risks/concerns.

[THIS SPACE INTENTIONALLY BLANK]

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	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	X
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Only PII/BII required to validate a NOAA user's access rights to NOAA0520 managed facilities is processed, stored and transmitted.			

[THIS SPACE INTENTIONALLY BLANK]

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).

Collected via the established processes and procedures for obtaining PII/BII from a common access card (CAC).

Maintained in the system long term and protected with role-based access controls (RBAC)

Information is not disseminated outside of the enterprise physical access control system (ePACS).

The PII/BII identified in section 2.1 is for all federal employees/contractors and visitors accessing NOAA maintained facilities.
The individual-supplied data is used only for identification and coding of their CAC as well as for contact purposes if there should be a problem with the account. The user base consists of Federal employees and contractors.

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.)

An insider threat is a malicious threat to an organization that comes from people within the organization. DOC and NOAA have put in place mandatory training for all its uses. The Security Awareness and Insider Threat is an annual requirement, intended to reduce the risk and minimize the impact of an authorized user intentionally or unintentionally disclosing data, and causing adverse impact to sensitive data and mission.

The NOAA0520 Stakeholders have restricted and limited access to facilities and technology by requiring permissions for access determination to be data stored within Smartsheets. Additionally, they have restricted and limited access to only privileged security management personnel. Finally, purging of data is in accordance with the retention schedule and system users receive training regarding appropriate handling of information.

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

*In case of a privacy incident.

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: ● Interconnected with NOAA0100 Cyber Security Center for Security Operations Center (SOC) Continuous Monitoring activities. ● Interconnected with NOAA0550 N-Wave for transport services between NOAA0520 locations. ● Interconnected with NOAA0700 High Availability Enterprise Services for Active Directory Federation Services for domain administration.

	• Interconnected with NOAA1200 Corporate Services for laptop distribution and network accounts.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

[THIS SPACE INTENTIONALLY BLANK]

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://sites.google.com/noaa.gov/ocio-edc/edc-resources/edc-access_forms (See the sample Privacy Act Statement at the bottom of this Privacy Impact Assessment).	
X	Yes, notice is provided by other means.	Specify how: Signs are posted in the area(s) that are under video surveillance.
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals have the opportunity to decline to provide PII by not enrolling their badge to the access control system. Failure to do so constitutes the need for escorted access to a facility. Additionally, individuals can elect not to enter areas under video surveillance.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Individuals have the opportunity to decline to provide PII by not enrolling their badge to the access control system. Failure to do so constitutes the need for escorted access to a facility.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Currently, there are signs posted at each elevator making personnel / visitors aware of the existence of video surveillance.

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: Individuals who would like access to the NOAA Restricted spaces within EDC must supply the requested/required data on a form. Those requests and associated data supplied by the individual are stored in limited access Smartsheets and only accessible by authorized privileged account administrators. The individual-supplied data is used only for identification and coding of physical access badges as well as for contact purposes if there should be a problem with the account.
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): 15 SEP 2024 ☐ 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 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.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	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).*

NOAA0520 employs the following defensive architecture approach and technologies to protect PII/BII:

- Virtual Local Area Network (VLAN) Topology - all assets within NOAA0520 are logically separated from other data traffic and each type of service is again logically separated from each other.
- NOAA0520 coordinates and meets with N-Wave routinely to ensure boundary protection compliance.
- ERAV Virtual Private Network (VPN) - all administrative users within NOAA0520 must first authenticate to the ERAV VPN in order to gain access to NOAA0520 assets.

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-13, Investigative and Security Records COMMERCE/DEPT-18, Employees Personnel Files not Covered by other Notices; COMMERCE/DEPT-25, Access Control and Identity Management System; and GSA/Govt-7, Federal Personal Identity Verification Identity Management System covers the EDC Access Request, via a Smartsheets form, and the video surveillance.
	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.

[THIS SPACE INTENTIONALLY BLANK]

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: General Records Schedule 5.6 May 2024, US National Archives and Records Administration https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify): Forms are deleted once the retention period is reached. Data located on any NOAA0520 system is shredded prior to disposal of the system. Data located on the access control system would be removed via degaussing techniques upon disposal of the system.			

[THIS SPACE INTENTIONALLY BLANK]

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	**High –** the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: An individual may be identified from information in the NOAA0520 information system.
X	Quantity of PII	Provide explanation: PII for thousands of NOAA staff is contained in the access control system.
	Data Field Sensitivity	Provide explanation:
X	Context of Use	Provide explanation: If a malicious actor were to obtain unauthorized access to a facility, the security of personnel and information could be compromised.
X	Obligation to Protect Confidentiality	Provide explanation: At a minimum, NOAA0520 protects confidentiality, integrity and availability by virtually restricting access to PII. All NOAA0520 data is only accessible internally to NOAA IP space by vetted and authorized personnel.
	Access to and Location of PII	Provide explanation:
	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.)

Potential threats consist primarily of an insider-type threat based on how the information is collected, stored or accessed. Security controls are in place to restrict or limit access to information based on role. The type and quantity of information collected was evaluated to determine the least amount of data required to perform badge coding and physical access control.

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.

[THIS SPACE INTENTIONALLY BLANK]

Sample Privacy Act Statement (Found on All Access Request Forms)

Privacy Act Statement

Authority: 5 U.S.C. 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: The purpose of this collection is to create an identity card to allow employees unescorted access throughout the work site.

Routine Uses: NOAA will use this information to determine qualification for unescorted access. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA 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-25, http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html Access Control and Identity Management System.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent the individual from obtaining unescorted access in the work place.