

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



**Privacy Impact Assessment
NOAA5009 National Climactic Data Center Local Area Network**

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

CHARLES CUTSHALL

Digitally signed by CHARLES CUTSHALL
Date: 2024.09.26 17:21:20 -04'00'

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 brief description of the information system.

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.

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.

Address the following elements:

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

NOAA's NCEI is a General Support System (GSS).

(b) *System location*

North Carolina location (NCEI-NC):
Veatch-Baley Federal Building
Asheville, NC

Mississippi location (NCEI-MS):

Mississippi State University Research and Technology Corporation (MSURTC) Building 1021 at Stennis Space Center (SSC), MS

Maryland location (NCEI-MD):

Silver Spring Metro Center 3

Silver Spring, MD

*Colorado location (NCEI-CO):

David Skaggs Research Center

Boulder, CO.

* The NOAA5009 and NOAA5011 FISMA systems were consolidated and merged into one Security Authorization boundary (NOAA5009) on 04/30/2024. All functions for NOAA5011 were absorbed into NOAA5009. No NOAA5009 or NOAA5011 hardware were decommissioned as a direct result of this consolidation. Existing NOAA5011 hardware have been transitioned to NOAA5009. Hardware includes laptops, desktops, servers, printers, storage arrays, and network devices.

(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
- NOAA5040, Comprehensive Large Array-data Stewardship System
- NOAA5050, Geostationary Environmental Operational Satellite Series-R Ground System
- NOAA8102, Automated Surface Observing System
- NOAA8864, Space Weather Prediction Center*

*The interconnection with NOAA8864 was previously present with NOAA5011. NCEI provides a real-time ionospheric data stream and a near real-time Global Positioning System (GPS) data stream to Space Weather Prediction Center (SWPC). SWPC provides archive files to NCEI. Due to the consolidation of the NOAA5009 and NOAA5011 security authorization boundaries, this interconnection will now be incorporated into NOAA5009.

(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 Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP).

(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, and FTP.

Organizational users authenticate using Government Furnished Equipment (GFE) and their Common Access Card (CAC) to access 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

NOAA5009 has implemented the Trusted Internet Connection (TIC) via N-Wave for all external network connections which provides reliable, secure, skilled, and a highly available network infrastructure for data transmission.

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

Additionally, NOAA5009 receives some data from data submitters via shipped external hard drives.

(g) Any information sharing conducted by the system

Information sharing is conducted by the system. As it relates to Personal Identifiable Information (PII), NOAA5009 will share usernames with other NOAA entities in support of NOAA Incident Response (the system does not share this information directly with the Department of Commerce (DOC)).

In addition, NOAA5009 sends public customer name/address info collected during order placement to a FEDRAMP authorized cloud service (SalesForce at TheLandmark @ One Market Suite 300 San Francisco, CA 94105). The purpose is to get meaningful information such as which products are important to a particular group of users or what particular variables (ex., temperature, precipitation, irradiance) within products customers from various sectors are asking for. 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.

As part of the consolidation with the NCEI-CO site, the system will now conduct a data and data-information service in all scientific and technical areas involving solid earth geophysics, marine geology and geophysics, glaciology, space environment, solar activity and the other areas of solar-terrestrial physics. The Center prepares systematic and special data products and performs data-related research studies to enhance the utility of the service to the users. It performs all functions related to data acquisition, archiving, retrieval, indexing, quality assessments, evaluation, synthesis, dissemination, and publication. This information is shared with collaborators from numerous internal and external organizations, as well as the general public where appropriate.

In order to better fulfill its mission, NCEI-CO receives data from other NOAA groups, other federal government agencies such as The National Aeronautics and Space Administration (NASA), the U.S. Air Force, the U.S. Geological Survey; federally funded research institutions such as the National Center for Atmospheric Research (NCAR), and the Woods Hole Oceanographic Institution; universities such as the University of Colorado - National Snow and Ice Data Center (NSIDC), and the Ocean Drilling Program at Texas A&M University; state agencies such as the Alaska Department of Natural Resources, California Department of Water Resources; and intergovernmental entities such as the European Space Agency, and the Australian Surveying and Land Information Group (AUSLIG).

Employee information is not shared outside of the organization.

(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:

Type of Information Collected (Introduction h.)	Applicable SORNs (Section 9.2)	Programmatic Authorities (Introduction h.)
1. Contact Information for the Public	NOAA-11	5 U.S.C. 301, Departmental Regulations
		15 U.S.C. 1512, Powers and duties of Department
2. Badging & CAC Issuance	COMMERCE/DEPT-18	Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		5 U.S.C. 301
	GSA/GOVT-7	5 U.S.C. 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Federal Information Security Management Act of 2002 (44 U.S.C. 3554)
		E-Government Act of 2002 (Pub. L. 107-347, Sec. 203)

3. System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
		Electronic Signatures in Global and National Commerce Act, Public Law 106-229
		28 U.S.C. 533-535
4. Security Investigations (Security Clearance actions)	COMMERCE/DEPT-13	Executive Orders 10450, 11478
		5 U.S.C. 7531-332
		28 U.S.C. 533-535
		Equal Employment Act of 1972

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

NOAA5009 is a FIPS 199 moderate impact system.

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	X	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):

* The NOAA5009 and NOAA5011 FISMA systems were consolidated and merged into one Security Authorization boundary (NOAA5009) on 04/30/2024. All functions for NOAA5011 were absorbed into NOAA5009. No NOAA5009 or NOAA5011 hardware were decommissioned as a direct result of this consolidation. Existing NOAA5011 hardware have been transitioned to NOAA5009. There is also a new interconnection with NOAA8864, which was present between NOAA5011 and NOAA8864. This interconnection does not create new privacy risks. The privacy risk only pertains to the consolidation of the two systems.

_____ 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.

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. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	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			
i. 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		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.

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

Other Information (specify)
Photos and video recordings: The Ocean Exploration and Research (OER) Science group will be submitting video and still image files from seven projects dating from 2011-2017 to the NCEI Archival Storage systems. These videos and images contain people's faces on the deck of the vessel or at the NOAA facility/dock, as well as during instrument deployment and retrieval. The information will not be distributed to the public. The data will not be accessible to anyone outside of NCEI unless an FOIA request is received. Also, the metadata records would be searchable within NCEI, so no unique identifier would be needed to access the data.

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): Email and online apply to data subscribers and submitters. NOAA5009 requires the use of cryptographic mechanisms by those sending data to the system whenever possible, to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. The mechanisms [for web-based transmissions, including web-based forms] include Secure Sockets Layer/Transport Layer Security encryption.					

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	X
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. Supervisors and IT staff review information pertaining to account information for access control to systems and web applications (names, email addresses, and Work Related Data of employees and contractors) 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 3206-0182
	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		Electronic purchase transactions	
Other (specify):			

X	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	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	X
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 Internet Protocol (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.

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

With regard to NCEI-CO, Customer contact information includes: Name, Company or Organization, Company or Organization Address, Company or Organization Email Address, and Company or Organization Phone Number. This information is used by the NCEI-CO data administrator staff to provide the data in compressed format for later retrieval by the user/customer. In some cases, customer provided data is used by NCEI-CO data administrator staff to manage account information for customer access to web applications (members of the public).

- 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 threats 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, titled "Authorization to share Personally Identifiable Information with non-Department of Commerce entities" 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		

Public			X
Private sector		X	
Foreign governments	X		
Foreign entities	X		
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 • NOAA5040, Comprehensive Large Array-data Stewardship System • NOAA5050, Geostationary Environmental Operational Satellite Series-R Ground System • NOAA8102, Automated Surface Observing System • NOAA8864, Space Weather Prediction Center 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. NCEI has an online ordering system through which users input their data. The business analytics team is the team that accesses salesforce.
---	--

	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. Where a higher level of integrity and/or confidentiality is required, NOAA5009 employs cryptographic mechanisms, such as SSH, HTTPS, or FTPS. Secure Sockets Layer or Transport Layer Security (SSL/TLS) is used to protect the confidentiality of data transmission when authentication is required.
	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	X	Government Employees	X
Contractors	X		
Other (specify): External users have access to publicly available scientific data and information, but, do not have access to PII, other than Data Provider's PII, including name, email, and physical address that may be included with publicly available metadata for contributed data.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _ https://www.ncei.noaa.gov/privacy and a form for the Physical Access Control System (PACS) authorizing permission with a PAS can be found at the end of this document as it is a paper form (first attachment) The NOAA Submission agreement template contains an "Appendix D", which has been added at the end of this document (fifth attachment). This Appendix details a PAS whenever a Submission agreement is utilized. For subscribers: https://www.ngdc.noaa.gov/privacy-act-statement-data-requestors.pdf For Salesforce, a Privacy Act Statement is available on the on-line ordering system for the customers to review. A copy has been attached at the end of this document (fourth attachment).	
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 (third attachment at the end of this document). 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-306) during the employee on-boarding process when Federal and contract personnel fill out the OF-306. For data submitted by the Ocean Exploration and Research (OER) Science group to NCEI Archival Storage systems, notice was constructively obtained at the time of the videography per the Magnuson-Stevens Fishery Conservation and Management Act. Data providers and principal investigators are notified in the Data Submission User Agreement that their information will be stored in the metadata associated with their data. This includes notice regarding redistribution of research data (in the Executive Summary). 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 can be found at the end of this document (second attachment). 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. Information collected for account management is requested in writing or via email by the user's supervisor in the request for 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/requesting 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. If identifying information is not provided, the employee will not be granted access to the restricted area. The employee sensitive information is stored within the NOAA5006 boundary, not NOAA5009. For Salesforce, customers can choose to provide their information in the system if they want to place an order. However, if they choose not to, their order will not be filled.
	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, along with completing the PACS form (first attachment), for the collection of the information stored on their government issued PIV card (photograph and fingerprint template). Written consent is required before using employee photographs. Data providers and principal investigators consent to the collection and publication of their data when they submit data for archiving – as stated in appendix D of the signed Data Submission Agreements. The notice is provided when users access this link: ncei.noaa.gov/archive/send2ncei/terms_new.html, and sign in. A copy of this form can be found at the end of this document (fifth attachment). Customers who place orders through Salesforce must consent to the collection and use of their information and that consent is given through the online ordering system. Customers place orders via their government issued equipment and the data includes business analytics data that is used to help determine market sector associated with the order to help better tailor information and services to the different stake holder groups.
	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 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. Data providers receive a copy of the NCEI Data Submission Agreement they have signed, and have the opportunity to submit updates pertaining to the BII, by email to the database administrator, as will be stated in the revised agreement. Customers who place orders through Salesforce can review and update the PII/BII pertaining to them by accessing and reviewing their information through the online ordering system.
	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): 08/06/2024 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is 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 output devices (monitors, printers and audio devices) 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. <i>(list all that apply):</i> COMMERCE/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, COMMERCE/DEPT-13, Investigative and Security Records
X	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u>. COMMERCE/DEPT-30, Public Affairs Archives (submitted on 08/21/2019)
	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	
Degaussing	X	Deleting	X
Other (specify):			

* NOAA5009 maintains the world's largest climate data and thus contains information that can be used by different science groups. If this data/information is printed out for use by different users, shredding is an effective method of disposal of data that may contain PII/BII.

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, all NCEI employees and affiliates would be affected.
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 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 consist 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 (found at the end of 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.

Version Number: 01-2017

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

Authorization to share Personally Identifiable Information with non-Department of
Commerce entities

I, _____ give permission for my name, SSN, personal and work address, personal and work phone number, personal and work email address, and photograph to be shared with the National Aeronautics and Space Administration (NASA), in order to receive a local NASA badge for access to the NASA John C. Stennis Space Center, MS.

I understand that if I do not give permission, I will not receive a local NASA badge, and thus will not have access to the NASA facility in order to perform my job.

I, _____ give permission for my name and photograph to be shared with the Mississippi State University Research and Technology Consortium, in order to receive a building badge for access to Building 1021 at the John C. Stennis Space Center, MS.

I understand that if I do not give permission, I will not receive a building badge, and thus will not have building access in order to perform my job.

Please sign and return this form to the National Centers for Environmental Information Mississippi (NCEI-MS) Site Manager.

Signature

Date



Submit Data: User Agreement

Please read the following User Agreement:

NCEI Data Submission User Agreement

You, the submitter of data, agree to provide a copy of data identified in the NCEI online data submission process Send2NCEI ('S2N') or any other data submission process for inclusion in the NCEI archives of environmental data and information. You also agree to provide contact information (name, email, and physical address) to NCEI to enable NCEI to authenticate your data submission request and to contact you with any questions about your data. Your contact information will be stored and redistributed as part of the metadata about the data you send to NCEI.

Collecting contact information is authorized as part of standard metadata defined by the Federal Geographic Data Committee (FGDC) in accordance with Executive Order 12906, "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure", as amended by Executive Order 13286 of February 28, 2003.

NCEI requires at least your name and email address to enable NCEI to validate your identity as the data provider and to contact you with information about the progress of your data submission through the archival ingest and data management life cycle.

The inclusion of additional contact information (e.g., institutional affiliation, mailing address, phone number) is optional, but the absence of additional contact information limits the ability of NCEI to contact you if there are problems with data you are sending to be archived at NCEI. Contact information is used to provide proper attribution in standard metadata representations (e.g., ISO 19115 Geographic Metadata) of your efforts to collect, organize, process, and/or manage those data. Your contact information may also be used to facilitate discovery of data that were collected, analyzed, quality controlled, and/or sent to NCEI by you. Incomplete contact information may result in inaccurate or improperly attributed standard metadata and limited or inaccurate recognition of your efforts to collect or otherwise be connected to these data.

By submitting data for inclusion in the NCEI archives, you warrant that these data may be copied and distributed by NCEI for any purposes. NCEI may make these data available via electronic or other means without restrictions. You understand that NCEI will not compensate you in any way or pay you for use of these data. To the extent that any part of this submission is subject to the intellectual property rights of a third party, you warrant that you have obtained permission from that third party to submit that party's property to NCEI for the purposes specified in this agreement.

If you provide names, email and/or physical addresses, or other contact information for other people or organizations who are responsible for producing, maintaining, or providing additional information about the data you submit to NCEI, you warrant that you have obtained permission from those named persons to submit their contact information to NCEI for the purposes specified in this agreement. NCEI and NOAA may acquire, keep, and redistribute contact information about individual data providers as documented in and pursuant to System of Records Notice COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission (<https://www.osec.doc.gov/opog/PrivacyAct/SORNS/noaa-11.html>) and authorized by U.S. Government Policy on Open Data M-13-13 – Memorandum for the Heads of Executive Departments and Agencies, Section 1, "Open data will be consistent with the following principles: Managed Post-Release. A point of contact must be designated to assist with data use and to respond to complaints about adherence to these open data requirements." As noted in Systems of Records Notice COMMERCE/NOAA-11, "This record system is necessary to facilitate provision of information to the requesting public and to post researchers' contact information on applicable Web sites."

Upon receipt of these data, NCEI may make a copy of the original data files and assign an identifier (NCEI Accession Number or other identifier) to the data collection, in accordance with current NCEI archival practices. A description of these practices can be reviewed at <http://www.ncei.noaa.gov/archive> or obtained by contacting NCEI.

Upon acceptance for inclusion in the NCEI repository, NCEI agrees to maintain an exact copy of these data 'as is' in accordance with the current records retention schedule for "In situ and remotely sensed environmental data" (NOAA 1406-01) and "Metadata management database" (NOAA 1406-03) or other relevant records series retention, as determined by NCEI appraisal practices. NCEI may make translations of these data and files as necessary to maintain any electronic files on current media. NCEI will make every attempt to maintain the integrity of these data as files are migrated from obsolete technology to new technology. NCEI will maintain backup copies of these data at local and off-site locations, in accordance with current NCEI archiving practices.

NCEI may use some or all data archived at NCEI in products created or derived by NCEI, with appropriate attribution to the original data producer and/or provider.

Data Liability Policy

The data defined by this Data Submission User Agreement is only as good as the quality assurance and quality control procedures outlined by the enclosed metadata reporting statement. Any subsequent users of data specified in this agreement bear all responsibility for its subsequent use in any further analyses or comparisons. The Federal government does not assume liability to any Recipient of data defined here, nor will the Federal government reimburse or indemnify any Recipient for its liability due to any losses resulting in any way from the use of these data.

These terms constitute the entire agreement between you and NCEI regarding the data submission process used to transfer data and metadata from you to NCEI. These terms supersede (a) any prior agreements between you and NCEI and (b) any licenses you submit to NCEI in conjunction with your data submission.

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 the Department.

Purpose: The Department of Commerce (Department) is collecting this information as a means to directly ship ordered data to the requester and generate analytical reports to understand representation by sector of those entities ordering data. The purpose of the analytical reports is to gather 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 (e.g., temperature, precipitation, irradiance). Additionally, these reports show how those requests change over time to ensure the Department is not under- or over-investing in any particular product or portfolio.

Routine Uses: The Department will use this information to disclose to a contractor of the Department having need for the information in the performance of the contract but not operating a system of records within the meaning of 5 U.S.C. 552a(m). Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among Department staff and affiliates for mission-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-NOAA-11](#), Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary. However, the failure to provide accurate information may delay or prevent you from receiving the requested data.

[PROJECT_ABBREV] SA between
[PROVIDER_ABBREV] and [ARCHIVE_ABBREV]

[DCM]
[Version], [Release Date]

APPENDIX D. Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations.

Purpose: As part of the signed Data Submission Agreements, data providers' and principal investigators' name, email, and physical address are recorded as part of the metadata for the submitted data set, and for contact purposes when needed. Information on the data providers and principal investigators is necessary in order for a system administrator to contact an individual 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.

Routine Uses: The Department will use this information to contact data providers in the event of a problem during the archiving process, and to properly credit providers and principal investigators on the individual holdings in the archive. 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/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent required contacts regarding archiving problems, as well as proper archiving.