

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration
(NOAA)**



**Privacy Impact Assessment
for the
Data Archive Management and User System
NOAA5011**

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

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

Date

U.S. Department of Commerce Privacy Impact Assessment NOAA / Data Archive Management and User System

Unique Project Identifier: [Number]

Introduction: System Description

The National Geophysical Data Center (NGDC) mission is to provide long-term scientific data stewardship for the Nation's geophysical data, ensuring quality, integrity, and accessibility. NGDC provides stewardship, products and services for geophysical data describing the solid earth, marine, and solar-terrestrial environment, as well as earth observations from space.

NGDC conducts 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.

In order to better fulfill its mission, NGDC receives data from other NOAA groups, other federal government agencies such as NASA, the U.S. Air Force, the US 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).

PII and BII information contained within the NGDC system boundary provide the System Owner, ISSO, and administrators with the identity and contact information of all authorized users of the system. This information is used for data sharing, to reset passwords, notify users of outages, and support NGDC COOP operations.

Typical Transactions on the NOAA5011 System

Customer: A typical Web-based transaction on the NGDC (NOAA5011) system involves a customer browsing NGDC data holdings and then downloading data based on that browse activity or – in instances where the data to be downloaded is too large to acquire in a single session – the customer fills out an online form – the form contains a link to the NGDC/NOAA5011 Web privacy policy (<http://www.ngdc.noaa.gov/ngdcinfo/privacy.html>). Also see section 7.1.

Data Provider: Data providers and principal investigators may be U.S. Federal, state and local governments, for-profit businesses, non-profit organizations, and academia, their non-U.S.

equivalents, and intergovernmental entities. These organizations have signed Data Submission Agreements to provide NOAA with raw data and derived products. The data can be provided in analog or digital form, and can be submitted to NGDC via the Internet, or shipped to NGDC (tape, disk, etc.).

NOAA Employee or Contractor: Employee and contractor work-related data is collected in paper format, and includes: name, job title, work address, work and home email address, and work and home telephone numbers.

Purposes for Collection of PII and BII

Customer provided PII: 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 to provide the data in compressed format for later retrieval by the user/customer. In some cases, customer provided data is used to manage account information for access to web applications.

Data Providers' PII/BII: 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 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 NGDC, especially for properly crediting the providers and principal investigators on the individual holdings in the archive. Data providers and principal investigators may be U.S. Federal, state and local governments, for-profit businesses, non-profit organizations, and academia, their non-U.S. equivalents, and intergovernmental entities.

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

Work related PII data:

- Names, work addresses and work email addresses collected from employees and contractors are used to manage account information for access control to systems and web applications.
- Names and work email addresses of employees and contractors are used to direct the public to appropriate personnel within the organization.
- For emergency, disaster recovery, and continuity of operations, employee and contractor
- Employee job titles and salaries are collected for Workforce Management purposes.
- 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.

Contractor roles are based on qualifications and training, with the exception they have do not have supervisory roles.

NOAA5011 Information Sharing.

NOAA5011 (NGDC) does not share any of the customer information provided with agencies outside of the Department of Commerce. NOAA5011 does not distribute the information collected from www.ngdc.noaa.gov except for information or data explicitly submitted for redistribution; for example, scientific data, *including metadata*, submitted to NESDIS Data Centers for archiving are made available to customers and other public entities, with notice of such possible distribution given on the data submitters' agreement form (see Section 7.1).

Legal Authority.

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

NGDC (NOAA5011) is a moderate impact system.

Section 1: Status of the Information System – NEW question

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	X
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		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	X
b. IP Address	X	d. Queries Run	X	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		Online	X
Telephone		Email	X		
Other (specify): Email and online apply to data subscribers, and submitters					

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

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

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

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

Purposes for Collection of PII and BII

Customer provided PII: 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 NOAA5011 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 NOAA5011 data administrator staff to manage account information for customer access to web applications (members of the public).

Data Providers PII/BII: 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 NGDC, especially for properly crediting the providers and principal investigators on the individual holdings in the archive. Data providers and principal investigators may be U.S. Federal, state and local governments, for-profit businesses, non-profit organizations, and academia, their non-U.S. equivalents, and intergovernmental entities.

The IP address of the computer submitting data using online forms is collected for security purposes. In the event that NGDC 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 (members of the public). Notification for collection of IP address is made in the NOAA5011 Privacy Policy This is also addressed in Section 7.1.

Work related PII data:

- Names, addresses, and email addresses collected from employees and contractors are

used to manage account information for access control to systems and web applications.

- Names and work email addresses of employees and contractors are used to direct the public to appropriate personnel within the organization.
- For emergency, disaster recovery, and continuity of operations, employee and contractor names, work and home emails and work and home telephone numbers are collected.
- Employee job titles and salaries are collected for Workforce Management purposes.

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):			

<input type="checkbox"/>	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: NCDC LAN/NOAA5009 and NGDC LAN/NOAA5010. 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 in Data Submission User Agreement Executive Summary, Pag ii, after cover page and approval page)	
X	Yes, notice is provided by other means.	<p>Specify how: Notice is provided to the customers via the NOAA5011 Web Privacy Policy (www.ngdc.noaa.gov/ngdcinfo/privacy.html) and the NOAA Privacy Policy (http://www.noaa.gov/privacy.html). This includes notice of collection of IP address.</p> <p>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).</p> <p>Information collected for employee/contractor emergency contact, and disaster recovery/continuity of operations is requested in writing. NOAA5011 distributes a request – via a paper form - for NCEI Emergency Contact information to each NOAA5011 staff member (federal and contractor). NOAA5011 Supervisors receive a paper copy: “NCEI Emergency Listing,” for their division, for COOP and other emergency contact. This Supervisor’s NCEI Emergency Listing paper form is marked: “Confidential.”</p> <p>Information collected for account management is requested in writing or via email by the user’s supervisor in the request for</p>

		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: Only contact information, in the form selected by the customer or data provider is requested. The customer will provide this information only if he/she wants certain products and information. As stated in the NGDC privacy policy (http://www.ngdc.noaa.gov/ngdcinfo/privacy.html), stating that any information to NGDC is voluntary. Employees filling out forms may decline to provide PII /BII for emergency contact and disaster recovery. However, in choosing to do so, they will not be contacted in the event of an emergency or COOP situation.
	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: The NOAA5011 web-site, Privacy Policy page (http://www.ngdc.noaa.gov/ngdcinfo/privacy.html) details how customer and data-provider information may be used. <i>By checking products and notifications desired, the customer consents to the use of his/her contact information for the purpose of providing those items.</i> Data providers and principal investigators consent to the collection and publication of their data when they submit data for archiving – as stated in the NOAA5011 signed Data Submission Agreements. Employee and contractor information is required for emergency notifications. Employees and contractors are informed of the use of their data as stated in the Emergency Contact forms the employee fills out and updates.
	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: Instructions for updating contact information fields are provided in the forms the customer fills out. Data providers receive a copy of the NOAA5011 Data Submission Agreement they have signed, and have the
---	---	---

		<p>opportunity to submit updates pertaining to the BII , by email to the database administrator, as will be stated in the revised agreement.</p> <p>The employee fills out and updates the Emergency Contact form at least annually.</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.
	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: Access or attempted access to PII/BII on the system is recorded in system logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u> 01/18/2016 </u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

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

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

All NOAA5011 output devices (monitors, printers and audio devices) are operated within NOAA5011 controlled spaces. Critical consoles for NOAA5011 servers are located in keycard access controlled computer rooms. NOAA5011 positions monitors away from windows whenever possible.

- Encryption is used for PII/BII in electronic transit.
- Backup tapes containing PII/BII are transported in locked containers.
- Media is sanitized prior to disposal or reuse.
- A shredder has been made available to NOAA5011 personnel for destruction of sensitive documents.

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> : Commerce/NOAA - 11 – “Contact Information for Members of the Public Requesting or Providing Information Related to NOAA’s Mission”; Commerce/Department 18 - "Employees Personnel Files Not Covered by Notices of Other Agencies"
	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 3.1 General Technology Management Records, Item 040: Information technology oversight and compliance records, GRS 3.2 Information Systems Security Record, Items 030, 031: System access 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.) - **NEWquestion**

Disposal			
Shredding	X	Overwriting	
Degaussing	X	Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels – NEW question (see link in [PIA guidance](#) in this part of the guidance-imbedded template, for how to answer this.

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.)

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: There is little PII and it is not sensitive.
X	Data Field Sensitivity	Provide explanation: There is no sensitive information.
X	Context of Use	Provide explanation: Information is not used in sensitive context.
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	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: Note that metadata will be included in shared research, and Privacy Act Statement, added to Data Submission Agreement.
	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.

	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.

Points of Contact and Signatures

<p>Information System Security Officer or System Owner Name: Marcus O. Ertle, NOAA5011 ISSO Office: NOAA/NESDIS/NCEI Phone: (303) 497-6139 Email: Marcus.O.Ertle@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 IT system.</p> <p style="text-align: center;">ERTLE.MARCUS <small>Digitally signed by ERTLE.MARCUS.O.1365880871 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=ERTLE.MARCUS.O.1365880871 Date: 2016.06.01 13:41:52 -04'00'</small></p> <p>Signature: <u>.O.1365880871</u></p> <p>Date signed: <u>6/1/2016</u></p>	<p>Information Technology Security Officer Name: Nancy A. DeFrancesco Office: NOAA/NESDIS/ACIO-S Phone: (240) 429-0285 Email: Nancy.DeFrancesco@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 IT system.</p> <p style="text-align: center;">DEFRANCESCO.NA <small>Digitally signed by DEFRANCESCO.NANCY.A.1377370917 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=DEFRANCESCO.NANCY.A.1377370917 Date: 2016.06.01 16:27:09 -04'00'</small></p> <p>Signature: <u>NCY.A.1377370917</u></p> <p>Date signed: <u>06/01/2016</u></p>
<p>Authorizing Official Name: Margarita Gregg Office: NOAA/NESDIS/NCEI Phone: (301) 713-3270 Email: Margarita.Gregg@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 IT system.</p> <p style="text-align: center;">GREGG.MARGARITA <small>Digitally signed by GREGG.MARGARITA.ELENA.1365899017 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GREGG.MARGARITA.ELENA.1365899017 Date: 2016.06.07 12:26:34 -04'00'</small></p> <p>Signature: <u>.ELENA.1365899017</u></p> <p>Date signed: <u>06-07-2016</u></p>	<p>Bureau Chief Privacy Officer Name: Mark Graff Office: NOAA OCIO Phone: 301-628-5658 Email: mark.graff@noaa.gov</p> <p>I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.</p> <p style="text-align: center;">GRAFF.MARK.HYR <small>Digitally signed by GRAFF.MARK.HYRUM.1514447892 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OTHER, cn=GRAFF.MARK.HYRUM.1514447892 Date: 2016.06.16 10:38:33 -04'00'</small></p> <p>Signature: <u>UM.1514447892</u></p> <p>Date signed: _____</p>

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.