Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
NOAA Environmental Security Computing Center

(NESCC) – NOAA0520

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.08.11 16:13:46 -04'00'

8/8/2017

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA Environmental Security Computing Center
(NESCC) – NOAA0520

Unique Project Identifier: NOAA0520

Introduction: System Description

The NESCC supervisory control and data acquisition (SCADA) integrated information system (NOAA0520) is a general facility support system which provides multiple environmental and physical access control resources to the NOAA Environmental Security Computing Center (NESCC) facility and multiple NOAA programs, therein. The main purpose of the NOAA0520 system is that of a SCADA system which monitors the facility's environment controls and physical access control points. The NESCC facility's primary function is to provide co-location resources and services which include common physical and environmental controls to the various NOAA programs who reside in the building. The tenants within the NOAA NESCC facility include:

1. The NOAA Research and Development High Performance Computing System (R&D HPCS);
2. NOAA Security Operations Center (SOC);
3. NWS Telecommunications Operations Center (TOC);
4. Two (2) NESDIS Continuity of Operations (COOP) sites;
5. One (1) NOAA Leadership COOP site;

NOAA0520 falls under the Department of Commerce, National Oceanic and Atmospheric Administration, Office of the Chief Information Officer (DOC/NOAA/OCIO). It is located Fairmont, West Virginia inside a leased facility designed to support multiple mission requirements for NOAA, providing highly available and redundant building, environmental and physical capabilities. As a leased facility, NOAA0520 information systems share office and computer space with other NOAA Line Offices including associated directorates and programs, such as:

1. JPSS/GOES-R;
2. NOAA SOC;
3. R&D HPCS;

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.

Information sharing: The PII/BII in the system will not be shared outside of the bureau, except in case of privacy breach reporting.

Authorities for the collection of PII: 5 U.S.C. 301; 44 U.S.C. 3101; 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; Homeland Security Presidential Directive 12 and IRS Publication-1075; Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Services Act of 1949, as amended.

NESCC FIPS 199 Impact Level: MODERATE

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.

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address		h. Work History	
c. Work Address		f. Business Associates			
i. 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): At ingress and egress, through the CAC					

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 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			
To determine eligibility		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 NESCC environment. Access determination and authorization.			

Section 5: Use of the Information

5.1 Two separate cards may be required to gain entry to NOAA offices and work areas: One, to access the building itself issued by the Leaser (WVHTF); this is needed to use elevators and stairwells within the facility. The other is a CAC (or Common Access Card) authorized by NOAA, and issued by a Federal Government office. The NESCC SAR form should be used to request the issue of a building access card and for adding NESCC, GOES-R RBU, JPSS Operations and Office areas to an existing CAC.

In accordance with applicable security controls, unescorted access to NESCC must first be requested utilizing the NESCC SAR form prior to access approvals. Those individuals who would like unescorted access must supply the requested/required data on the NESCC SAR form. Those requested/required data items are Name, Telephone Number, Job Title. Additionally, information collected from CAC is CAC Number (4-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.

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 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 BII.
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: NESCC SAR Form (*paper only, submitted as pdf with this PIA).*	
	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 NESCC Facility Management Team, but if they want unescorted access to NESCC 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	Specify why not:

	opportunity to consent to particular uses of their PII/BII.	

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 NESCC 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 NESCC 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 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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): **2/08/2017** ☐ 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 and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
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 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.

NESCC 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. Two separate cards may be required to gain entry to NOAA offices and work areas: One, to access the building itself issued by the Leaser (WVHTF); this is needed to use elevators and stairwells within the facility. The other is a CAC (or Common Access Card) authorized by NOAA, and issued by a Federal Government office. This form should be used to request the issue of a building access card and for adding to NESCC, GOES-R RBU, JPSS Operations and Office areas to your 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 SAR form for requesting unescorted access to sensitive IT areas requires confirmation that the applicant has passed at least a BI level, (Background Investigation) or higher than BI level investigation, 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 limited to Federal employees and contractors involved in the access determinations.

Section 9: Privacy Act

9.1 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 and number *(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, a SORN is not being created.

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 Levels

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.

	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 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Addition of a Privacy Act Statement on NESCC SAR Form
	No, the conduct of this PIA does not result in any required business process changes.

12.2 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.