

U.S. Department of Commerce
NOAA



Privacy Impact Assessment
for the
National Oceanographic Data Center
(NOAA5010)

Reviewed by: _____, Bureau Privacy Officer or Designee

Approved by:  _____, DOC Chief Privacy Officer

Date approved: 7/31/2015

U.S. Department of Commerce Privacy Impact Assessment NOAA/NODC

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

Introduction: System Description

The National Oceanographic Data Center (NODC) is an enterprise organization that provides scientific and public stewardship for national and international marine environmental and ecosystem data and information. The NODC 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. NODC 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.

NODC 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. The NODC represents NESDIS and NOAA to the general public, government agencies, academic institutions, foreign governments, and the private sector on matters involving oceanographic data.

NODC Stennis 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, and SSNs 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 NASA in order to receive a site badge, and photographs and names are shared with Mississippi State University in order to receive a building keycard/badge. For these instances of sharing, NOAA Headquarters maintains a disclosure log. 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.

In order to better fulfill its mission, NODC receives data and information about the data providers 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 developed to provide another means to collect this data and hold it for review before permanently placing it in the NODC archive holdings. Contact information on data providers consists of name, email address and physical address. Data provider information (see Section 3.1 for description) 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 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).

NODC (NOAA5010) is a moderate-impact system.

Section 1: Information in the System

1.1 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	<input type="checkbox"/>	e. Alien Registration	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>
c. Employee ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>
d. File/Case ID	<input type="checkbox"/>	h. Credit Card	<input type="checkbox"/>
		i. Financial Account	<input type="checkbox"/>
		j. Financial Transaction	<input type="checkbox"/>
		k. Vehicle Identifier	<input type="checkbox"/>
		l. Employer ID Number	<input type="checkbox"/>
m. Other identifying numbers (specify): DoD ID (CAC) Number for employees and contractors			

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

Work-Related Data (WRD)			
a. Occupation	<input type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input type="checkbox"/>
g. Salary			
h. Work History			
i. Other work-related data (specify):			

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

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

Other Information (specify)			

1.2 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	Public Media, Internet		Private Sector	X
Commercial Data Brokers					
Other (specify):					

Section 2: Purpose of the System

2.1 Indicate why the PII/BII in the system is being collected, maintained, or disseminated. Check all that apply.

Purpose					
To determine eligibility	X	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			
Other (specify): Continuity of Operations (COOP)	X				

Section 3: Use of the System

3.1 Provide an explanation of how the bureau will use the PII/BII to accomplish the checked purpose(s), e.g., to verify existing data. Describe why the PII/BII that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and further the mission of the bureau and/or the Department. Indicate if the PII/BII identified in Section 1.1 of this document is in reference to a federal employee/contractor, member of public, foreign national, visitor or other (specify).

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

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/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 NODC, especially for properly crediting the providers and principal investigators on the individual holdings in the archive.

The IP address of the computer submitting data using the online form is collected for security purposes. In the event that NODC 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.

Additionally at NODC Stennis, 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 all 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. NODC Stennis 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 4: Information Sharing

4.1 Indicate with whom the bureau intends to share the PII/BII in the system and how the PII/BII will be shared.

Recipient	How Information will be Shared			
	Case-by-Case	Bulk Transfer	Direct Access	Other (specify)
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.

Section 5: Notice and Consent

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

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 6.	
X	Yes, notice is provided by other means.	<p>Specify how: Notice is provided in the user agreement for Send2NODC service. 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> <p>Information collected for badging purposes, emergency contact, and disaster recovery/continuity of operations: Notice is given in writing during the job application process.</p> <p>Before an employee's/contractor's photograph can be used for a poster, notice is provided by means of a form requesting permission for use, to be signed by the employee.</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:

5.2 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. 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 government 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 for their photographs to be used 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:
--	---	------------------

5.3 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. Employee and contractor General Personal Data information is required for badging and emergency notifications. Employees and contractors are informed of the use of their data at the time the information is collected and data is not used for any other purpose. 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.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

5.4 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 NODC at any time via the online submission service, email to NODC.DataOfficer@noaa.gov , or telephone request to NODC 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 NODC Silver Spring. For NODC Stennis, 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.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 6: Administrative and Technological Controls

6.1 Indicate the administrative and technological controls for the system. Check all that apply.

	All users signed a confidentiality agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff received training on privacy and confidentiality policies and practices.
X	Access to PII/BII is restricted to authorized personnel only.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization: 9/6/2014.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST 800-122 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM). See Appendix A.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Other (specify):

Section 7: Privacy Act

7.1 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. Provide the system name and number: NOAA-11, NOAA Mailing Lists (updated SORN under review at DOC); COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons; and COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
	Yes, a system of records notice has been submitted to the Department for approval on (date).
	No, a system of records is not being created.

Section 8: Retention of Information

8.1 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
	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:

This page is a supplement for item 6.1. Upon final approval, this page must be removed prior to publication of the PIA.

Points of Contact and Signatures

<p>Information Technology Security Officer Name: Amy Bennett Office: NESDIS CID Phone: 301-713-7185 Email: Amy.Bennett@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.</p> <p>BENNETT.AMY.ELIZABETH Signature: <u>H.1169704216</u></p> <p>Date signed: <u>2/13/2015</u></p> <p><small>Digitally signed by BENNETT.AMY.ELIZABETH 1169704216 DN: cn=US, o=U.S. Government, ou=DOC, ou=PII, ou=OTHER, ou=BENNETT.AMY.ELIZABETH.1169704216 Date: 2015.02.13 16:37:05 -0500</small></p>	<p>System Owner Name: Juanita Sandidge Office: NESDIS/NODC Phone: 228-688-4812 Email: Juanita.Sandidge@noaa.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this system.</p> <p>SANDIDGE.JUANITA.C.123 Signature: <u>2228055</u></p> <p>Date signed: <u>2-13-2015</u></p> <p><small>Digitally signed by SANDIDGE.JUANITA.C.1232228055 DN: cn=US, o=U.S. Government, ou=DOC, ou=PII, ou=OTHER, cn=SANDIDGE.JUANITA.C.1232228055 Date: 2015.02.13 15:25:16 -0600</small></p>
<p>NOAA Privacy Officer or Designee Name: Robert Swisher Office: NOAA Office of the Chief Information Officer Phone: 301-628-5755 Email: Robert.swisher@noaa.gov</p> <p>I certify that the PII/BII processed in this system is necessary and this PIA ensures compliance with DOC policy to protect privacy.</p> <p>SWISHER.DONALD.R OBERT.1376511460 Signature: _____</p> <p>Date signed: _____</p> <p><small>Digitally signed by SWISHER.DONALD.R.ROBERT.1376511460 DN: cn=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=SWISHER.DONALD.R.ROBERT.1376511460 Date: 2015.02.19 08:30:17 -0500</small></p>	<p>DOC Chief Privacy Officer Name: Catrina Purvis Office: Office of Privacy and Open Government Phone: 202-482-1190 Email: CPurvis@doc.gov</p> <p>I certify that I have reviewed this PIA for compliance with DOC policy to protect privacy and authorize for this PIA to be published on DOC websites.</p> <p>Signature:  _____</p> <p>Date signed: <u>2/31/2015</u></p>