Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA8885

National Weather Service (NWS) Western Region General Support System

Reviewed by: Mark Graff Bureau Chief Privacy Officer

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2024.04.02 09:12:04 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/ National Weather Service (NWS) Western Region
General Support System

Unique Project Identifier: NOAA8885

Introduction: System Description

NOAA8885 data and products assist in the formation of a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community. NOAA8885 also provides administrative functions as well as scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

NOAA8885's data and products assist in developing a comprehensive informational architecture for national weather information, encompassing hydrologic, climate forecasts, observations, and warnings across the United States. This architecture enhances data accessibility for government agencies, private entities, the general public, and the global community. Additionally, NOAA8885 provides a range of administrative functions, including personnel onboarding, in/out processing, personnel management, budget oversight, financial operations, acquisitions, resource allocation, and strategic planning. It also offers scientific & technical research support for the NWS Western Region Headquarters (WRHQ) and all offices within the NWS Western Region (WR) boundary.

Address the following elements:

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

The NOAA8885 System is a General Support System (GSS) which is designed and used to collect, process, and disseminate supplemental weather data that supports warning and forecast products for the protection of life, property, and the enhancement of the national economy.

(b) System location

The NOAA8885 system is distributed over eight states and provides computing resources and networks for personnel at the following offices: NWS Western Region Headquarters (WRH) in Salt Lake City, UT; 24 Weather Forecast Offices (WFOs); four Central Weather Service Units (CWSUs); three River Forecast Centers (RFCs); and two Port Meteorological Offices (PMOs):

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

Although there are a variety of hardware and operating systems, several of the activities are interconnected. NOAA8885 provides direct and indirect mission support for the NWS as a Government agency. NOAA8885 primarily interconnects with federal and state governmental

agencies:

- NOAA8106 Upper Air Observing System (UAOS) - The UAOS provides the NWS with environmental sounding measurements from balloon borne radiosondes launched twice daily.
- NOAA8104 Weather Surveillance Radar 88D (WSR-88D) - Facilitates the transfer of WSR-88D data to the NWS Level II Collection and Dissemination System which is collected at Western Region Weather Forecast Offices (WFOs).
- NOAA8107 Advanced Weather Interactive Processing System (AWIPS) - AWIPS is an interactive system that integrates meteorological, hydrological, satellite, and radar data that enables the forecaster to prepare and issue forecasts and warnings.
- NOAA8860 Weather and Climate Computing Infrastructure Services (WCCIS) – This system provides Wide Area Network (WAN) services for interconnecting WRHQ, all WFOs, and RFCs.
- NOAA0100 NOAA Cyber Security Center (NCSC) - The NCSC is a functional body of technologies, processes, and practices designed to support the NCSC mission to protect NOAA networks, computers, programs, and data from cyber-attack, damage, and unauthorized access.
- NOAA0201 Web Operation Center (WOC) - The WOC provides a wide range of information technology services and functions. The core services are the WOC Domain Name System Services (WOCDNSS), WOC Information Sharing Services (WOCISS), WOC Adoptive System Framework (WOCASF), WOC NOAA Enterprise Message System (WOCNEMS) and WOC Collaboration Services (WOCCS).
- NOAA8850 Enterprise Mission Enabling System (EMES) - EMES operates a group of servers throughout the NWS that include Active Directory (AD) domain controllers, Enterprise Continuous Monitoring Operations (ECMO) relays, and McAfee ePolicy Orchestrator (McAfee ePO) servers.
- NOAA0550 NOAA Science Network (N-Wave) - N-Wave is a general-purpose shared network consisting of a private carrier class network backbone that supports the NOAA's scientific mission by providing high speed networking services to NOAA customer sites, programs, line offices, and research facilities.
- California Dept. Of Water Resources – This connection enables the collection, analysis and display of meteorological data collected throughout the Western United States.

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

NOAA8885 employs an information security architecture that promotes segmentation, redundancy, and the elimination of single points of failure to the fullest extent possible, which enables NOAA8885 to more effectively manage risk. In addition, NOAA8885 takes into consideration its mission/business programs and applications when considering new processes or services to help determine areas where shared resources can be leveraged or implemented. NOAA8885 strives to implement security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

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

Publicly available information is retrieved using standard techniques and protocols (i.e., https). Access to and retrieval of internal information is controlled by the use of account permissions, firewall access lists, and two-factor authentication. Access is based on "need to have" and the least privilege principle.

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

NOAA8885 implements managed interfaces for all devices through the uses of intelligent network devices that use access groups and access control lists which limit access to only the essential functions and services. As noted above, much of the information transmitted is public information and utilizes standard techniques and protocols. Information deemed not to be public (i.e., internal), is transmitted using the underlying operating system and device capabilities which afford a level of protection commensurate with the information sensitivity.

(g) Any information sharing

Collaborative information sharing of public information such as weather information, observations, hydrologic data, and other weather-related information occurs on a regular basis and is an essential element of the NWS mission. PII/BII information outlined in the PIA such as employee, contractor, or volunteer data is not shared with any third parties or unauthorized personnel. The information is not available to the general public, other NWS Regions, or other NOAA components. PII is shared with other Department of Commerce (DOC) bureaus or federal agencies only when necessary for official administrative purposes. This includes, but is not limited to, personnel actions such as employee transfers, terminations, retirements, and for fulfilling legal or regulatory obligations.

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

(i)

Type of Information Collected	Applicable SORNS	Programmatic Authorities
Personnel Actions Including Training	COMMERCE/DEPT-1	31 U.S.C. 66a
		44 U.S.C. 3101, 3309
		Title 5 U.S.C.
	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
Employee Performance Info	OPM/GOVT-2	Executive Order 12107
		5 U.S.C. Sections 1104, 3321, 4305, and 5405
Security Investigations (Security Clearance actions)	COMMERCE/DEPT-13	Executive Orders 10450, 11478
		5 U.S.C. 7531-332
		28 U.S.C. 533-535
		Equal Employment Act of 1972
Building Entry/Access & Surveillance	COMMERCE/DEPT-25	5 USC 301
		Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
System Administration/Audit Data (SAAD)	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
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
Contract / Grant Information	COMMERCE/DEPT-2	28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365)
		26 U.S.C. 6402(d)
		31 U.S.C. 3711
Contact Information for the Public	NOAA-11	5 U.S.C. 301, Departmental Regulations
		15 U.S.C. 1512, Powers and duties of Department

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

NOAA8885 has been categorized as a moderate impact system in accordance with the Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

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.

__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.

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. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	

g. Citizenship		n. Religion			
u. Other general personal data (specify)): For volunteers: County, spotter ID, elevation, the hours they can be contacted for severe weather reports, whether they have a rain gauge, anemometer, thermometer, snow stick, or weather station, radio call sign, twitter account, Facebook account, last time attended spotter class, and their latitude/longitude.					

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

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	X	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		Online	X
Telephone	X	Email			
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.

Information accuracy is ensured by utilizing proper handling techniques and storage methods as well as employing access control mechanisms that restrict access to only approved individuals. Access controls enable data consistency, accuracy, and trustworthiness. In person and telephone information is obtained directly from the person the information pertains to and is provided voluntarily. There is no validation process at the point of information collection, as the data is provided on a volunteer basis and isn't immediately critical to our operations. Inaccuracies, such as incorrect contact information, typically come to light during subsequent communication attempts. In such cases, there would be no further contact with the individual. Given the non-critical nature of this information, this approach has been sufficient for our needs. Government specific information such as personnel data (name, position, GS Level, division/organization, office location) is obtained from authoritative sources including the NOAA staff directory, HR connect, and the Management Analysis & Reporting System (MARS) which are recognized for their reliability and accuracy. The individual has the opportunity to request the information to be updated through their supervisor.

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. The observer agreements are currently awaiting OMB approval. Once clearance is granted, the OMB Control Number will be provided.
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	X	Building entry readers	
Video surveillance	X	Electronic purchase transactions	
Other (specify): Video recordings			
	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	X
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)		For web measurement and customization technologies (multi-session)	
Other (specify): Information on volunteers is utilized to determine suitability for the SKYWARN Storm Spotter program and to provide reports pertaining to local weather conditions. NOAA8885 may record video images and audio of Federal employees while conducting virtual meetings or training sessions in order to disseminate the information to individuals who were not able to attend the live meeting and to use as a future training vehicle.			

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).

There are local databases at the local Weather Forecast Office (WFO) and the River Forecast Center (RFC) that maintain information on volunteers who provide weather reports to staff. The WFO/RFC database information is collected to contact volunteers when severe weather information is needed. The database holds the following information on these volunteers:

- First and last name
- Mailing address
- County
- Phone (home/cell)
- Spotter ID
- Elevation
- Email address
- The hours they can be contacted for severe weather reports
- Whether they have a rain gauge, anemometer, thermometer, snow stick, or weather station
- Radio Call sign
- Twitter account
- Facebook account
- Last time attended spotter class
- Latitude / Longitude

Information in this database is provided on a voluntary basis; volunteers sign up and provide the information during spotter talks the NWS provides in preparation for the severe weather season. Volunteers have the opportunity to decline providing their information, if they do not want to participate in the future. This database information is accessible to forecast staff so they can contact volunteers for severe weather information.

Forecast products are made available online to improve federal services.

Administrative matters and human resources programs supported by the system include personnel management, budget oversight, financial operations, acquisitions, resource allocation, and strategic planning. This data collection enables the effective and efficient management of human resources, financial planning, and strategic decision-making processes, ensuring that the organization operates smoothly and complies with relevant regulations and policies.

NWS Western Region may record virtual meetings and training sessions for Federal employees that could capture an individual's image or voice. Typically, virtually recorded meetings will not have a need to record the attendees' images or audio and will use best practices such as presenter mode, phone only meetings or call in numbers, blurred backgrounds, etc., to limit the inadvertent capture of an individual's image or audio. However, in some cases attendees' images and audio may be recorded or captured both intentionally or unintentionally. The recordings are used to disseminate information and training to employees at a later date. Prior to the start of a recorded virtual meeting and training session, meeting participants are provided with a Privacy Act Statement and must consent to the potential recording of their image and/or audio. If consent is not given, the employee can decline to participate or turn off their webcam. If an employee's image or background images are inadvertently captured and the employee requests that this image be deleted, the recording will be edited to remove the unwanted material. If the recording cannot be sufficiently edited, the recording will be destroyed.

Video surveillance at facility points of ingress and egress to ensure safety and security, with audio capture being unlikely, but a potential component.

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.)

Potential threats to privacy information are primarily insider threat, the inadvertent disclosure of the information due to unauthorized access to the system, or unintentional disclosure. Mitigations include the use of system security controls (i.e., Access Control, Identification and Authentication, and Audit and Accountability) which limits access to the information as well as monitors the access to the information system. Access to information is granted on a "need to have" basis and the least privilege principle. Users undergo annual mandatory security awareness and privacy training with includes the proper handling of information. Users acknowledge the rules of behavior to ensure they understand their responsibilities.

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			
DOC bureaus	X		
Federal agencies	X		
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: NOAA8106 Upper Air Observing System NOAA8104 Weather Surveillance Radar 88D (WSR-88D NOAA8107 Advanced Weather Interactive Processing System (AWIPS) NOAA8860 Weather and Climate Computing Infrastructure Services (WCCIS) NOAA0100 NOAA Cyber Security NOAA0201 Web Operation Center (WOC) NOAA8850 Enterprise Mission Enabling System (EMES) NOAA0550 NOAA Science California Dept. Of Water NOAA8885 does not share PII/BII with interconnected systems. However, NOAA8885 prevents data leakage by using strict access controls including account permissions firewall access lists, two factor authentication. Only authorized individuals have access to data. In addition, managed interfaces are in use that utilize access groups and access control lists which limit access to only the essential functions and services as well as provide boundary protection. NOAA8885 employs an information security architecture that is segmented, monitored, assessed for vulnerabilities, is current (i.e., patched), and inventoried.
	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			
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 .	
X	Yes, notice is provided by other means.	Specify how: For the volunteer database, information is provided on a voluntary basis and users are notified by a statement on the volunteer and emergency planning forms. For virtually recorded meetings and training, employees are provided a Privacy Act Statement and must consent to the use of their image or voice.

		Individuals are notified of video surveillance via posted signs on the grounds in addition to signage at points of ingress/egress that video recording is occurring.
	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 volunteer database, the information is provided on a purely volunteer basis and users are not required to provide information. For virtually recorded meetings and training, employees can decline to participate or request to have their image removed from the recording if it is inadvertently captured. If the recording cannot be sufficiently edited, the recording will be destroyed. Individuals have the opportunity to decline to provide PII via video surveillance by not entering areas where signage is posted and video imagery is captured.
	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 volunteer data, the information is provided on a purely volunteer basis and users provide the information to participate in the program which constitutes consent to use the information for the stated purpose. See the "Consent to Voluntary Information Collection and Sharing" section within NOAA Web site privacy policy. For virtually recorded meetings and training, employees are provided a Privacy Act Statement, which explains the particular use of the PII. Employees may decline a particular use by not using their webcam or by phoning into a meeting that may be recorded. Signage is posted at all points of ingress/egress at the facilities where imagery is captured. Individuals are informed that the purpose is for facility safety and security. Individuals consent to this use by continuing to access these locations.
	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 volunteer data, users may request their data from, and send updates, if needed, to their local station manager. For virtually recorded meetings and training, participants have access to the recording and can review the contents at any time and request that their image be removed.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: There is no opportunity for individuals to update the video images recorded for safety & security purposes.

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:** Standard system audit logs.
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): 8/31/2023 ☐ 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.
N/A	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 data is controlled by the use of account permissions, firewall access lists, and two-factor authentication. Active Directory group memberships and assigned permissions are employed to manage control of the access to folders, files and shares. Access is based on a "need to have" and the least privilege principle. Only authorized individuals have access to information.

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. COMMERCE/DEPT-1 - Attendance, Leave, and Payroll Records of Employees and Certain Other Persons. COMMERCE/DEPT-2 - Accounts Receivable COMMERCE/DEPT-13, Investigative and Security Records COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-25, Access Control and Identity Management System OPM/GOVT-2 - Employee Performance File System Records
	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: Chapter 1300 National Weather Service Records Disposition Schedule NOAA Records Schedule 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: Although name, general location, and phone number can be used to identify individuals, this information is available via other sources. There would be low impact to the individual if information was released.
X	Quantity of PII	Provide explanation: A moderate amount of PII is collected (name, phone, number, location); however, the data is not in a sensitive context.
X	Data Field Sensitivity	Provide explanation: Data fields contain items such as name and phone, however there is not a sensitive context related to the data (e.g., not health information).
X	Context of Use	Provide explanation: Based on the use of the information outlined in section 5.1, the impact would be low if information was accessed.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access is limited to internal authorized federal employees. Access restrictions are in place as outlined in PIA Section 8 as well as the NOAA8885 System Security Plan (SSP).
	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.)

NOAA8885 collects only the minimum required information necessary for the purpose in which it is intended. Volunteer data is provided on a voluntary basis by users who wish to participate in the program. Recorded meetings and training sessions are reviewed prior to being released to ensure that the recording is suitable to be provided to individuals that have a need for the information. NOAA8885 undergoes annual Assessment and Authorization (A&A) activities that evaluate, test, and examine security controls to help ensure they are implemented in a way to adequately mitigate risk to the unauthorized information 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.

NWS Reno SKYWARN™ Spotter Program

All of your answers will be kept strictly confidential. By answering this form, you are agreeing to volunteer for the SKYWARN™ Spotter Network and help report significant weather conditions in your area. If you have any questions, please contact Amanda Young (Amanda.Young@noaa.gov) or call our office at: (775) 673-8100.

* Indicates required question

Name (First and Last) *

If applicable, please provide agency name and a contact person

Your answer

Mailing address? *

Your answer

Physical Address? If different from above. *

Your answer

Telephone Number? *

Home, Work, and/or Cell. Please only provide those numbers we can contact you on.

Your answer

Are you willing to call us when you observe significant weather as defined by your spotter training? *

We are here 24/7/365 and will provide you a toll free number to call in reports.

Your answer

Can the NWS call you if we suspect hazardous weather in your area? *

Your answer

If the answer to the above question is "yes", what times of the day may we call you? *

If these hours differ between your home, cell, and work numbers, please specify each.

Your answer

County of Residence? *

If in a rural location, please provide the distance and direction of nearest town (i.e. 3W of town)

Your answer

Your elevation?

If known

Your answer

Your latitude and longitude?

If known. If not, we can look it up using your physical address.

Your answer

Do you live or work near a river, creek, or other body of water? *

If so, which one, and the distance and direction from your home or office.

Your answer

What is your email address? (We promise no spam!) *

Your answer

Are you an amateur radio operator? If so, what is your sign? *

Your answer

Do you own any weather observing equipment? If so, please specify. *

thermometer, rain gauge, anemometer, etc

Your answer

Thank you for you interest in the SKYWARN™ Program! We will be in contact with you shortly!

Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

Purpose: NOAA collects this information for the purpose of: 1) obtaining an agreement with a cooperative observer, storm warning displayman, flood warning distributor. etc., 2) with a company or 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: Name, home address, 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, twitter account/Facebook or any other social media account information, last time attended spotter class.

NOAA Routine Uses: NOAA will use this information to formalize user eligibility and to contact the user when needed regarding weather–related activities. 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 all of the published routine uses as 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 from being available for contact when needed for voluntary weather–related activities.