Version Number: 01-2020

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

**Privacy Threshold Analysis**
**for the**
**NOAA5040**

Comprehensive Large Array-data Stewardship System (CLASS)

Version Number: 01-2020

# U.S. Department of Commerce Privacy Threshold Analysis

# NOAA/NESDIS/Comprehensive Large Array-data Stewardship System (CLASS)

**Unique Project Identifier: NOAA5040**

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system and its purpose:** 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.

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

*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 purpose that the system is designed to serve*

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) The way the system operates to achieve the purpose*

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 ingests, archives, and provides timely access to, and distribution of, this environmental data.

*f) A general description of the type of information collected, maintained, used, or disseminated by the system*

NESDIS is responsible for the collection, archiving, and dissemination of environmental data collected by a variety of in-situ and remote sensing observing systems operated by NOAA and by a number of its partners. To prepare for large increases in its data holdings, NESDIS has developed the CLASS.
The CLASS is an electronic archive of environmental data. CLASS distributes weather, climate and geophysical data supplied by NOAA, NASA, US Department of Defense (DoD) and other sources.

*g) Identify individuals who have access to information on the system*

All users that have access to PII on the information system are internal. These include system administrators, security analysts, and database administrators.

*h) 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 weather 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

*i) 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.

**Questionnaire:**

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

| **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. *Continue to answer questions and complete certification.*

____ 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). *Continue to answer questions and complete certification.*

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). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X_ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

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

_X_ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

_X_ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

_X_ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_X_ DOC employees
_X_ Contractors working on behalf of DOC
____ Other Federal Government personnel
_X_ Members of the public

____ No, this IT system does not collect any PII.

***If the answer is "yes" to question 4a, please respond to the following questions.***

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

| |
|---|
| Provide an explanation for the business need requiring the collection of SSNs, including truncated form. |
| Provide the legal authority which permits the collection of SSNs, including truncated form. |

_X_ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

_X_ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

_X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

***If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.***

# CERTIFICATION

_X____ I certify the criteria implied by one or more of the questions above **apply** to the Comprehensive Large Array-data Stewardship System (CLASS) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

| | |
|---|---|
| **Information System Security Officer or System Owner**<br>Name: Thomas Byrd<br>Office: CLASS ISSO<br>Phone: 828-257-3172<br>Email: Thomas.Byrd@noaa.gov<br><br>Signature: BYRD.THOMAS.E.II.1386145438 Digitally signed by BYRD.THOMAS.E.II.1386145438 Date: 2021.05.12 10:40:13 -04'00'<br>Date signed: | **Information Technology Security Officer**<br>Name: Robert Bunge<br>Office: NESDIS/ACIO-S<br>Phone: 301-683-3565<br>Email: Robert.Bunge@noaa.bov<br><br>Signature: BUNGE.ROBERT.DAVID.1207631279 Digitally signed by BUNGE.ROBERT.DAVID.1207631279 Date: 2021.05.17 10:59:06 -04'00'<br>Date signed: |
| **Privacy Act Officer**<br>Name: Adrienne Thomas<br>Office: NOAA OCIO<br>Phone: 240-577-2372<br>Email: Adrienne.Thomas@noaa.gov<br><br>Signature: THOMAS.ADRIENNE.M.1365859600 Digitally signed by THOMAS.ADRIENNE.M.1365859600 Date: 2021.05.17 14:43:43 -05'00'<br>Date signed: | **Authorizing Official**<br>Name: Richard Marlow<br>Office: NESDIS/OSPO<br>Phone: 301-817-4105<br>Email: Richard.Marlow@noaa.gov<br><br>Signature: MARLOW.RICHARD.GREGORY.1522118490 Digitally signed by MARLOW.RICHARD.GREGORY.1522118490 Date: 2021.05.17 11:49:24 -04'00'<br>Date signed: |
| **Bureau Chief Privacy Officer**<br>Name: Mark Graff<br>Office: NOAA OCIO<br>Phone: 301-628-5658<br>Email: Mark.Graff@noaa.gov<br><br>Signature: GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892 Date: 2021.05.24 15:21:28 -04'00'<br>Date signed: | |