

**U.S. Department of Commerce
National Oceanic and Atmospheric Administration**



**Privacy Impact Assessment
for the
NOAA8884
Southern Region (SR) General Support System (GSS)**

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

CHARLES CUTSHALL

Digitally signed by CHARLES CUTSHALL
Date: 2024.03.04 18:43:30 -05'00'

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

Date

**U.S. Department of Commerce Privacy Impact Assessment
National Weather Service (NWS) Southern Region (SR) General Support System (GSS)**

Unique Project Identifier: NOAA8884

Introduction: System Description

Provide a brief description of the information system.

General Support System

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. This system is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions and the scientific & technical research and innovations activities of employees within the organization.

Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Local Area Networks (LAN), host computer systems; client-server and non-public facing web-based server systems. The system supports a variety of users, functions, and applications; including word processing, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development and collaboration.

Address the following elements:

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

This is a General Support System (GSS).

(b) System location

System headquarters is located in Fort Worth TX, but the WAN extends across 11 states which support 1 Regional Headquarters, 32 Weather Forecast Offices (WFO), 4 River Forecast Centers (RFC), and 7 Center Weather Service Units (CWSU).

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

The SR GSS is a system with interconnections only to trusted NWS-NOAA internal systems with no direct interconnections to the outside. Although there are a variety of hardware and operating systems, all the operational activities are interconnected. The system provides direct or indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, and client-server systems. The system supports a variety of users, functions, and applications, including word processing, employee data, financial data, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training, research and development, and collaboration.

The following systems interconnect internally with NOAA8884:

NOAA0201 - Web Operation Center (H)
 NOAA0900 – Cloud Computing Services
 NOAA1101 - Information Technology Center (M)
 NOAA8106 - Upper Air Observing System (UAOS)
 NOAA8107 - Advanced Weather Interactive Processing System (AWIPS)
 NOAA8850 - NWS Enterprise Mission Enabling System (MES)
 NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS),
 OneNWSNet

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

The National Weather Service (NWS) Southern Region provides weather, hydrologic, and climate forecasts and warnings for the United States, its territories, adjacent waters and ocean areas, for the protection of life and property and the enhancement of the national economy. NWS data and products form a national information database and infrastructure, which can be used by our partners, the public, and the global community. Issuance of products including forecasts and warning is dependent on a complex interaction of many information resources and systems. The NOAA8884 General Support System (GSS) is designed and used to support the collection, processing, and dissemination of data that supports the mission of the organization. It also supports the administrative functions alongside the scientific and technical research and innovation activities of employees within the organization.

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

MARS Data:

Authorized NOAA8884 users can log into the Management Analysis and reporting System (MARS) via interconnection with NOAA1101. The Southern Region (SR) database administrator downloads MARS data from the NOAA1101 portal and populates a SQL Server database. Access to the database is restricted to database administrators only.

Select authorized SR users (the System Owner and Financial Officer) can request data to generate reports from the secure web portal. Access to the portal is password protected and

controlled through access control lists managed by the database administrator; access to specific data fields is restricted in the same manner. Users generate reports to conduct past, present, and future financial costs analyses which are returned in .xlsx format. These reports are for internal use and are not shared or transmitted external to SR.

Volunteer Observer Data:

Volunteer personal data is collected using the WS Form B-30 in person, and securely stored by the Observer Program Lead at each WFO at each of the 32 Weather Forecast Offices on workstation hard drives or centralized network attached storage devices. The data collected is name, address, phone number, and email address. The data is not transmitted or released, it is used to contact volunteers as needed.

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

All data is transmitted and received via NWSOneNet cloud. All internal NWS data is on the Multiprotocol Label Switching (MPLS) cloud network and all Internet connectivity is supplied through the NOAA Trusted Internet Connection (TIC) sites.

MARS Data:

NOAA8884 Authorized users generate queries on the SQL Server Web Portal by selecting data elements desired for the reports; SQL generates the results which are downloaded by the users to their computers via secure data transfer using Hypertext Transfer Protocol Secure (https, port 443).

Volunteer Observer Data:

Observed Weather data from volunteers is transmitted to the Weather Service through one of two NOAA funded systems:

- Phone updates through the Interactive Voice Remote Observation Collection System (IV-ROCS) for voice calls, approximately 10% of the reporting.
- Online input to the Weather Coder Web Server, which is hosted by the Western Region Climate Center (WRCC), approximately 90% of the reporting.

(g) Any information sharing

MARS Data:

Management Analysis and Reporting System (MARS) is a NOAA enterprise system within the NOAA1101 GSS accreditation boundary that provides a common source for business information and financial transactions for all NOAA line offices. NOAA8884 extracts non-sensitive employee, business, and financial data and stores it on encrypted centralized servers, authorized employee workstations, and in authorized Google Workspace cloud environments. The data is then used by authorized agency employees, and contractors within the NOAA organization in the performance of their official duties.

Volunteer Observer Data:

There is no information sharing within or outside of the system.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting,

maintaining, using, and disseminating the information

Type of Information Collected (Introduction h.)	Applicable SORNs (Section 9.2)	Programmatic Authorities (Introduction h.)
1. Contact Information for the Public	NOAA-11	5 U.S.C. 301, Departmental Regulations
		15 U.S.C. 1512, Powers and duties of Department
2. Personnel Actions Including Training	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
	OPM/GOVT-1	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 5379, 8347
		Executive Orders 9397 , as amended by 13478 , 9830 , and 12107
3. System Administration/Audit Data (SAAD)	COMMERCE/DEPT-25	5 U.S.C. 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

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

NOAA8884 is a Moderate categorized 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
<p>j. Other changes that create new privacy risks (specify): During the March 8, 2023 online meeting between NOAA Privacy Office and NOAA8884 (attendees listed below), the result of a discussion of the NOAA8884 use and handling of MARS data (detailed in sections (e), (f), and (g) above) was the direction of the NOAA Privacy Officer to raise the level from Low to Moderate. Attendees: Mark Graff, NOAA Privacy Officer Robin Burress, NOAA Privacy Act Officer Adrienne Thomas, NOAA OFA John Duxbury, NOAA8884 System Owner Jeff Williams NOAA8884 Systems Integration Branch Chief Chuck Burrows, NOAA Information Systems Security Officer</p> <p>NOAA8860 interconnection has been added since the last SAOP approved document. This connection was documented in previous versions of the NOAA8884 PIA; as it is a change from the most recently approved PIA, it is included as a new risk.</p>				

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	X	i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify): Volunteer Observer Data: Volunteer data consists of Name, Address, Phone number and email address. No additional PII is collected.					
*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): Volunteer Observer Data.					

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	X
c. Work Address	X	g. Work History		k. Procurement/contracting records	X
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	X
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	
Telephone		Email			
Other (specify): Volunteer Observer data collected in person.					

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.

<p>MARS Data: There is no data change or modification when data is downloaded from the MARS system. Only the database administrators have access to the SQL database. Selected users authorized to request data in the form of generated reports have read-only privilege.</p> <p>Volunteer Observer Data: All of this PII information is directly received from the user when accounts are created. It is manually input into the local office database and only the OPL (Observation Program Leader) has access to make changes to the data, either to update any contact information that may have changed (i.e., A new phone number) and to remove the data either when the volunteer requests it or discontinues participation in the Observer Program.</p>
--

2.4 Is the information covered by the Paperwork Reduction Act?

<p>Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.</p>

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	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)	X	For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

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

Volunteer Observer Data: NOAA8884 collects, stores, and uses volunteer observer general personal data who provide daily climate and weather reports. The data resides within each of the 32 Weather Forecast Offices on workstation hard drives or centralized network attached storage devices. The contact information is used by NWS staff members responsible for providing meteorological, hydrological, and climatological data collection oversight as part of their official duties.

Volunteer observer PII data collected and stored within the NOAA8884 accreditation boundary is limited to general personal data including name, home address, email address, and telephone number. A limited amount of contact information is retained in the local office for quick access to contact the volunteer observer in case of equipment outages.

The volunteer observer has the right to opt-out of the program at any time. Once collected the information is stored on workstation or network attached storage device and also entered into a NOAA database called the Station Information System (SIS) located and maintained by NWS Office of Observations. Once the volunteer opts out of the program the PII is purged from the system.

Volunteer Observer Data is not shared outside the National Weather Service.

MARS Data: This data is used by authorized agency employees, and contractors within NOAA8884's accreditation boundary in the performance of their official duties. Uses include decisions related to agency staffing, budgeting, acquisitions, finance, and mission delivery.

Employee data consists of the name of the employee, the email address of the employee, CBS employee number, job title, employee grade, step, series, org code, project-task, employee salary, employee benefits, FLSA code, and BUS code.

NOAA8884 uses MARS employee data in conjunction with directly related financial data to formulate and track labor costs by portfolio, project code, program code, assigned org code and physical location for the purposes of Financial Management Center (FMC) budget planning, oversight, forecasting, and execution. The FMC uses all specific data to accurately manage budget allocations, status, analyze variances and historical spending trends to support the formulation of future resource needs. Data is used to calculate, analyze, and track FTE, benefits, premium pay shift differential, overtime, locality pay, cost of living allowances, special IT pay, awards, and annual pay raises in a complex budget accounting environment that requires daily detailed analysis. Information is shared with managers and supervisors responsible and accountable for programmatic oversight of costing and controls. All associated accounting is categorized in accordance with the Accounting Classification Code Structure (ACCS), cost category, funding source, and in

accordance with NWS' Appropriations Reference Manual.

NOAA8884 extracts non-sensitive employee, business, and financial data directly from MARS and stores it in a restricted access database on encrypted centralized servers, select employee workstations, and in authorized Google Workspace cloud environments. MARS PII data downloaded to the SR SQL Server database consists only of employees' name, email, and employee number. Derivatives of data originating from the MARS system are received from agency officials outside our accreditation boundary using a variety of communication technologies (i.e., attachments to Email, DOC secure file sharing sites, Google cloud file sharing technologies, etc.) and in a variety of electronic formats and is stored on both centralized servers, employee workstations, and in authorized Google Workspace cloud environments.

MARS data is not shared outside the DOC, including externally to any National Weather Service Southern Region office or entity.

- 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.)

An insider threat is a malicious threat to an organization that comes from people within the organization. DOC and NOAA have put in place mandatory training for all its uses. The Security Awareness and Privacy training is an annual requirement, intended to reduce the risk and minimize the impact of an authorized user intentionally or unintentionally disclosing data, and causing adverse impact to sensitive data and the NOAA mission.

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			
State, local, tribal gov't agencies			

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

<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.
<input checked="" type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.</p> <p>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:</p> <p>NOAA0201 - Web Operation Center NOAA0900 - Cloud Services NOAA1101 - Information Technology Center NOAA8106 - Upper Air Observing System (UAOS) NOAA8107 - Advanced Weather Interactive Processing System NOAA8850 - NWS Enterprise Mission Enabling System NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS), OneNWSNet</p> <p>Employee and financial data are extracted from NOAA1101 system by authorized users within NOAA8884 using standardized user interface tools every two (2) weeks corresponding with Federal pay schedules, or more frequently as needed by management. The reports are then saved as an .XLS file that is ingested to the SR SQL server, resides on the server for four (4) years. SQL server data at rest is encrypted, and only accessible to authorized users using CAC authentication. Once into the SR System, the users access the secure portal to retrieve their relevant data in HTML format.</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		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	
X	Yes, notice is provided by other means.	Specify how: For Volunteer Observer Data : Notice to volunteers is provided when information is collected, via the WS Form B-30, Cooperative Agreement With Observer. For MARS Data : Notice to employees is provided when the information is collected. All personnel forms contain the appropriate Privacy Act Statement.
	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 Volunteer Observer Data : All of this information is voluntary, as part of the cooperative agreement to work with the NWS on providing
---	---	---

		<p>observations. The only means of providing the PII is by completing and signing the cooperative agreement form. Declining to sign the agreement will void the observer duties with NWS.</p> <p>For MARS Data: Employees may decline to provide PII during onboarding and during employment; however, failure to provide the requested PII may impact their eligibility for employment or for continuation of employment.</p>
	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.	<p>Specify how:</p> <p>For Volunteer Observer Data: The volunteer observer information is for contact purposes only which is given as part of the signed agreement. No other uses are suggested or specified. The volunteer has an opportunity to consent or question the form's contents prior to signing with the local forecast office POC.</p> <p>For MARS Data: The personnel forms used for collection of PII provide employees the opportunity to consent for the specific uses of their personal information, and this data is used for human resources purposes only. Employees may decline to provide PII during onboarding and during employment; however, failure to provide the requested PII may impact their eligibility for employment or for continuation of employment.</p>
	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.	<p>Specify how:</p> <p>For Volunteer Observer Data: The local manager visits each volunteer twice monthly to monitor equipment and answer questions. Updates can be made then, or emailed, as</p>
---	---	--

		<p>explained by the manager during orientation. Pursuant to 5 USC 552a(d)(1), volunteers may review and update their record or information pertaining to them in the system upon request.</p> <p>For MARS Data: Employees may review their personnel information via an electronic personnel folder. Information can be updated in a separate web-based application and the user can provide updated contact information to his/her supervisor.</p>
	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	<p>Access to the PII/BII is being monitored, tracked, or recorded.</p> <p>Explanation: System logging is enabled and all access is tracked.</p>
X	<p>The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.</p> <p>Provide date of most recent Assessment and Authorization (A&A): <u>March 6, 2023 (ATO)</u></p> <p><input type="checkbox"/> This is a new system.</p>
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).*

Volunteer Observer Data: Access to the system maintaining the PII is controlled by access via Active Directory and the use of CAC (PIV) cards. Only employees with authority to maintain this database are allowed access to the information.

MARS Data: Connections to the MARS server and to the local database are made via https (port 443) using Transport Layer Security (TLS) encryption. Database server has data at rest encryption, and the server is physically located in an access-controlled server room facility in a federal building.

Section 9: Privacy Act

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

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	<p>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></p> <p>NOAA-11, Contact information for members of the public requesting or providing information related to NOAA’s mission; COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies; COMMERCE/DEPT-25, Access Control and Identity Management OPM GOVT-1: General Personal Records</p>
	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	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p> <ul style="list-style-type: none"> • NOAA Records Schedule, Chapter 1300, Weather, 1307-05, Service Locations Data Networks • NOAA Records Schedule, Chapter: 900, 904-01, Building Identification Credential Files • NOAA Records Schedule, Chapter 100, Enterprise-Wide Functions Electronic Records schedule
---	--

	<ul style="list-style-type: none"> • NOAA Records Schedule, Chapter 402, Employee Compensation and Benefits Records • NOAA Records Schedule, Chapter 403, Financial Management and Reporting Records • NARA General Records Schedule- 3.1, General Technology Management Records • NARA General Records Schedule- 3.2, Information Systems Security Records
	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): * Over write is done using the NIST compliant Dell BIOS Wipe Utility.			

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.*)

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	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.

Confidentiality Impact Level has been raised from Low to Moderate because of the MARS data in the system.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. (Check all that apply.)

X	Identifiability	Provide explanation: An employee, contractor, or volunteer can be identified by their name or contact information, such as address or phone number.
X	Quantity of PII	Provide explanation: PII is limited to general personal data or work-related data for less than 500 individuals.

X	Data Field Sensitivity	Provide explanation: No sensitive data is captured.
X	Context of Use	Provide explanation: Volunteer Observer PII is used to contact volunteers and visit their site to monitor equipment. MARS data is used for administrative and budgetary purposes.
X	Obligation to Protect Confidentiality	Provide explanation: Any PII collected will be protected consistent with Privacy Act guidelines.
X	Access to and Location of PII	Provide explanation: Secured local database managed by limited Federal employees.
	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.)

<p>Only the information that is required for the given financial reports is selected and downloaded from the MARS database. By selecting only certain fields and not the entire report we can ensure that sensitive or private information is not included with the broader reports. Reports are also broken down by individual office ORG codes so only data for that particular office is included in the reports. This ensures that only data needed by that office is available for that office to view.</p>
--

- 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.

COOPERATIVE AGREEMENT WITH OBSERVER

Station _____ County _____ State _____

Effective date of agreement _____

I agree to give reasonable care and protection to the instruments furnished by the National Weather Service, and to furnish free of charge observations and/or services listed below and suitable space for installation and exposure of instruments, until this agreement is terminated by notice by either party to the other. During the term of this agreement, I will permit National Weather Service officials and/or alternate observers free ingress and egress to the equipment for purposes of taking observations, inspections, or maintenance but assume no liability for injuries which might occur to such persons while on the premise.

(signature of cooperative observer)

Mr.. Mrs., Ms., Miss _____
(type one given name, initial or initials, and surname of observer, or name of organization)

Equipment is located at _____
(street address, building name, room number, highway number, etc.)

Observations and/or services to be provided _____

Equipment provided _____

Remarks _____

Approved _____ Title _____ Date _____

Original to RCMP, Copies to Cooperative Program Manager and Observer.

(Follow instructions on other side)

ACTIONS REQUIRING THE USE OF WS FORM B-30

1. The original agreement with a cooperative observer, storm warning displayman, flood warning distributor. etc.
2. The original agreement with a company of organization to provide observations to be taken by its personnel at one or more locations.
3. 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.
4. Space 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.

INSTRUCTIONS FOR PREPARATION OF THE FORM

Sufficient copies should be prepared to provide one for the observer, the RCMP, the direct supervising office (if other than RCMP), and the Cooperative Program Manager. The forms may be prepared by any Weather Service employee who is authorized to recruit cooperative station personnel, but must be approved by a person authorized to approve appointments as outlined in Weather Service Operations Manual Chapter B-17.

The agreement, in order to be effective, must indicate what personal services and what space or facilities, if any, the observer will furnish. It should be stated in general terms, however, so as to avoid the necessity of preparing new forms frequently because of insignificant changes in procedure or reporting instructions. One or more of the items listed below will cover the activities at most stations, but others might be included also. For example, "Communications facilities for transmission of reports" might be furnished by an airline operating company or a Government agency.

- Suitable space for exposure of instruments.
- Weather (or river) observations and reports.
- Distribution of flood warnings.
- Display and/or distribution of storm warnings.
- Weather reports to local newspaper (or radio station).
- Distribution of weather (or river) reports and/or forecasts.

At a second order station or a cooperative station where an airline company or other organization agrees to provide personnel for observational duties on company time, the Weather Service's agreement is, in effect, with the organization and not with the individual. Therefore, one agreement should be executed with a responsible officer of the organization, covering all services to be rendered for the Weather Service at that second order station or cooperative station. The same procedure should be followed where a Government agency agrees to render a cooperative service, except in the case of Federal Aviation Agency personnel where this form is not required.

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.