Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Climatic Data Center Local Area Network (NOAA5009)

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 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: 2017.07.14 16:11:15 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/National Climatic Data Center Local Area Network

Unique Project Identifier: 006-48-00-00-01-3209-00-108-023

Introduction: System Description

(a) NOAA's National Centers for Environmental Information (NCEI)-NC, a general support system, maintains the world's largest climate data archive and provides climatological services and data to every sector of the U.S. economy and to users worldwide. Records in the archive range from paleoclimate data to centuries-old journals to data less than an hour old. The Center's mission is to preserve these data and make them available to the public, business, industry, government, and researchers.

NCEI-NC develops national and global datasets, which maximize the use of our climatic and natural resources while also minimizing the risks caused by climate variability and weather extremes. NCEI has a statutory mission to describe the climate of the United States and it acts as the "Nation's Scorekeeper" regarding the trends and anomalies of weather and climate. NCEI-NC's climate data have been used in a variety of applications including agriculture, air quality, construction, education, energy, engineering, forestry, health, insurance, landscape design, livestock management, manufacturing, national security, recreation and tourism, retail, transportation, and water resources management.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI-NC coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service. NCEI-NC manages and contributes to a variety of climate service partnerships including the Regional Climate Services Directors, Regional Climate Centers, State Climatologists, and Cooperative Institute for Climate and Satellites– North Carolina. To facilitate a global data and information exchange, the Center also operates two World Data Centers—one for meteorology and one for paleoclimatology—and plays an active role in professional societies and user engagement activities. *Data available through these partnerships does not require access accounts.*

NCEI-NC has approximately 310 users that connect within NCEI-NC's security boundary. The NCEI-NC user environment consists mainly of web developers, scientists, system administrators, administrative assistants, managers, customer service representatives, database administrators, graphic designers, order fulfillers, and computer operators.

(b) A typical transaction conducted on the system, where PII is collected, includes public access to data products via an ordering mechanism for customized order fulfillment.

(c) Information sharing is conducted by the system. As it relates to PII, NCEI-NC will share usernames with other NOAA entities in support of NOAA Incident Response (the system does not share this information directly with DOC). In addition, NCEI sends, to a FEDRAMP authorized cloud service (SalesForce at The Landmark @ One Market Suite 300 San Francisco, CA 94105), public customer name/address info that was collected during order placement. NCEI is trying to get meaningful information such as which products are important to a particular group of users or what particular variables within products customers from various sectors are asking for (ex. temperature, precipitation, irradiance). We are also interested in seeing how those requests change over time so that we can make sure NCEI is not under- or over-investing in any particular product or portfolio. If possible, we would also like to capture benefits that users derive from the data. Without some individual identifier, we could not determine how customer needs change, we would only be able to see the mass movement of users as a whole or an entire sector.

(d) The legal authority for collection of information addressed in this PIA is: 5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records; additional authorities: 44 U.S.C. 3101, Records Management by Agency Heads; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

(e) NOAA5009 is categorized as a FIPS 199 moderate system.

NCEI-NC has various requirements to collect PII from its employees. These include employee contact information for contingency planning, information related to performance plans, photographs for internal use, and biometric information used to authenticate certain employees to restricted areas. The following information is collected and maintained:

A. Employee's Name
B. Personal email address
C. Personal phone number
D. Photograph for internal use (voluntary posting to intranet for face recognition)
E. Dates for the period of performance
F. Title, Series, and Grade of the position

G. Employee's Division
H. Information about the employee's work and work performance, constituting the plan or appraisal
I. Photograph (copied from government issued PIV card)
J. Fingerprint template file (copied from government issued PIV card)

NCEI-NC offers data to the public through its website. In order for the data to be shipped to the customer, the customer must provide their name and mailing address. It is optional for the customer to leave their phone number and email address as another way of communication. NCEI-NC website utilizes a third party for submitting and authorizing credit cards for data product purchase that require payment. Those credit card numbers are entered directly into the Pay.gov system. The credit card numbers are not stored at NCEI-NC. The information collected is as follows:

A. Name
B. Address
C. Email address (optional)
D. Phone number (optional)

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):					

*A physical access control system (PACS) is in place to authorize employees who require access to the computer room. This system requires the employee to present their government issued PIV card and their fingerprint to register; once registered, the CAC only is required. The PACS system stores the PIV information on a database in a restricted network where only IT Security personnel have access.

__ This is an existing information system in which changes do no 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	X	m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age	X	k. Email Address	X	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	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Performance information					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X*	d. Photographs	X**	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):					

*From the CAC, to generate the building registration card.

** From the CAC, and for internal use after signed consent.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

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	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify					

Non-government Sources					
Public Organizations	X	Private Sector	X	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*	X
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

*A physical access control system (PACS) is in place to authorize employees who require access to the computer room. This system requires the employee to present their government issued PIV card and their fingerprint to register; once registered, the CAC only is required. The PACS system stores the PIV information on a database in a restricted network where only IT Security personnel have access.

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	X	Electronic purchase transactions	
Other (specify):			

- Entry points into the computer room and within the computer room are under video surveillance, with warning signs posted. The cameras record on motion and the video files stored on an air gapped system. Access to that system is restricted to the computer operators (staff and contractors) and the IT Security team.

	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	
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)		For web measurement and customization technologies (multi-session)	
Other (specify): Continuity of Operations (COOP); Physical Access Control Authorization; Cybersecurity Incident Response			

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).

NCEI-NC has various requirements to collect PII from its employees. These include employee contact information for contingency planning, information related to performance plans, photographs for internal use, and biometric information used to authenticate certain employees to restricted areas. The following information is collected and maintained:

A. Employee's Name
B. Personal email address
C. Personal phone number
D. Photograph for internal use (voluntarily posted to the intranet for face recognition)
E. Dates for the period of performance
F. Title, Series, and Grade of the position
G. Employee's Division
H. Information about the employee's work and work performance, constituting the plan or appraisal
I. Photograph (copied from government issued PIV card) for computer room access
J. Fingerprint template file (copied from government issued PIV card) for computer room access

Information is not shared outside the bureau unless there is a breach notification.

NCEI-NC offers data to the public through its website. If data delivery is not feasible online, then an alternative method is direct shipment to the customer. In order for the data to be shipped, the customer must provide their name and mailing address. It is optional for the customer to leave their phone number and email address as another way of communication. The NCEI-NC website utilizes a third party for submitting and authorizing credit cards for data product purchase that require payment. Those credit card numbers are entered directly into the Pay.gov system. The credit card numbers are not stored at NCEI-NC. The information collected is as follows:

A. Name
B. Address
C. Email address (optional)
D. Phone number (optional)

This information is not shared outside the bureau except with Salesforce, for data analytics.

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		X	
Foreign governments			
Foreign entities			
Other (specify):			

	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.

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: National Geophysical Data Center (NGDC)/NOAA5011, National Oceanographic Data Center (NGDC)/NOAA5010. HR info may be shared because the support services division has employees from each FISMA system who may need to access information on employees in another NCEI system. DOC authorized cloud service (SalesForce): NCEI sends public customer name/address info that was collected during order placement, for generation of analytic reports to understand representation by sector of those entities ordering data. Physical and logical access to PII/BII is restricted to authorized personnel only. Encryption is used for PII/BII in transit. Media is sanitized prior to disposal or reuse.
	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. A Privacy Act Statement is available at the NCDC customer order page and a form for PACs permission with a PAS is included at the end of this PIA, as it is a paper form. The NCEI Privacy Policy is also located on the customer order page of the online store. Link: https://www.ncei.noaa.gov/privacy.	
X	Yes, notice is provided by other means.	Specify how: Before an employee's/contractor's photograph can be used for internal use, notice is provided by means of the DOC written consent form requesting permission and obtaining the

		employee's signature. A Privacy Notice is posted at the registration station to those employees who require unescorted access to restricted areas. The notice reads, "As part of the registration process for the system granting access to the restricted area, the photo and fingerprint template will be collected from the CAC. This information is protected under the Privacy Act. Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent access to the restricted area." The authentication system requires the collection of the information stored on their government issued PIV card (photograph and fingerprint template.)
	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: When ordering public data, the customer can choose not to enter their personal email address and phone number and still receive the data they ordered. Additionally, they can choose not to provide name and address but if so, they will be unable to receive the requested data. In the following circumstance individuals are provided instruction on the forms that they may decline to provide the information, but the related services could then not be provided: Employees must provide the General Personal Data and Social Security number (in hardcopy form) in order to receive an identification card once they have accepted employment. Employees/contractors may decline the use of their photographs for internal use by not granting permission via consent form. Employees who require unescorted access to restricted areas may also decline to provide a copy of the data on their PIV card (photograph, fingerprint template) (both the Privacy Act Statement and the sign state that the collection is voluntary) but this will affect their unescorted access.
	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: Customers are provided a link to the Privacy Act Statement on the customer order page for data. The NOAA Web site privacy policy states "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose. When users click the "Submit" button on any of the Web forms found on our site, they are indicating voluntary consent to use of the information they submit for the stated purpose."

		Employee and contractor General Personal Data information is required for ID and emergency notifications. Employees are informed in writing (OF 306) of the use of their data at the time the information is collected when they are onboarding. This form is not stored in NOAA5009. Employees who require unescorted access to the restricted areas provide verbal consent to the collection of the information stored on their government issued PIV card (photograph and fingerprint template). Written consent is required before using employee photographs.
	No, individuals do not have an 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: Customers ordering data can change their PII information under their account settings. Employees review and discuss performance plans with supervisors during annual performance plan meetings. Any updates will be made at this time. The NCEI-NC Contingency Plans are updated annually. Employees are requested to update their personal information. When employees who require access to restricted areas are issued new PIV (CAC) credentials. Their previous PIV information (photograph and fingerprint template) is deleted and replaced with the updated information on the PIV card.
	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.)*

	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: PII/BII on the system is located in access restricted folders. Access or attempted access to these folders is recorded in system logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 8/6/2016

	☐ 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.

Physical and logical access to PII/BII is restricted to authorized personnel only.

All NOAA5009 monitors and printers are operated within NOAA5009 controlled spaces. Server consoles are located in the multi-factor access controlled computer room. NOAA5009 positions monitors away from windows whenever possible. Cubicle configuration within the financial branch are completely enclosed and designed with high partition walls.

Encryption is used for PII/BII in transit.
Backup tapes are encrypted and transported in locked containers.
Media is sanitized prior to disposal or reuse.
Shredders are available to NCEI personnel.

The physical access system database containing fingerprints and photos is encrypted at rest.

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)*: NOAA-11, Contact Information for Members of Public Requesting or Providing Information Related to NOAA's Mission, COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies, COMMERCE/DEPT-25, Access Control and Identity Management System, GSA/Govt-7, Federal Personal Identity Verification Identity Management System.
	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: GRS 1: Civilian Personnel Records, GRS 20, item 3: Electronic Records That Replace Temporary Hard Copy 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	X	Overwriting	X
Degaussing	X	Deleting	X
Other (specify):			

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: NOAA5009 maintains very little sensitive PII. The potential adverse effects of the PII collected (name, address, phone number) is limited.
X	Quantity of PII	Provide explanation: If NOAA5009 had a breach of PII, the number of employees affected would be less than 300.

X	Data Field Sensitivity	Provide explanation: NOAA5009 does not maintain sensitive PII on the information system.
X	Context of Use	Provide explanation: Cybersecurity Incident Response and employee performance information are part of the context.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Physical and logical access controls are in place.
	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: Yes, creation of form with PAS, for PACS.
	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.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Yes, creation of form with PAS, for PACS.
	No, the conduct of this PIA does not result in any required technology changes.

PACS Consent Form

As part of the registration process for the system granting access to the restricted area, the photo and fingerprint template will be collected from the CAC. This information is protected under the Privacy Act of 1974 (5 U.S.C. Section 552a).

Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations and 15 U.S.C. 1512, Powers and duties of Department.

Purpose: Authentication for access to restricted areas.

Routine Uses: 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-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 access to the restricted area.

By signing this document I consent to providing the information stored on my CAC (name, photograph, and fingerprint) for use in gaining access to the computer room.

_____

Print Name

_____

Signature