

**U.S. Department of Commerce
NOAA**



**Privacy Impact Assessment
for the
National Oceanographic Data Center (NODC) Local Area Network
(LAN)
NOAA5010**

Reviewed by: Mark Graff, Bureau Chief Privacy Officer

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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.07.31 14:36:09 -04'00'

7/27/2017

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

Date

U.S. Department of Commerce Privacy Impact Assessment National Oceanographic Data Center LAN/NOAA5010

Unique Project Identifier: 006-000321800 00-48-01-13-02-00

Introduction: System Description

NOAA's National Centers for Environmental Information (NCEI) are responsible for hosting and providing access to one of the most significant archives on earth, with comprehensive oceanic, atmospheric, and geophysical data. From the depths of the ocean to the surface of the sun and from million-year-old tree rings to near real-time satellite images, NCEI is the Nation's leading authority for environmental information. By preserving, stewarding, and maximizing the utility of the Federal government's billion-dollar investment in high-quality environmental data, NCEI remains committed to providing products and services to private industry and businesses, local to international governments, academia, as well as the general public.

The demand for high-value environmental data and information has dramatically increased in recent years. NCEI is designed to improve NOAA's ability to meet that demand. The Consolidated and Further Continuing Appropriations Act, 2015, Public Law 113-235, approved the consolidation of NOAA's existing three National Data Centers: the National Climatic Data Center, the National Geophysical Data Center, and the National Oceanographic Data Center into the National Centers for Environmental Information. NCEI has employees in four major locations: Asheville, NC, Boulder, CO, Silver Spring, MD, and Stennis Space Center, MS. NCEI located in Maryland and Mississippi comprise the NOAA5010 system.

The NCEI-MD and NOAA Central Library, with its regional branch assets, are integrated to provide access to the world's most comprehensive sources of marine environmental data and information. NCEI-MD maintains and updates a national ocean archive with environmental data acquired from domestic and foreign activities and produces products and metadata, and research from these data that help monitor global environmental changes.

These data include physical, biological, and chemical measurements derived from in situ oceanographic observations, satellite remote sensing of the oceans, and ocean model simulations. NCEI-MD manages and operates the World Data Center (WDC) for Oceanography in Silver Spring, MD. Its personnel directly interact with federal, state, academic, and industrial oceanographic activities; represent NESDIS on various interagency domestic panels, committees and councils; and represent the United States in various international organizations, such as the International Oceanographic Data Exchange. NCEI-MD and NCEI-MS represent NESDIS and NOAA to the general public, government agencies, academic institutions, foreign governments,

and the private sector on matters involving oceanographic data.

External users of the Public Web consist of an average of 170,000 unique visitors per month. These users include, but are not limited, to other NOAA agencies, other federal government agencies such as U.S. Geological Survey, the Environmental Protection Agency, universities- Mississippi State University, University of New Hampshire, Texas A&M, University of South Florida, and state agencies- Mississippi Department of Marine Resources, Louisiana Department of Natural Resources, Alabama Department of Conservation and Natural Resources, Texas Parks and Wildlife, and Florida Fish and Wildlife Commission.

NCEI-MS resides on the first and third floors of the Mississippi State University Research and Technology Corporation (MSURTC) Building 1021 at Stennis Space Center (SSC), MS. Access to this facility is restricted with keycard/badge access. Photographs, names, job titles, home and work addresses, home and work email addresses, home and work telephone numbers are collected from Federal employees and contractors for badging purposes. SSNs are collected in hardcopy form only and are not stored on the IT system. Employee and contractor names, home and work addresses, home and work email addresses, home and work telephone numbers, and SSNs are shared with the National Aeronautics and Space Administration (NASA) in order to receive a site badge, and photographs and names are shared with Mississippi State University (MSU) in order to receive a building keycard/badge. For these instances of sharing, NOAA Headquarters maintains a disclosure log and there are also license agreements (between MSU and NOAA for the physical access controls pertaining to the building and between MSU and NASA as a tenant that covers the physical access into the site). These are in active process of being updated and re-signed as of 8-26-16.

The System of Records Notice (SORN): COMMERCE/DEPT-25, Access Control and Identity Management System covers the collection of this information.

If written consent is obtained using the DOC consent form, employee and contractor photographs may also be used for staff posters and shared with the public. The applicable SORN is COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.

In order to better fulfill its mission, NCEI-MS receives data and information about the data providers (contact information on data providers consists of name, email address and physical address) from other NOAA groups, other federal government agencies such as Department of the Interior/Bureau of Ocean Energy Management, NASA, and the U.S. Navy; state agencies such as Alabama Department of Conservation and Natural Resources and Alaska Department of Environmental Management; academia such as Appalachian State University, Auburn University, Binghamton University, etc.; for-profit businesses such as Alpine Geophysical Associates, Inc., Arthur D. Little, Inc., Barry A. Vittor and Associates, Inc., etc.; non-profit organizations such as Battelle Memorial Institute, Bernice Apuahi Bishop Museum, etc.; and their non-U.S. equivalents such as South African Data Centre for Oceanography, Australian

Oceanographic Data Center, Aichi Prefectural Fisheries Experimental Station (Japan), etc., and intergovernmental entities such as European Space Agency, World Climate Research Programme, International Oceanographic Data and Information Exchange, etc. Metadata information is initiated at the time of data collection and acquisition planning. As part of the data management process, metadata citation and contacts are reviewed and approved by the data owner. A Web-based submission form is being used to provide another means to collect this data and hold it for review before permanently placing it in the NCEI archive holdings. Data provider information is found within the metadata for archived data and is made available to the public when data is downloaded from the archive. Per the 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.” Thus the contact information collected is made available to the public for contact purposes. In addition, the Project Open Data Metadata Resources for Schema v1.1 states the implementation requirements for Project Open Data metadata and name and email address are minimally required based on this guidance, see <https://project-open-data.cio.gov/v1.1/schema/>. NOAA NAO 212-15, the NOAA Data Documentation Directive, and the NOAA Plan for Public Access to Research Results all provide specific citation guidance for general documentation including metadata. The data provider contact information is covered by this SORN: COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission.

Contractors provide support for the NOAA5010 mission by supporting acquisition, preservation, monitoring, and assessment of the Nation's treasure of coastal, oceanographic, and geophysical data and information. Contractors perform scientific analyses, product development, and data ingest, archive, and dissemination support. Contractors also provide system and network administration and security support of the NOAA5010 IT infrastructure.

The legal authority for civil service employment is 5 U.S.C. 301, Departmental Regulations (see COMMERCE/DEPT-18 System of Records Notice). For the data provider information, 5 U.S.C. 301 and 15 U.S.C. 1512, Powers and duties of Department [of Commerce], are applicable (see COMMERCE/NOAA-11 System of Records Notice). Additional authorities: 35 U.S.C. 2; the Electronic Signatures in Global and National Commerce Act, Public Law 106-229; 28 U.S.C. 533-535; 44 U.S.C. 1301; Homeland Security Presidential Directive 12 and IRS Publication-1075.

NODC LAN (NOAA5010) is a 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		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

This is an existing information system in which changes do not create new privacy risks.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

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

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

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	

b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

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

Other Information (specify)					

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone		Email	X		
Other (specify):					

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

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

Technologies Used Containing PII/BII Not Previously Deployed (TUCBPNPD)					
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			
To determine eligibility		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Continuity of Operations (COOP)			

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).

User IDs, Date/Time of Access, and IP addresses are collected from organizational users, i.e. NCEI federal employees and contractors who access the NOAA5010 information system, to facilitate the IT and IT security administration of the system.

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.

Additionally at NCEI-MS, names, addresses, and email addresses collected from employees, contractors, and the public are used to manage account information for access control to systems and web applications; names, email addresses, and Work Related Data of employees and contractors are used to direct the public to appropriate personnel within the organization; and for emergency, disaster recovery, and continuity of operations.

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 is required to have NASA badges for entrance to the site.

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

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			
Federal agencies	X		
State, local, tribal gov't agencies			
Public			X

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

	The PII/BII in the system will not be shared.
--	---

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.</p> <p>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA Climatic Data Center (NCDC) LAN LAN/NOAA5009 and NOAA Geophysical Data Center (NGDC) LAN/NOAA5011.</p> <p>Physical and logical access to PII/BII is restricted to authorized personnel only. Encryption is used for PII/BII in transit. Backup tapes containing PII/BII are transported in locked containers. Media is sanitized prior to disposal or reuse.</p>
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

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

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _ 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: 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.

		<p>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.</p> <p>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. The ISSO has added the consent form to the procedures for onboarding new employees and all 46 current employees have signed and received a copy of the form.</p> <p>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.</p> <p>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.</p>
	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.	<p>Specify how: The inclusion of additional contact information (beyond name & email address) when using the online data submission service is optional.</p> <p>In the two following instances, individuals are provided instruction on the forms that they may decline to provide the information, but the related services could then not be provided: 1) Employees must provide the General Personal Data and Social Security number (in hardcopy form) in order to receive a Department of Commerce identification card and other badges once they have accepted employment; and 2) Name and email address are required in order to use the online data submission service.</p> <p>Employees/contractors may decline the use of their photographs on posters by not granting permission via the DOC consent form. Photographs will not be used if written permission is not obtained.</p>
	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
---	--	--

		<p>requested on the online form.</p> <p>Employee and contractor General Personal Data information is required for badging and emergency notifications. Employees and contractors are informed in writing (OF optional form 306) of the use of their data at the time the information is collected and data is not used for any other purpose.</p> <p>For use of employee and contractor photographs, written consent is requested by the supervisor or the person who is creating the poster. If consent is not received, the photographs are not used.</p>
	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.	<p>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.</p> <p>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.</p>
	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	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p>Explanation: PII/BII on the system is located in access restricted folders. Access or attempted access to these folders is recorded in system logs.</p>
X	<p>The information is secured in accordance with FISMA requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&A): <u>9/6/2016</u></p> <p><input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.</p>

X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

<p>-Physical and logical access to PII/BII is restricted to authorized personnel only.</p> <p>-All NOAA5010 output devices (monitors, printers and audio devices) are operated within NOAA5010 controlled spaces. Critical consoles for NOAA5010 servers are located in keycard access controlled computer rooms. NCEI positions monitors away from windows whenever possible. Publicly viewable monitors (e.g., the receptionist’s monitor) have privacy filters installed.</p> <p>-Encryption is used for PII/BII in transit.</p> <p>-Backup tapes containing PII/BII are transported in locked containers.</p> <p>-Media is sanitized prior to disposal or reuse.</p> <p>-Shredder has been made available to NCEI personnel for destruction of sensitive documents.</p>

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C.

§ 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> : NOAA-11 , Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission, COMMERCE/DEPT-18 , Employees Personnel Files Not Covered by Notices of Other Agencies DEPT-25 , Access Control and Identity Management System
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 1: Civilian Personnel Records, GRS 20, item 3: Electronic Records That Replace Temporary Hard Copy Records, NOAA Records Schedules 1406-01: In Situ and Remotely Sensed Environmental Data; 1406-02, Order Processing Information Systems, 1406-03, Metadata Management Database;
	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		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

X	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Although name, address, and phone number can be used to identify specific individuals, this information is publicly available, so there would be low adverse effect to individuals if that information was accessed or disclosed from NOAA5010.
---	-----------------	--

X	Quantity of PII	Provide explanation: If NOAA5010 had a breach of PII, the number of employee information would be less than a 100 individuals so would be low impact.
X	Data Field Sensitivity	Provide explanation: NOAA5010 does not maintain sensitive PII information on the system therefore the impact would be low.
X	Context of Use	Provide explanation: Based on NOAA5010's 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 Indicate whether the conduct of this PIA results in any required business process changes.

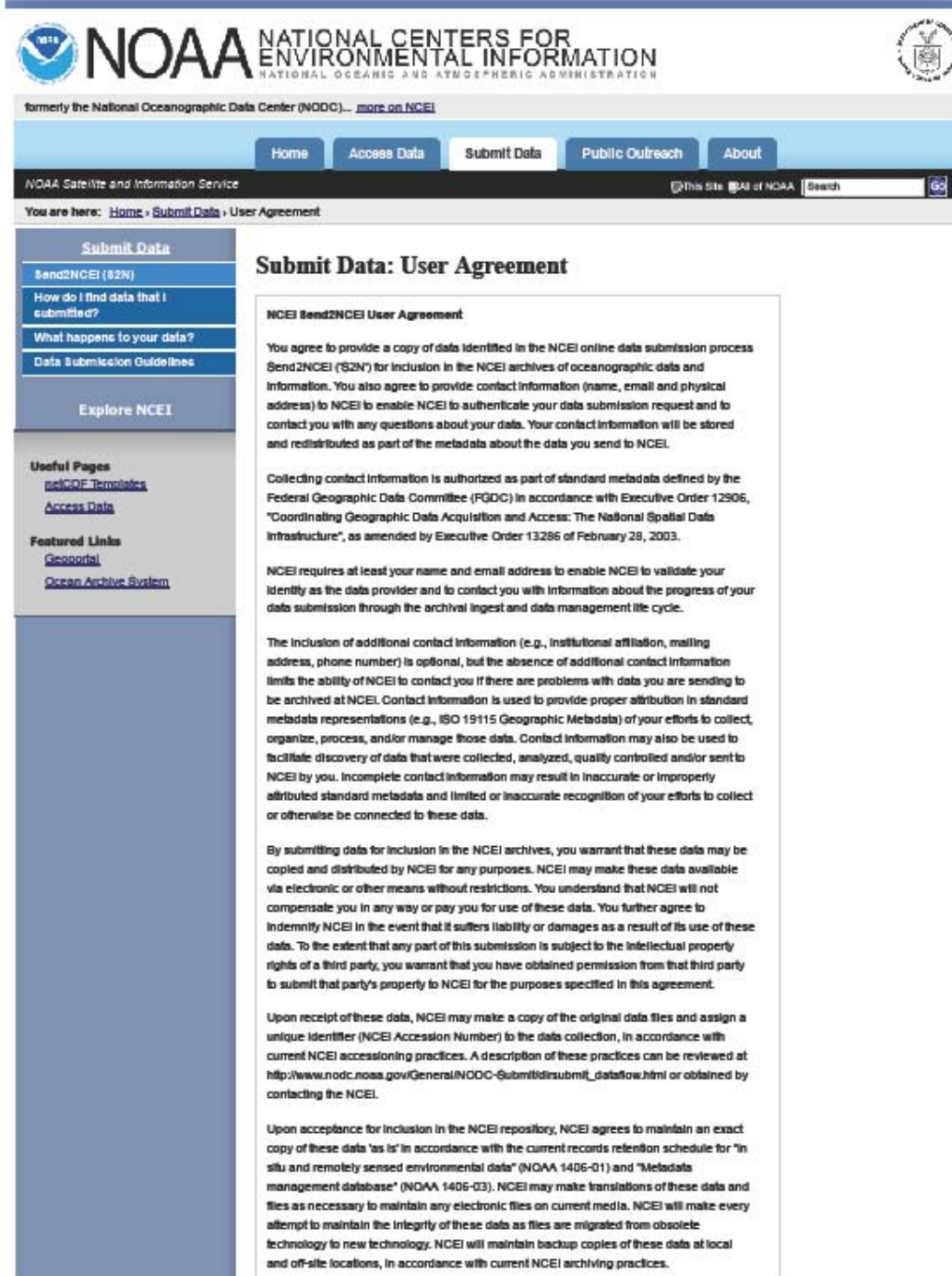
X	Yes, the conduct of this PIA results in required business process changes. Explanation: Addition of NCEI PAS link
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Addition of NCEI PAS link
	No, the conduct of this PIA does not result in any required technology changes.

Attachment

Send2NCEI User Agreement



The screenshot shows the NOAA National Centers for Environmental Information website. The header includes the NOAA logo and the text "NATIONAL CENTERS FOR ENVIRONMENTAL INFORMATION" and "NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION". Below the header is a navigation bar with buttons for "Home", "Access Data", "Submit Data", "Public Outreach", and "About". The "Submit Data" button is highlighted. Below the navigation bar is a search bar and a "You are here" breadcrumb trail: "Home > Submit Data > User Agreement".

The main content area is titled "Submit Data: User Agreement". It contains the following text:

NCEI Send2NCEI User Agreement

You agree to provide a copy of data identified in the NCEI online data submission process Send2NCEI (S2N) for inclusion in the NCEI archives of oceanographic 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. 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. You further agree to indemnify NCEI in the event that it suffers liability or damages as a result of its 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.

Upon receipt of these data, NCEI may make a copy of the original data files and assign a unique identifier (NCEI Accession Number) to the data collection, in accordance with current NCEI accessioning practices. A description of these practices can be reviewed at http://www.nodc.noaa.gov/General/NOODC-SubmitData/submit_dataflow.html or obtained by contacting the 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). 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 Send2NCEI. 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.

I accept the terms and conditions of the User Agreement.


I do not accept the terms and conditions of the User Agreement.

[Continue](#)

[Access Data](#) - [Submit Data](#) - [Inscribed Use of the Data?](#) - [Online Store](#) - [Customer Service](#)

Last modified: Monday, 23-Feb-2015 15:27:17 UTC
[Dept. of Commerce](#) - [NOAA](#) - [NESDIS](#) - [NCEI](#)
[NCEI Main and Other Website Survey](#)
 Onsite Link Notification

[NCEI Info@noaa.gov](#)
[Like us on Facebook](#) | [Follow us on Twitter](#)
[Privacy Policy](#) - [Disclaimer](#) - [Information Quality](#)
[Freedom of Information Act \(FOIA\)](#)
[USA.gov](#) - The U.S. Government's Web Portal



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 _____