Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

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

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.06.30 17:42:48 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
National Weather Service (NWS) Western Region General Support System (GSS) (NOAA8885)

Unique Project Identifier: 006-48-02-00-01-0511-00

Introduction: System Description

The NOAA8885 System 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. 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.

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. The mission support infrastructure encompasses Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems; client-server and web-based server systems. The system also supports a variety of users, functions, and applications.

The NWS Western Region Headquarters Workforce Database, located in Salt Lake City, Utah, consists of basic identifying information about employees and contractors. The database is maintained as a supplement to other employee records and is used by Western Region Headquarters Administration staff to aid in tracking job vacancies, developing statistical reports, and performing other related administrative tasks. There are also local databases at the WFO/RFC that maintain information on volunteers who provide weather reports to NWS staff.

Information Sharing: Employee/contractor information 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. General information is only available to members of the NWS Western Region. Specific information about individual personnel is only available to authorized NWS Western Region Headquarters Administration Staff. Volunteer database information is accessible to forecast staff so they can contact volunteers for severe weather information.

The statutory authorities covering the collection of this data are 5 U.S.C 301, Departmental Regulations and 15 USC 1512 - Sec. 1512, Powers and Duties of Department [of Commerce]. In addition: 44 U.S.C. 3101; 5 U.S.C. 4101 et seq., 5 U.SC. 1302, 3302, E.O. 10577, 3 CFR 1954-1958 Comp. p. 218, E.O. 12107, 3 CFR 1978 Comp. p264; and Federal Personnel Manual and related directives for NOAA and the Department of Commerce.

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):					

__X__ This is an existing information system in which changes do not create new privacy risks.

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*		e. File/Case ID		i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify): Spotter ID , radio call sign if applicable (volunteers)					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): For volunteers: County, elevation, latitude/longitude, what hours can be contacted for severe weather reports, possession of a rain gauge, anemometer, thermometer, snow stick, or weather station , twitter account/facebook account information, last time attended spotter class.					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates			
Other work-related data (specify): GS level series, position, division/organization name, regional office location, optional text field with current/relevant personnel issues.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. 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	
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 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			
To determine eligibility		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	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Information on volunteers that is utilized to determine suitability for the program and to provide reports pertaining to local weather conditions.			

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).

The NWS Western Region Headquarters Workforce Database maintains information concerning federal employees and contractors in the Western Region workforce. This information is managed by the NWS Western Region Headquarters Administration Personnel.
The information maintained includes:

- Name
- Position
- GS Level/Series
- Division/Organization Name
- Regional Office Location
- Optional text field with current/relevant personnel issues.

This information is maintained to aid in tracking job vacancies, maintenance of organization structures, and other administrative related activities. The information is used by Western Region Headquarters Administration staff to supplement managing employee records, providing statistical data, etc. The information 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. General information is only available to members of the NWS Western Region. Specific information about individual personnel is only available to authorized NWS Western Region Headquarters Administration Staff.

There are also local databases at the local WFO/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
- What hours they can be contacted for severe weather reports
- Do 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.

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 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	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:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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 updated Volunteer Privacy Act statement, and privacy policy, can be found at: http://www.nws.noaa.gov/om/coop/index.htm.	
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 the workforce database, individuals are notified at the time of employment that the collection of this information is mandatory as a condition of employment.
	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 the workforce database, individuals (federal employees) may decline, in writing to their supervisor, not to have their information added to the database with the understanding that it may affect their employment.
	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. The NOAA Web site privacy policy states "Submitting voluntary information constitutes your consent to the use of the information for the stated purpose." For the workforce data, employees and contractors are required to provide the information as a condition of employment, but may consent to only particular uses, in writing, to their supervisors, with the understanding that it may affect their employment.
	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 the workforce data, information is routinely updated as an employee's role or position changes. Employees cannot review the information, but may request their information, and ask that it be updated, through their supervisor. 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.

	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Standard system audit logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): ___8/30/2016_____ ☐ 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 and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
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 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.

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" basis and the least privilege principle. Only authorized individuals have access to information.

Section 9: Privacy Act

9.1 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 and number *(list all that apply)*: NOAA–11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, a SORN is not being created.

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 Control Schedule Chapter 300
	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 Levels

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.

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 levels. *(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, GS Level, 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 section 8 as well as the NOAA8885 System Security Plan (SSP).
	Other:	Provide explanation:

Section 12: Analysis

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Addition of volunteer data elements to PAS and NOAA-11 SORN.
	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes.