

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




Privacy Impact Assessment
for the
NOAA8882
National Weather Service Eastern Region

Reviewed by: Robin Burrress for 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

Robin.Burrress Digitally signed on

 2025.07.14 08:44:48 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment

NOAA/NWS/ER General Support System

Unique Project Identifier: NOAA8882

Introduction: System Description

The National Weather Service (NWS) delivers weather, hydrologic, and climate forecasts and warnings for the United States, its territories, and surrounding waters, with the primary mission of protecting life and property, as well as enhancing the national economy. The environmental data and products produced by NWS contribute to a national information infrastructure that serves government agencies, the private sector, the public, and international partners.

Within this framework, the NOAA8882 system plays a critical role in collecting, processing, and disseminating supplemental weather data that enhances warning and forecasting capabilities. The system also supports the Eastern Region's administrative operations, as well as scientific and technical research and innovation efforts at both the regional headquarters and field offices.

NOAA8882 operates across a diverse array of hardware and software platforms, many of which are interconnected to enable seamless mission execution. The system infrastructure includes Wide Area Networks (WANs), Local Area Networks (LANs), host systems, and client-server architectures. Supported functions and applications include communication, office productivity tools, database management, and image and data processing, all of which are essential to NWS operations.

Address the following elements:

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

NOAA8882 is a general support system.

(b) System location

NOAA8882 is a distributed system composed of the Eastern Region Headquarters (ERHQ) located in Bohemia, New York, along with 23 Weather Forecast Offices (WFOs), 3 River Forecast Centers (RFCs), and 4 Center Weather Service Units (CWSUs) strategically located throughout the region.

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

NOAA8882 interconnects with the following FISMA systems (ALL internal to National Oceanic & Atmospheric Administration (NOAA)):

NOAA0100 – NOAA Cyber Security Center (H)*

NOAA8102 – Automated Surface Observation System (ASOS)

NOAA8106 – Upper Air Observing System (UAOS)

NOAA8107 – Advanced Weather Interactive Processing System (AWIPS)

NOAA8850 – Enterprise Mission Enabling System (EMES)

NOAA8860 – Weather and Climate Computing Infrastructure Services (WCCIS)

*Note: The interconnection with NOAA0100 is not a new interconnection. NOAA0100 has been updating the documentation in CSAM to reflect its interconnections with the other NOAA FISMA systems.

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

NOAA8882 operates within a security architecture designed to promote network segmentation, redundancy, and the elimination of single points of failure, enhancing the system's ability to manage risk effectively. The system's design and operations are informed by its mission, business needs, and applications, with an emphasis on identifying opportunities to leverage shared resources and implement efficient, scalable solutions. NOAA8882 is committed to implementing security measures that are commensurate with the associated risks and potential impacts of data loss, misuse, or unauthorized access or modification. This includes ensuring that all systems and applications function securely and reliably, with appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, personnel, and technical controls.

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

Information is retrieved via an internal network, which requires secure authentication.

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

Personally identifiable information (PII) related to the spotter program is initially collected from volunteers through a Google Form, which includes a Privacy Act Statement. This information—such as name, location of the forecast area, email address, and phone number—is then manually entered by NWS personnel into the Integrated Real-time Impacts Services (IRIS) system, which is maintained outside of the NOAA8882 boundary. Spotter volunteers submit weather-related observations to NWS employees via phone or email; these observations are recorded in IRIS and attributed to the reporting individual. Locally, PII may also be stored on encrypted thumb drives. All information transmissions occur over authorized and secured NOAA networks.

(g) Any information sharing

PII is collected and stored for employees, as well as for spotter volunteers (members of the public). The PII/business identifiable information (BII) in this system is not shared except within the bureau, and in case of a security or privacy breach, with the Department or other Federal Agencies.

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

| Type of Information Collected | Applicable SORNs | Programmatic Authorities |
|--|------------------|--|
| Contact Information for the Public | NOAA-11 | 5 U.S.C. 301, Departmental Regulations |
| | | 15 U.S.C. 1512, Powers and duties of Department |
| | | |
| Info Collected Electronically in Connection w/ DOC Activities, Events & Programs | COMMERCE/DEPT-23 | 15 U.S.C. § 272 |
| | | 15 U.S.C. § 1151 |
| | | 15 U.S.C. § 1512 |
| | | 15 U.S.C. § 1516 |
| | | E.O. 11625 |
| | | |
| Managing Access Accounts and Login Names | COMMERCE/DEPT-25 | 5 USC 301 |
| | | Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors |
| | | Electronic Signatures in Global and National Commerce Act, Public Law 106-229 |
| | | 28 U.S.C. 533-535 |
| | | |
| Investigative and Security Records | COMMERCE/DEPT-13 | 5 U.S.C 301 |
| | | 5 U.S.C. 7531-332 |
| | | 28 U.S.C. 533-535 |
| | | Equal Employment Act of 1972 |
| | | |
| Personnel Information | COMMERCE/DEPT-18 | 44 U.S.C. 3101 |
| | | Executive Orders 12107, 13164, |
| | | 41 U.S.C. 433(d) |
| | | 5 U.S.C. 5379 |
| | | 5 CFR Part 537 |
| | | Executive Order 12564 |
| | | Public Law 100-71 |
| | | Executive Order 11246 |
| | | 26 U.S.C. 3402 |

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

This is a FIPS 199 moderate level 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): Sec. 2.1 WRD - Employment Performance Ratings or other Performance Information is selected to correspond to information identified in Sec. 5.1. Sec. 2.1 DFB Video Recording and Voice/Audio recording were added. Sec. 3.1 - Audio recordings was added. | | | | | |

☐ 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.

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. Sex | | k. Telephone Number | X | r. Criminal Record | |
| e. Age | | l. Email Address | X | s. Marital Status | |
| 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 | X | e. Work Email Address | X | i. Business Associates | |
| b. Job Title | X | f. Salary | X | j. Proprietary or Business Information | |
| c. Work Address | X | g. Work History | X | k. Procurement/contracting records | |
| d. Work Telephone Number | X | h. Employment Performance Ratings or other Performance Information | X | | |
| 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 | X | h. Eye Color | | m. DNA Sample or Profile | |
| d. Video Recording | X | 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 | | 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 | X | Email | X | | |
| Other (specify): | | | | | |

| Government Sources | | | | | |
|----------------------|---|-------------------|--|------------------------|--|
| Within the Bureau | X | 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.

| |
|---|
| NOAA8882 does not process personally identifiable information (PII); it only stores the information. All PII collected is provided directly by the individual through email, phone, Google Form, or in-person communication. The accuracy of the information is ensured by relying on the individual to validate the information at the time of submission. |
|---|

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| X | Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0648-0828. |
| | 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 (TUCBPNPD) | | | |
| 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 | X | 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 | X |
| 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 | X |
| 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).

NWS Eastern Region collects and maintains PII from NWS employees, contractors, and student volunteers. This information is collected in support of employment-related functions such as performance reviews, internal documentation, and administrative processes. While there is no centralized PII database, most information is maintained in paper format by NWS ERHQ administrative personnel. In some cases, this data may be digitized and uploaded to official enterprise systems such as the Office of Human Capital Services systems, the Office of Security, or other human resources (HR) platforms.

The types of employee information maintained may include:

- Full name
- Position title
- General Schedule (GS) level, series, and service computation date
- Date of grade and date of separation (if applicable)
- Residential contact information (address and phone numbers)
- Government-issued email address
- Division and organization name

- Regional office location
- Notes on current or relevant personnel issues (optional field)

This information serves as a supplement to other official employee records maintained by the agency elsewhere.

Additionally, WFOs and RFCs collect and maintain information on volunteer weather spotters, who are members of the public, providing real-time weather observations.

The data collected includes:

- First and last name
- Mailing address
- Phone number (home and/or cell)
- Email address

All volunteer-provided information is submitted voluntarily. Eastern Region staff are responsible for maintaining this data. It is accessible to NWS staff for operational use, including contacting spotters during severe weather events and entering observational data into appropriate systems.

- 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 of appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential privacy threats primarily stem from unintentional or unauthorized disclosures of information. To mitigate these risks, system security controls are implemented to restrict and monitor access based on operational necessity following the principle of least privilege. All users must complete annual mandatory security awareness and privacy training, which includes instruction on the proper handling and protection of sensitive information. Users must also acknowledge the Rules of Behavior, affirming their understanding of and responsibility for safeguarding privacy-related data.

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 | | | |
| Public | | | |
| Private sector | | | |
| Foreign governments | | | |
| Foreign entities | | | |
| Other (specify): | | | |

* PII is only shared with Law Enforcement if a security or privacy incident occurs.

| | |
|--------------------------|---|
| <input type="checkbox"/> | 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?

| | |
|--------------------------|---|
| <input type="checkbox"/> | Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII. |
| <input type="checkbox"/> | 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 | <p>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:</p> <p>NOAA0100 - NOAA Cyber Security Center NOAA8102 – Automated Surface Observation System NOAA8106 – Upper Air Observing System NOAA8107 – Advanced Weather Interactive Processing System NOAA8850 – Enterprise Mission Enabling System NOAA8860 – Weather and Climate Computing Infrastructure Services</p> <p>Mitigations include the use of system security controls, which limit access to the information and monitor access to the information system. Access to information is granted on a “need-to-know” basis and the principle of least privilege.</p> <p>Authentication is verified using Common Access Card (CAC) IDs and Personal Identity Verification (PIV) Cards. Only employees with the authority to maintain these databases are allowed access to the information.</p> |
| <input type="checkbox"/> | 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 | <input type="checkbox"/> | 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.weather.gov/privacy Citizen Science & Crowdsourcing Information Collections | |
| X | Yes, notice is provided by other means. | Specify how: For the workforce database, employees are notified at the time of recruitment that the collection of their information is mandatory as a condition of employment. For the Spotter Volunteers, notice is provided using a Privacy Act Statement, which is attached to the end of the Privacy Impact Assessment. |
| | 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: For the workforce database, individuals may inform HR staff, verbally or in writing, that they do not want their information added to the database; however, provision of the information is a condition of employment. All information is voluntary for Spotter Volunteers, as stated in the Privacy Act Statement, which is attached to the end of the Privacy Impact Assessment. |
| | 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: For the workforce database, employees may opt out of consenting to all uses (administrative, job vacancy tracking, |
|---|--|--|

| | | |
|--|--|---|
| | | and statistical reports) by informing HR staff verbally or in writing; however, they are required to provide the information as a condition of employment. The only use of the information for volunteers is for contact purposes, which is explained in the cooperative agreement. No other uses are suggested or specified. The provision of the information and the signing of the cooperative agreement imply consent to that use. |
| | 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: For the workforce data, information is routinely updated as an employee's role or position changes. Employees cannot directly review the information but may request to review their information and ask that it be updated, through their supervisors. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Management Division (AMD) Chief. The local manager who recruited the volunteer updates their information when notified by them to do so. Updates are not solicited but the instructions for submitting updates are in the cooperative agreement. |
| | 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. |
| | Access to the PII/BII is being monitored, tracked, or recorded. Explanation: |
| 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): <u>3/31/2025</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved. |
| X | The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. |

| | |
|---|--|
| X | NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 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).*

Access to systems containing PII is controlled through Active Directory and authenticated using CAC and PIV credentials. Access is limited to authorized personnel with a defined need to maintain or manage the data, in accordance with their official duties.

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. <i>(list all that apply):</i> COMMERCE/DEPT-13, Investigative and Security Records COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-23, Info Collected Electronically in Connection w/ DOC Activities, Events & Programs COMMERCE/DEPT-25, Access Control and Identity Management System 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 <u>(date)</u> . |
| | 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: Chapter 1300 – Weather, 1307-05, Chapter 300–Personnel |
| | 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 | X | Overwriting | X |
| Degaussing | | 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.)*

| | | |
|---|------------------------|---|
| X | Identifiability | Provide explanation: Name and contact information for volunteers, and names of employees are in the system. |
| X | Quantity of PII | Provide explanation: Limited amount of PII stored. |
| X | Data Field Sensitivity | Provide explanation: There are no sensitive data fields other than optional text field with current/relevant personnel issues (where completed). |

| | | |
|---|---------------------------------------|---|
| X | Context of Use | Provide explanation: The PII collected is stored for purposes of collecting weather observations. |
| | Obligation to Protect Confidentiality | Provide explanation: |
| X | Access to and Location of PII | Provide explanation: Secured database managed by federal employees with limited user privileges. |
| | 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.)

NOAA8882 adheres to the principle of data minimization, collecting only the information necessary to support its authorized functions. Volunteer data is provided voluntarily by individuals participating in the program, and workforce-related data is accessible only to individuals with appropriate authorization. To ensure ongoing protection of sensitive information, NOAA8882 participates in annual Assessment and Authorization (A&A) activities that assess, test, and validate the effectiveness of implemented security controls in mitigating the risk of unauthorized access or disclosure.

- 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. |

Privacy Act Statement (Spotter Volunteer)

Authority: The collection of this information is authorized under 5 U.S.C. 301 (*Departmental regulations*), 5 USC 552a (*Records maintained on individuals*), 15 U.S.C. 1512 (*Powers and duties of Department*), and 44 U.S.C. 2904 (General responsibilities for records management).

Purpose: NOAA collects this information for the purpose of 1) obtaining an agreement with a cooperative observer, storm warning displayman, flood warning distributor, spotter volunteer, etc., 2) with an individual, company, organization to provide observations to be taken by its personnel at one or more locations, 3) agreement to any material change in terms of agreement with cooperative personnel already rendering service to the Weather Service, such as adding river observations at a climatological station, etc., and/or agreement for installation of instrumental equipment when the property upon which it is proposed to install instrumental equipment is controlled by an individual or organization other than the individual or organization responsible for the personal service.

Information collected: May collect, but not limited to, first and last name, home address/city, home telephone number, email address, Spotter ID, radio call sign if applicable, county, elevation, latitude/longitude, what hours a spotter can be contacted for severe weather reports, possession of a rain gauge, anemometer, thermometer, snow stick, or weather station, and/or last time attended spotter class.

NOAA Routine Uses: NOAA will use this information to formalize user eligibility and contact the user regarding weather-related activities when needed. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among NOAA staff for work-related purposes. Disclosure of this information is also subject to the published routine uses identified in the Privacy Act System of Records Notice Commerce/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent the individual from completing the agreement and, thus, being available for contact when necessary for voluntary weather-related activities.