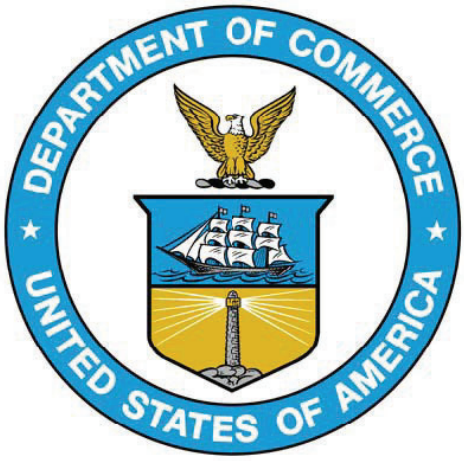
Version Number: 01-2020

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




## Privacy Impact Assessment
## for the
## NOAA5011
## National Geophysical Data Center Data Archive Management and User System (NGDC)

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

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2021.08.02 16:36:01 -04'00'

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

# U.S. Department of Commerce Privacy Impact Assessment
# NOAA/NESDIS/NGDC

**Unique Project Identifier: NOAA5011 (06-000321900)**

**Introduction: System Description**

NOAA's National Center for Environmental Information (NCEI) maintains the world's largest climate data archive and provides climatological services and data to every sector of the U.S. economy and to users worldwide. NCEI operates data centers in Asheville, NC and Boulder, CO with additional offices at Stennis Space Center, MS and College Park, MD. NCEI located in Boulder, CO, comprises the NOAA5011 system.

The NCEI archive contains more than 37 petabytes of data, equivalent to about 400 million filing cabinets filled with documents. NCEI facilitates the acquisition of these environmental data collected by NOAA, by other agencies and departments of the U.S. government, as well as by other institutions, organizations, and governments in the U.S. and around the world.

NCEI, as part of the data stewardship mission of providing access and dissemination of the archive holdings, offers users access to tens of thousands of datasets and hundreds of products. NCEI provides search and discovery web platforms to enable the user community to efficiently find and retrieve data through a number of interfaces and services.

NCEI resources are used for scientific research and commercial applications in many fields, including agriculture, forestry, marine and coastal ecosystems, tourism, transportation, civil infrastructure, energy, transportation, water resources, energy, health, insurance, litigation, and national security. NCEI scientists work as lead contributors to the National Climate Assessment, as well publish periodic publications such as the Annual and Monthly State of the Climate Reports.

As part of the National Environmental Satellite, Data, and Information Service (NESDIS), NCEI coordinates with other data centers in related scientific and technical areas to provide standardized, robust, and efficient service.

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

| |
|---|
| NOAA's National Centers for Environmental Information (NCEI) is a General Support System (GSS). |

*(b) System location*

NOAA5011 is physically located in the David Skaggs Research Center in Boulder, CO.

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

NOAA5011 has an interconnection with NCEI-NC (NOAA5009) which was created to facilitate sharing of internal resources. The interconnection includes access to the system's intranet applications and shared code repositories. Access to resources is approved via the configuration management process. NOAA5009 and NOAA5011 are classified as moderate systems and may exchange data at that categorization level. NOAA5011 agreements are in place for services between NOAA5011 and other government agencies or universities.

The below connection agreements are in force:

| Organization | Purpose | Agreement Type |
|---|---|---|
| **NOAA0100 - NOAA Cyber Security Center** | SOC ISAs/SLAs | NOAA CIO Waiver |
| **NOAA0550 – NOAA NWAVE** | NW Connectivity | ICD |
| **NOAA5006 - Headquarters Information Technology Support Local Area Network** | NW / Office Apps | ICD |
| **NOAA5040 - Comprehensive Large Array-data Stewardship System** | Internet & Office Space | ICD |
| **NOAA8864 – Space Weather Prediction Center** | Data acquisition | ISA |
| **NOAA5009 – National Climatic Data Center Local Area Network** | NCEI interconnectivity | Organizational – Same AO / SO. |

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

NCEI-CO receives data from other NOAA groups, other federal government agencies such as NASA, the U.S. Air Force, the U.S. 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).
The system operates in the traditional client-server model. Data is hosted on servers and made available via various protocols such as HTTPS, FTP, SFTP, and SSH.

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

Internal NOAA5011 users retrieve data via internal file servers, the public web presence, and via anonymous FTP. External users retrieve data via the NOAA5011 public web presence and via anonymous FTP downloads of public data.

Organizational users authenticate using GFE and their Common Access Card to access in the information system. This provides users secure access that is managed by the program and supported by NOAA5011.

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

NOAA5011 (NCEI-CO) has a dedicated 10 gigabits per second (Gbps) link providing Wide Area Network (WAN) access from NCEI-CO to the Internet through the NOAA NWAVE (NOAA0550). Physical connectivity is provided via standard Ethernet configured at 10 Gbps. Endpoint access to the Internet is configured at 30 Gbps and provided via the N_WAVE TICAP Service in Boulder, CO. In addition, NCEI-CO receives data from NOAA ships via external disk drives for data processing. The data from these disks are loaded onto local file servers on NOAA5011. Information is transmitted to and from the system using the following protocols using a client/server model: SFTP, FTP, SSH, and HTTPS.

*(g) Any information sharing conducted by the system*

NCEI-CO 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, as well as the general public where appropriate.

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

Employee information is not shared outside of the organization.

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

The legal authority for collection of information addressed in this PIA include:

- 5 U.S.C. § 301, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records;
- 44 U.S.C. 3101, Records Management by Agency Heads;
- The Electronic Signatures in Global and National Commerce Act, Public Law 106-229;
- Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504 note);
- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004;

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

NOAA5011 is a FIPS 199 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): | | | | | |

____ 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 | X | f. Salary | | j. Proprietary or Business Information | X |
| 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 | X |
| b. IP Address | X | f. 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 | X | Online | X |
| Telephone | | Email | X | | |

| |
|---|
| Other (specify):<br>Email and online apply to data subscribers, and submitters. NOAA5011 requires the use of cryptographic mechanisms by those sending data to the system whenever possible, to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. The mechanisms [for web-based transmissions, including web-based forms] include SSL/TLS encryption. |

| **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 | X |
| Third Party Website or Application | | | | | |
| Other (specify): | | | | | |

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

| |
|---|
| Access control lists are used to ensure that both reading and modifying data is limited to authorized personnel. Additionally, encryption and file integrity tools are used where required. |

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| | Yes, the information is covered by the Paperwork Reduction Act.<br>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 | X | 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).

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 NCEI, 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 NCEI 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 are collected for Workforce Management purposes.

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.)

Mishandling of privacy information by authorized users is the primary threat to privacy. To counter this threat, users are required to take annual IT security awareness training regarding appropriate handling of privacy information. Other threats include a malicious user

| |
|---|
| compromises an internal system and gains unauthorized access. Technical controls are used to mitigate that threat. Those include the use of access control lists, encryption of data at rest and in motion, and multi-factor authentication. |

## 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): | | | |

| | |
|---|---|
| | 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?

| | |
|---|---|
| X | 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. |
| | 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.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:<br>• NOAA0100, NOAA Security Operations Center<br>• NOAA0550 – NOAA NWAVE |

| | |
|---|---|
| | • NOAA5006, NESDIS HQ LAN<br>• NOAA5040, Comprehensive Large Array-data Stewardship System<br>• NOAA8864, Space Weather Prediction Center<br>• NOAA5009, National Climatic Data Center Local Area Network<br><br>Physical and logical access to PII/BII is restricted to authorized personnel only. Encryption is used for PII/BII in transit. Media is sanitized prior to disposal.<br><br>Where a higher level of integrity and/or confidentiality is required, NOAA5011 employs cryptographic mechanisms, such as SSH, HTTPS, or FTPS. Secure Sockets Layer or Transport Layer Security (SSL/TLS) is used to protect the confidentiality of data transmission when authentication is required. |
| | 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):<br><br>External users have access to publicly available scientific data and information, but, do not have access to PII, other than Data Provider's PII, including name, email, and physical address that may be included with publicly available metadata for contributed data. | | | |

## 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:<br>.<br>http://www.ngdc.noaa.gov/wiki/images/f/f4/NOAA_Sub_Agreement.docx (link in Data Submission User Agreement Executive Summary, Page ii, after cover page and approval page – internal wiki page); and for subscribers: https://www.ngdc.noaa.gov/privacy-act-statement-data-requestors.pdf. For continuity of operations, there is a PAS on the document enclosed with this PIA. |

| | | |
|---|---|---|
| X | Yes, notice is provided by other means. | Specify how:<br><br>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.<br><br>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**).**<br><br>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."<br><br>Information collected for account management is requested in writing or via email by the user's supervisor in the request for 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:<br><br>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 NCEI-CO privacy policy (https://www.ngdc.noaa.gov/ngdcinfo/privacy.html), stating that any information to NCEI-CO is voluntary.<br><br>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:<br><br>The NOAA5011 web-site, Privacy Policy page (https://www.ngdc.noaa.gov/ngdcinfo/privacy.html) details how customer and data-provider information may be used. *By checking products and notifications desired, the customer consents to the use of his/her contact information for the purpose of providing those items.* 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.<br><br>Employee and contractor information is requested 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:<br><br>Instructions for updating contact information fields are provided in the forms the customer fills out.<br><br>Data providers receive a copy of the NOAA5011 Data Submission Agreement they have signed, and have the opportunity to submit updates pertaining to the BII, by email to the database administrator, as will be stated in the revised agreement.<br><br>The employee fills out and updates the Emergency Contact form at least annually. |
| | 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.<br>Explanation:<br>PII/BII on the system is located in access restricted folders. Access or attempted access to these folders is recorded in system logs. |

| | |
|---|---|
| X | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): **1/18/2021**<br>☐ 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. **MODERATE** |
| 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).*

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 and at rest. Secure protocols such as HTTPS and SFTP for data in motion.
- 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 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).<br>Provide the SORN name, number, and link. *(list all that apply)*:<br><br>Commerce/NOAA - 11 – "Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission";<br>Commerce/Department 18 - "Employees Personnel Files Not Covered by Notices of Other Agencies"<br>Commerce/Department 13, Investigative and Security Records<br><br>COMMERCE/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.<br>Provide the name of the record control schedule:<br><br>2.1 Employee Acquisition Records<br>2.2 Employee Management Records<br>2.3 Employee Relations Records<br>2.4 Employee Compensation & Benefits Records<br>2.5 Employee Separation Records<br>2.6 Employee Training Records<br>2.7 Employee Health & Safety Records<br>,<br>GRS 3.1 General Technology Management Records, Item 040: Information technology oversight and compliance records,<br>GRS 3.2 Information Systems Security Record, Items 030, 031: System access records,<br>NOAA Records Schedules 1406-01: In Situ and Remotely Sensed Environmental Data;<br>1406-02, Order Processing Information Systems,<br>1406-03, Metadata Management Database |
| | No, there is not an approved record control schedule.<br>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.<br>Provide explanation: |

*10.2* Indicate the disposal method of the PII/BII. *(Check all that apply.)*

| **Disposal** | | | |
|---|---|---|---|
| Shredding | X | Overwriting | |
| Degaussing | X | Deleting | X |
| Other (specify): | | | |

## 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.)*

| | | |
|---|---|---|
| | Identifiability | Provide explanation: |
| X | Quantity of PII | Provide explanation:<br>There is little PII and it is not sensitive. |
| X | Data Field Sensitivity | Provide explanation:<br>There is no sensitive information. |
| X | Context of Use | Provide explanation:<br>Information is not used in sensitive context. |
| | Obligation to Protect Confidentiality | Provide explanation: |
| X | Access to and Location of PII | Provide explanation:<br>Access to PII is described above in Section 8.2 Physical and logical access restrictions are in place as prescribed in NIST SP 800-53. |
| | 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.)

| |
|---|
| NCEI-CO collects very little privacy information. With the introduction of the Administration LAN (NOAA5006), much of the employees' personal information collected for HR requirements have been moved to that FISMA system. Threats and mitigations to the remaining non-sensitive PII are identified in sections 5 and 8 above. |

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.<br>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.<br>Explanation: |
| X | No, the conduct of this PIA does not result in any required technology changes. |