Version Number: 01-2020

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

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

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

Jennifer Goode 06/02/2021

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NESDIS/NCDC LAN

Unique Project Identifier: NOAA5009

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

NOAA's National Centers for Environmental Information (NCEI) is a General Support System (GSS).

NOAA's National Center for Environmental Information (NCEI) 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. NCEI operates data centers in Asheville, NC and Boulder, CO with additional offices at Stennis Space Center, MS and College Park, MD.

The NCEI archive contains more than 37 petabytes of data, equivalent to about 400 million filing cabinets filled with documents. NCEI facilitates the acquisition of these environmental data collected by NOAA, by other agencies and departments of the U.S. government, as well as by other institutions, organizations, and governments in the U.S. and around the world.

NCEI, as part of the data stewardship mission of providing access and dissemination of the archive holdings, offers users access to tens of thousands of datasets and hundreds of products. NCEI provides search and discovery web platforms to enable the user community to efficiently find and retrieve data through a number of interfaces and services.

NCEI resources are used for scientific research and commercial applications in many fields, including agriculture, forestry, marine and coastal ecosystems, tourism, transportation, civil infrastructure, energy, transportation, water resources, energy, health, insurance, litigation, and national security. NCEI scientists work as lead contributors to the National Climate Assessment, as well publish periodic publications such as the Annual and Monthly State of the Climate Reports.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service.

(b) System location

North Carolina location:
Veach-Baley Federal Building
Asheville, NC

Mississippi location:
Mississippi State University Research and Technology Corporation (MSURTC) Building 1021 at Stennis Space Center (SSC).

Maryland location:
Silver Spring Metro Center 3
1315 E W Hwy
Silver Spring, MD 20910

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

NOAA5009 interconnects with the following general support systems to support information sharing and collaboration.

- NOAA0100, NOAA Security Operations Center
- NOAA0201, Web Operation Center
- NOAA0550, NOAA Enterprise Network
- NOAA5006, NESDIS Headquarters Information Technology Support Local Area Network
- NOAA5011, National Geophysical Data Center Data Archive Management and User System
- NOAA5040, Comprehensive Large Array-data Stewardship System
- NOAA5050, Geostationary Environmental Operational Satellite Series-R Ground System

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

The system operates in the traditional client server model. Data is hosted on servers and made available via various protocols such as HTTPS, FTP, SFTP, and SSH.

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

Information in the system is retrieved by using the following protocols in a client/server model: HTTPS, SFTP, SSH, and FTP. Organizational users authenticate using GFE and their Common Access Card to access in the information system. This provides users secure access that is managed by the program and supported by NOAA5009.

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

Information is transmitted to and from the system using the following protocols using a client/server model: SFTP, FTP, SSH, and HTTPS.

(g) Any information sharing conducted by the system

Information sharing is conducted by the system. As it relates to PII, NOAA5009 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, NOAA5009 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. The purpose is 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). Additionally, this serves to show how those requests change over time so that we can make sure NOAA5009 is not under- or over-investing in any particular product or portfolio.

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

The legal authority for collection of information addressed in this PIA include:

- 5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records;
- 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;

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

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, and there is not a SAOP approved Privacy Impact Assessment.

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

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 01-2019 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	X	o. Financial Information	

b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	X*	f. Scars, Marks, Tattoos	X	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):					

*From the CAC, to generate the building registration card.
** From the CAC, and for internal use after signed consent.
*** See section 3.1 below, regarding Video Surveillance

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	f. 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	X	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 Describe how the accuracy of the information in the system is ensured.

Access control lists are used to ensure that both reading and modifying data is limited to authorized personnel. Additionally, encryption and file integrity tools are used where required. For example, the database storing personal biometric information (photo and fingerprint) are encrypted.

NCEI Data Officers inspect all data submitted via the online data submission system (S2N) and contact the data providers to resolve any issues. Information pertaining to staff used for coordination with regional security offices for clearances and coordination with NASA for site badging purposes is verified by the inspection of the individual's identification card. Information pertaining to account information for access control to systems and web applications; names, email addresses, and Work Related Data of employees and contractors is reviewed by supervisors and IT staff during the creation of accounts.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0648-0024
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	

Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

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

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance	X*	Electronic purchase transactions	
Other (specify):			

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

*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.

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		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

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 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 (copied from government issued PIV card) for computer room access
E. 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.

The IP address of the computer submitting data using the online form is collected for security purposes. In the event that NCEI receives a malicious file, it will be necessary to have an audit trail showing what IP address was used to make the submission. The IP address will be recorded for possible security issue investigation and statistics related to the geographical distribution of data providers.

Data providers' and principal investigators' name, email, and physical address will be recorded as part of the metadata for the submitted data set, and for contact purposes when needed. Data providers (organizations) and principal investigators (individuals) may be part of U.S. Federal, state and local governments, for-profit businesses, non-profit organizations, and academia, their non-U.S. equivalents, and intergovernmental entities. Information on the data providers and principal investigators is necessary for contact purposes in the event of a problem during the archiving process. Such information is also necessary to identify the sources of data submitted to NCEI, especially for properly crediting the providers and principal investigators on the individual holdings in the archive.

Names, addresses, email addresses, and telephone numbers are used for coordination with regional security offices for clearances and coordination with NASA for site badging purposes. NCEI-MS is a tenant on a NASA facility and personnel are required to register their Non-NASA Smartcard (CAC) credentials with NASA. Once registered, the CAC must be presented at the guard gate checkpoint for entrance to the site.

Single session cookies are used to improve the user experience as well as record and analyze user behavior.

Video surveillance may be used for criminal law enforcement purposes.

Photographs of employees and contractors are collected for use in staff posters and Mississippi State University badging applications.

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.)

Insider threat and the mishandling of privacy information by authorized users are the primary threat to privacy. To counter this threat, users are required to take annual IT security awareness training regarding appropriate handling of privacy information. Other threats include a malicious user compromises an internal system and gains unauthorized access. Technical controls are used to mitigate that threat. Those include the use of access control lists, encryption of data at rest and in motion, and multi-factor authentication. The data provided to the organization as part of a submission via the S2N system is subject to the terms of the user agreement. Users submitting information via this platform acknowledge that all data provided via this system will be part of the publicly available data package preserved in the archive. Data from employees used for clearances and site badging purposes contain PII pertaining to individual staff members. The risk of exposure is mitigated by ensuring that the data is transmitted securely and that all users take mandatory training on how to protect PII and BII. Prospective staff are also required to consent to the sharing of this information with NASA and Mississippi State University (see attachment at the end of this document.)

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	X		X

Public			X
Private sector		X	
Foreign governments			
Foreign entities			
Other (specify): Mississippi State University	X		

	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?

X	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.
	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: NOAA5009 interconnects with the following general support systems to support information sharing and collaboration. - NOAA0100, NOAA Security Operations Center - NOAA0201, Web Operation Center - NOAA0550, NOAA Enterprise Network - NOAA5006, NESDIS Headquarters Information Technology Support Local Area Network - NOAA5011, National Geophysical Data Center Data Archive Management and User System - NOAA5040, Comprehensive Large Array-data Stewardship System - NOAA5050, Geostationary Environmental Operational Satellite Series-R Ground 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.

6.4 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):	Mississippi State personnel have limited access to video surveillance for criminal law enforcement purposes.		

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 (PAS) and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.ncdc.noaa.gov/about-ncdc/privacy/privacy_act_statement and a form for the Physical Access Control System (PACS) authorizing 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 http://www.ngdc.noaa.gov/wiki/images/f/f4/NOAA_Sub_Agreement.docx (link to PAS in Appendix D, in Executive Summary). .	
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.) Notice is provided in the user agreement for Send2NCEI service (attached to this PIA). Data providers and principal investigators are notified as part of the data submission process that their information will be stored in the metadata associated with their data. Information collected for badging purposes, emergency contact, and disaster recovery/continuity of operations: Notice is given in writing (OF optional form 306) during the employee on-boarding process when Federal and contract personnel fill out the OPM Optional Form 306. For NCEI-MS, there is a written consent form for sharing information for badging purposes with NASA (site access) and the Mississippi State University (building access). The form is attached to this PIA, just before the signature page. Before an employee's/contractor's photograph can be used for a poster, notice is provided by means of a DOC form requesting permission for use and obtaining the employee's signature. Information collected for account management: Notice is given in writing or via email at the time that the user requests an account on the information system.
	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: Data providers and principal investigators must consent to the collection and publication of their data when submitting oceanographic data for archiving. This consent is requested on the online form. 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 PlV 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.	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: Data providers and principal investigators may update their information stored by NCEI at any time via the online submission service, email to NODC.DataOfficer@noaa.gov or telephone request to NCEI Customer Service.

		Employees and contractors may review and update their General Personal Data at any time via email or in-person to the Administrative Services Unit for NCEI-MD. For NCEI-MS, the Customer Service Representative (CSR) is the main contact and also designated to maintain the emergency contact list. The CSR shares all updates with the System Owner, who updates badging information. When employees who require access to restricted areas are issued new PIV (CAC) credentials, they lose access to the restricted area until they re-register their new PIV card. At that time, their old information (photograph and fingerprint template) is deleted and replaced by the new PIV card info.
	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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): **8/06/2020** ☐ 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. **Moderate**
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish DOC ownership rights over data including PII/BII.
	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).

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 and at rest. Secure protocols such as HTTPS and SFTP for data in motion. 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 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/NOA-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. COMMERCE/DEPT-13, Investigative and Security Records
	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: GRS 20 3.1: General Technology Management Records NRS 400 Finance NRS 700 Procurement NRS 1200-06 Data Request Records NRS 1406 NOAA National Data Centers
	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 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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: NCEI 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 NCEI had a breach of PII, the number of employees affected would be less than 300.

X	Data Field Sensitivity	Provide explanation: NOAA5009 maintains limited sensitive PII (Date of birth) that is associated with an individual's name.
X	Context of Use	Provide explanation: Based on the context of use described in Section 5.1, there would be low impact if information was accessed or disclosed.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access to PII is described above in Section 8.2. Physical and logical access restrictions are in place as prescribed in NIST SP 800-53.
	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.)

NCEI-NC collects very little privacy information. With the introduction of the Administration LAN (NOAA5006), much of the employees' personal information collected for HR requirements have been moved to that FISMA system. Threats and mitigations to the remaining non-sensitive PII are identified in sections 5 and 8 above. Those consists of insider threat and accidental mishandling of PII.

Information submitted through the Send2NCEI application may contain contact information or scientific data which belongs to individuals other than the person who provides this information. This consideration was a major factor in the drafting of the user agreement (see attachment to this document) and the decision was made to make these data optional and to include a provision in the user agreement that states that the submitter warrants that they "have obtained permission from those named persons to submit their contact information to NCEI for the purposes specified in this agreement". Furthermore, the agreement requires them to warrant that they have obtained permission from any third party to submit that party's property to NCEI.

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.