Version Number: 01-2019

U.S. Department of Commerce
NOAA

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

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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.08.16 20:47:47 -04'00' 05/16/2020

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

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

Unique Project Identifier: NOAA0520

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

The NOAA Enterprise Data Center (NEDC) NOAA0520 is comprised of several "subsystems" or "locations." NOAA0520 is a general facility support system. The NEDC is responsible for the overall management of operations and oversight at NOAA's Enterprise Data Center locations. The NEDC NOAA0520 is missioned with a primary function requirement to provide co-location services which include common controls to the various NOAA programs who reside in the various rooms, buildings, or facilities managed under the NEDC umbrella. This information system is also capable of supporting SCADA information system (IS) which provides building power, badging and CCTV security support services and resources in select locations.

For the NOAA0520, the system boundary is defined both logically and physically. Logically, or from an IT services perspective, the scope or boundary of the NOAA0520 system is considered to include the SCADA systems used to monitor and maintain the facilities that NOAA maintains; environmental monitors for the locations that NOAA does not maintain; and the systems used to support those applications.

Previous PIA listed tenants (x7) that are no longer included on this PIA. There was no value in including those tenants as we have more than those seven tenants today under our purview.

(b) System location

Physically, the scope or boundary of the NOAA0520 system is considered to include all of the following data center locations:

Boulder, CO (additional)
Silver Spring, MD (additional)
Ashburn, VA (additional)
Fairmont, WV (primary)

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

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

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

PII consists of information provided for building and restricted area access, including video data. PII inside of the NOAA0520 system boundary is only accessible by Federal employees and NOAA0520 support contractors for the determination of access and badge coding. C-Cure is an application used to manage and monitor physical access.

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

Personnel with security responsibilities access door access and video data via an isolated workstation that has limited access to both the room and terminal. Access determinations are stored in either Google Drive or Smartsheet and are only accessible by those involved in access determinations.

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

Via email, smartsheets and via administrative input (workstation) for access determinations. Video data and door access data is transmitted to / from a workstation for security management.

(g) Any information sharing conducted by the system

The PII in the system will not be shared outside of the bureau, except in case of privacy breach reporting.

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

DEPT-18, Employees Personnel Files not Covered by other Notices; COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-25, Access Control and Identity Management System and GSA/Govt-7, Federal Personal Identity Verification Identity Management System cover the SAR and the video surveillance.

(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.

_____ 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):					

____ 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.

X 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).

____ 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 01-2017 or later).

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):					
*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. 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		e. Work Email Address		i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. Other work-related data (specify): NOAA Division, Contractor/Other org. Background check information is also asked on the Security Access Form.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. 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: CAC Number (4-digit), Agency, System Credential Series/Individual Credential Issue (CS/CI), CAC Personal ID, Organization ID (NOAA), Organization Category (Federal Government Agency).

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):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
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.

Access determinations information accuracy is ensured via input validation, user validation and encryption. Video and door access 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.

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.

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): System security. Archive and Storage only – no dissemination or processing within the NEDC environment. Access determination and authorization.			

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).

Two separate cards may be required to gain entry to NOAA offices and work areas:
One, to access the building itself issued by the facility; this is needed to use common areas within the facility. The other is a CAC (or Common Access Card) authorized by NOAA, and issued by a Federal Government office. The NEDC Access Request or SAR form should be used to request the issue of a building access card and for adding NEDC-managed areas to an existing CAC.
In accordance with applicable security controls, unescorted access to NEDC must first be requested utilizing the NEDC Access Request or SAR form prior to access approvals. Those individuals who would like unescorted access must supply the requested/required data on the NEDC Access Request or SAR form. Those requested/required data items are Name, Telephone Number, Job Title.
Additionally, information collected from CAC is CAC Number (10-digit), Agency, System CS/CI, Personal ID, Org ID and Org Category. Those requests and associated data supplied by the user are stored in a database and accessible only by authorized privileged account administrators. 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 has 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.

Restricted and limited access via permissions for access determination data stored in Google Drive or within Smartsheet. Restricted and limited access via privileged security management personnel. Purging of data is in accordance with 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	X*		
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 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	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:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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):			

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: SAR Form (*paper only, submitted as pdf with this PIA) and NEDC Form (Screenshot supplied).* .	
	Yes, notice is provided by other means.	Specify how:
	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 completing the form and by notifying the NEDC Facility Management Team, but if they want unescorted access to NEDC and associated restricted spaces, the SAR form must be completed.
	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: However, there is only one use for this PII and if the PII is not provided, then the individual will not have unescorted access. Provision of the information implies consent for the intended

		purpose.
	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.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: The individual may submit an updated SAR Form to the NEDC Facility Access Control POCs and/or the authorizing signatories.
	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: Individuals who would like access to the NOAA Restricted spaces within NEDC must supply the requested/required data on a form. Those requests and associated data supplied by the individual are stored in a restricted Google Drive folder or limited access SmartSheet 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): 08 Feb 2019 ☐ 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. FIPS 199 is HIGH.
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).*

NEDC employs C•CURE for physical access control. C•CURE is a scalable security management solution encompassing complete access control and advanced event monitoring. The system integrates with critical business applications including CCTV and video systems from American Dynamics (Intellex Digital Video Management Systems and VideoEdge NVR), visitor management, and third party devices such as fire alarms, intercoms, and burglar and other alarms.

Badge access to the NOAA facilities is supported 24x7 through the C•CURE system and/or security staff.

Two separate cards may be required to gain entry to NOAA offices and work areas:
One, to access the building itself issued by the facility; this is needed to use common areas within the facility. The other is a CAC (or Common Access Card) authorized by NOAA, and issued by a Federal Government office. The NEDC Access Request or SAR form should be used to request the issue of a building access card and for adding to NEDC-managed areas to an existing CAC.

IAW NOAA 0520's IT Security Policy, unescorted access to NOAA office spaces is provided to existing employees and contractors of NOAA using their existing NOAA badges, when they give a business justification. The NEDC Access Request of SAR form for requesting unescorted access to sensitive IT areas requires confirmation that the applicant has passed at least a Background Investigation of at least a NACI, but the background check itself does not originate and is not stored in the system.

Methods and technologies employed to protect PII, including video data, consist of physical security of the facility and room where the data is maintained with limited access to authorized contract personnel; discretionary access controls on the file system and Google Drive/Smartsheet limited to Federal employees and contractors involved in the access determinations.

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)*: DEPT-18, Employees Personnel Files not Covered by other Notices; COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-25, Access Control and Identity Management System and GSA/Govt-7, Federal Personal Identity Verification Identity Management System cover the SAR 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.

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: NOAA 1200-02, Research Notebooks and NOAA1200-6, Data Requests.
	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	
Degaussing	X	Deleting	X
Other (specify): Forms are shredded once the retention period is reached. Data located on the access control system would be removed via degaussing techniques upon disposal of the system.			

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.

X	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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: An individual may be identified from information in the accounts database.
X	Quantity of PII	Provide explanation: The only PII is account contact information and what is read on the CAC.
	Data Field Sensitivity	Provide explanation:
X	Context of Use	Provide explanation: Compromise of building access PII.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: AC-1, 3, 4, 5, 6, 14, 21, 22; AU-2, 6; IA-4, 5, 8; and SC-4, 7, 8
	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.