Version Number: 01-2015

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

Privacy Impact Assessment
for the
Comprehensive Large Array-data Stewardship System (NOAA5040)

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: 2017.08.04 10:23:04 -04'00'

7/20/2017

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

U.S. Department of Commerce Privacy Impact Assessment

Unique Project Identifier: 006-000320500 00-48-01-13-01-00

Introduction: System Description

CLASS promotes the NESDIS mission by providing a repository of environmental data provided by a variety of ground-based (in-situ) and remotely-sensed observing systems. CLASS is a multi-site system with production assets hosted at the NOAA Satellite Operations Facility (NSOF) in Greenbelt MD; the National Centers for Environmental Information – North Carolina (NCEI-NC) in Asheville NC; the National Centers for Environmental Information – Colorado (NCEI-CO) in Boulder CO, and a backup/fail-over presence at the NOAA Environmental Security Computing Center (NESSC) in Fairmont WV. Development facilitates are located in Greenbelt MD and Fairmont WV. CLASS ingests, archives, and provides timely access to, and distribution of, this environmental data. Specifically, CLASS ingests data from the:

- Geostationary Operational Environmental Satellites (GOES),
- Polar-orbiting Operational Environmental Satellites (POES),
- Defense Meteorological Satellite Program (DMSP),
- Joint Polar-orbiting Operational Satellite System (JPSS)
- European Meteorological Operational Satellite (MetOp)
- Canadian Space Agency's Synthetic Aperture Radar Satellites (Radarsat)
- Ocean Surface Topography (OSTM/Jason)
- Suomi National Polar-orbiting Partnership (S-NPP)
- Global Change Observation Mission - Water (GCOM-W)
- Continuing Operating Reference Stations and Derived Products data

Those requesting data could be federal employees/contractors, members of the public, foreign nationals or visitors, with federal employees and members of the public being the most frequent.

After the initial account creation, initiated via an email request, a typical user interaction (customer submitting an order) would be as follows:

1. The user logs on with the system-supplied user name and the user-selected password.
2. Once authenticated, the user selects the desired data and the required delivery format (electronic via shipment of physical media).
3. The user logs off the system.

Information Sharing: User contact information is shared within the bureau, with NOAA5009, in bulk orders for data.

The authority for collection of this information is 5 U.S.C. 301, Departmental Regulations. Additional authority

from COMMERCE/NOAA-11: 15 U.S.C. § 1512, Powers and duties of Department.

This 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):					

_X____ This is an existing 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		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	
b. IP Address	x	d. Queries Run	x	f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)
Facsimile number

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		Hard Copy: Mail/Fax		Online	x
Telephone		Email	x		
Other (specify):					

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

Non-government Sources					
Public Organizations		Private Sector		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):			

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).

Contact information is maintained for the purpose of sharing of environmental data, and secondarily, the reconciliation of ad hoc orders and for support of subscription orders. There is no requirement that information provided be directly related to an individual. For example: a CLASS user could submit an email address classdata@mydomain.com, or classdata@some.edu. The PII identified above could be for federal employees/contractors, members of the public, foreign nationals or visitors, with federal employees and members of the public being the most frequent.

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			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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	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, National Center for Environmental Information – North Carolina (NCEI-NC) 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.
	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: _www.class.noaa.gov/release/system_help/subs/index.htm_____The direct link to the PAS is https://www.class.ngdc.noaa.gov/privacy_act_statement.html _____.	
X	Yes, notice is provided by other means.	Specify how: Web registration form at www.class.noaa.gov/release/system_help/subs/index.htm describes the usage of submitted information, e.g. for the receipt of selected products and of email notifications.
	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 preferred by the subscriber, is requested. The subscriber will provide this information in the email requesting an account, only if he/she wants certain products and information.
	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	Specify how: By checking products and notifications desired, the subscriber consents to the use of his/her contact information

	PII/BII.	for the purpose of providing those items.
	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 information fields are provided in the subscription forms. The subscriber may provide these updates online at any time.
	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: Access to file systems in NOAA5040 CLASS maintained servers is logged as part of Continuous Monitoring compliance under NIST 800-53r4 control selection appropriate for a Moderate FISMA system.
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): August 24, 2016. ☐ 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 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.

As per relevant NIST 800-53r4 controls, NOAA5040 CLASS Access Control technologies, logging of file system activity and access control are applied, monitored, and audited as per FISMA compliance for a FIPS 199 categorized Moderate impact system. As an example; Access Control is regulated by multi-factor authentication, consisting of the use of a Common Access Card or CAC as a physical token and a 6 digit PIN, as required by NOAA's HSPD-12 strong authentication compliance program. In addition to multi-factor authentication, NOAA5040 CLASS limits access to PII that is collected and stored for the support of order reconciliation to only those staff members whose role within the organization requires their legitimate business use of that data.

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 *(list all that apply)*: NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission.
	Yes, a SORN has been submitted to the Department for approval on
	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: National Oceanic and Atmospheric Administration National Environmental Satellite, Data, and Information Services Revised 7/05 (N1-370-03-10) 11-16-2012, DAA-370-2012-001) 1404, Office of Satellite Data Processing and Distribution
	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		Overwriting	x
Degaussing	x	Deleting	
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: There is no requirement that the email address and other identification must be directly related to the individual.
	Quantity of PII	Provide explanation:
x	Data Field Sensitivity	Provide explanation: This information is not sensitive PII.
x	Context of Use	Provide explanation: The PII collected by CLASS is used to support order fulfillment of public domain information – publicly available climate data. The potential breach of PII would not significantly impact those users.
	Obligation to Protect Confidentiality	Provide explanation:
x	Access to and Location of PII	Provide explanation: Since the PII collected is used strictly for communication with end users of the system, and not shared with other agencies, or used for other business purposes, the potential for breach is limited. Access to this information by internal users of the system (Operations and System Administration staff) is restricted on a "need to know" basis for legitimate business purposes, such as order reconciliation and end user support.
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.