Version Number: 01-2020

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

Privacy Impact Assessment
for the
NOAA5040

Comprehensive Large Array-data Stewardship System (CLASS)

Reviewed by: Mark H. 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

Jennifer Goode 07/22/2021

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NESDIS/Comprehensive Large Array-data Stewardship System (CLASS)

Unique Project Identifier: NOAA5040

Introduction: System Description

The CLASS is an electronic archive of environmental data. CLASS is NOAA's on-line facility for the distribution of weather, climate and geophysical data supplied by NOAA, NASA, US Department of Defense (DoD) and other sources via direct and indirect connections.

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

NOAA5040 (CLASS) is a Major Application.

(b) System location

CLASS is a distributed system with components at five locations:

- National Satellite Operations Facility (NSOF) Suitland, MD hosts CLASS-Suitland (CLASS-SUI)
- National Center for Environmental Information-North Carolina (NCEI-NC) Asheville; NC hosts CLASS-Asheville (CLASS-AVL)
- National Center for Environmental Information-Colorado (NCEI-CO) at Boulder, CO hosts CLASS-Boulder (CLASS-BOU)
- National Environmental Data Center (NEDC) at Fairmont, WV hosts CLASS-Consolidated Back Up (CLASS-CBU).
- Amazon Web Services in WV hosts a CLASS instance in the Cloud (CLASS-AWS)

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The following list is the interconnections CLASS uses to collect, share and monitor activities (the first five and NSOF do not provide data to be archived):

- NOAA Cyber Security Center NOAA0100
- Web Operations Center NOAA0201
- N-Wave NOAA0550
- Headquarters Information Technology Support Local Area Network NOAA5006
- NCEI-NC NOAA5009
- NCEI-CO NOAA5011
- JPSS NOAA5042
- NSOF LAN NOAA5044
- ESPC NOAA5045 at NSOF

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The major functions that CLASS performs include the following:

- Ingest of environmental data from data providers
- Archiving of data
- Extraction and recording of descriptive information describing the data archived in CLASS
- Provision of browse and search capability to assist users in finding data
- Dissemination of CLASS data in response to user requests
- Operational support including 24x7 operation and disaster recovery

(e) How information in the system is retrieved by the user

Access to stored sensitive information is granted by roles and responsibilities. CLASS personnel must log into the system using encrypted authentication.
In order to retrieve publically available data, the user will create an account. 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.

(f) How information is transmitted to and from the system

Personally Identifiable Information is retained and stored after account creation in order to communicate with CLASS public users about system details such as planned outages and new data sets. Only CLASS internal personnel have access to this information.
All stored mission data is non-sensitive and most is publicly available. Exceptions are documented in Inter-Connection Documents (ICDs) or other agreements between CLASS and data providers.

(g) Any information sharing conducted by the system

CLASS applications do not share PII outside of NOAA.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

5 U.S.C. 301 E-Government Act of 2002 includes FISMA The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1) OMB Circular A-130 Managing Information as a Strategic Resource July 27, 2016 OMB M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 2003-09-26 OMB M-05-08 Designation of Senior Agency Officials for Privacy 2005-02-11 OMB M-06-16 Protection of Sensitive Agency Information 2006-06-23 OMB M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information 2007-05-22 OMB M-10-23 Guidance for Agency Use of Third-Party Websites and Applications 2010-06-25 Federal Acquisition Regulation website: https://www.acquisition.gov Federal Enterprise Architecture Security and Privacy Profile September 2010-12-04 DOC Information Technology Security Baseline Policy (ITSBP) v1.0 June 2019CITR-006 Information System Security Training for Significant Roles June 18 2013 NAO 212-1301 Information Technology Security Manual (ITSM), v6.1, November 13, 2019

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

Moderate

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, and there is not a SAOP approved Privacy Impact Assessment.

__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

X This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

Section 2: Information in the System

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

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

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement / contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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)

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 Describe how the accuracy of the information in the system is ensured.

Information collected by the NOAA5040 web application for external users requesting access to public facing data are required to provide information to CLASS for contact purposes. The user inputting the data is responsible for the accuracy of this information.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

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

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	

Other (specify):

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Contact information is maintained for the purpose of sharing 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.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Although there is a possibility of insider threat, risk is minimal since the PII contained in the system is limited. Mandatory training is provided for system users regarding appropriate handling of information. PII is degaussed, overwritten, or destroyed when no longer needed.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

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

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: • NOAA Cyber Security Center NOAA0100 • Web Operations Center NOAA0201 • N-Wave NOAA0550 • Headquarters Information Technology Support Local Area Network NOAA5006 • NCEI-NC NOAA5009 • NCEI-CO NOAA5011 • JPSS NOAA5042 • NSOF LAN NOAA5044 • ESPC NOAA5045 at NSOF • 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.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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

Class of Users			
General Public		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: https://www.avl.class.noaa.gov/privacy_act_statement.html	
X	Yes, notice is provided by other means.	Specify how: Web registration form at https://www.avl.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 PII/BII.	Specify how: By checking products and notifications desired, the subscriber consents to the use of his/her contact information 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 the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 9/25/2020 ☐ 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 controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

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 FIPS199 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 the legitimate business use of that data.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

__ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

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

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission 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 (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

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

X	There is an approved record control schedule. Provide the name of the record control schedule: 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): Solid State Drives (SSDs) cannot be degaussed, so NOAA5040 has these physically destroyed when they are no longer needed.			

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

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 level. *(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: The 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-publically 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 the 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 Identify and evaluate any potential threats to privacy that exist in light of the information

collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

No changes were made to CLASS information collection. The minimum amount of information is collected in order to provide the data requested.

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

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

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

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