

U.S. Department of Commerce National Weather Service



Privacy Impact Assessment for the Eastern Region NOAA8882

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

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

08/31/2019

Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: 006-000351104 00-48-02-00-02-00

Introduction: System Description

National Weather Service's Eastern Region is a General Support System, comprised by Eastern Region HQ located in Bohemia, NY and 23 additional offices across the region. The primary database servers are located at the Eastern Region HQ, in Bohemia, NY.

NWS Eastern Region (ER) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees and volunteers who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports and performing other related administrative tasks. In addition, Weather Forecast Office (WFO)/River Forecast Centers (RFC) maintain local databases that contain information on volunteers who provide weather reports to them.

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 Wide Area Networks (WAN), Local Area Networks (LAN), host computer systems, client-server and web-based server systems. The system supports a variety of users, functions, and applications, including word processing, budget and requisition information, spreadsheets, presentation graphics, database development and management, electronic mail, image processing, electronic commerce, project management, training (see above, no PII involved), research and development, and collaboration.

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

The legal authorities for information collection addressed in this PIA are:

- 5 U.S.C. § 301 authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.
- 44 U.S.C. 3101 addresses records management by Department agency heads.
- 15 U.S.C. § 1512 is an Organic Law which confers general powers and duties authority to executive agencies, vesting jurisdiction and control of departments, bureaus, offices and branches.
- Executive Orders 10450, 11478, 12065, 5 U.S.C. 301 and 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.
- 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

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):			

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*		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):			
*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	o. Medical Information
d. Gender		j. Telephone Number	p. Military Service
e. Age		k. Email Address	q. Physical Characteristics
f. Race/Ethnicity		l. Education	r. Mother's Maiden Name
s. Other general personal data (specify):			

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			
i. Other work-related data (specify): Division/organization name, regional location, optional text field that is not to contain PII.					

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)	
Latitude/Longitude for spotter reports.	

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X*
Telephone	X	Email	X		
Other (specify):					
*If requesting spotter newsletter					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

NOAA8882 does not process PII information and only stores the information. The information that is stored is collected directly from the individual via secure email transmission or in person. The individual providing the information validate that the information provided is accurate.

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.
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	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)	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).

The NWS ER WAN/LAN system maintains information concerning each member of the ER workforce (employees). This information is managed by the NWS Eastern Region Headquarters (ERH) Administration Personnel.

The administrative information maintained on these databases consists of:

- Name / Position / GS Level/Series/Service Computation Date/Date of Grade/ Date of separation
- Residential information (Address, phone numbers)
- Government email addresses
- Division/Organization Name
- Regional Office Location
- Optional text field with current/relevant personnel issues.

The information is maintained as a supplement to other employee records for purposes of developing statistical reports, and performing other related administrative tasks.

There are also local databases at the local WFO/RFC that maintain information on volunteers (members of the public) who provide them weather reports. The database holds the following information on these volunteers:

- First and last name
- Mailing address
- County
- Phone (home/cell)
- Email address (also collected on the Cooperative Web site if requesting the newsletter)
- Hours to be contacted for severe weather reports
- Possession of a rain gauge, anemometer, thermometer, snow stick, or weather station
- Brief description of location of spotter's personal residence
- Last time attended spotter class
- Community Weather Involvement Program Identification – (optional) not all offices use this. It's a locally assigned number from the field office.
- Latitude / Longitude

All of this information collected on volunteers is provided voluntarily and most people who sign up do so during a community outreach training program, known as "spotter talks." Eastern Region staff is responsible for the maintenance of this database. This database information is accessible for viewing by all staff members in order to make calls for severe weather information.

- 5.2 Describe any potential threats to privacy 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 is primarily 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. AC, IA, AU) 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	X		
DOC bureaus	X*		
Federal agencies	X*		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

*Law enforcement

	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	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: http://www.nws.noaa.gov/om/coop/index.htm	
X	Yes, notice is provided by other means.	Specify how: For the workforce database, employees are notified at the time of recruitment that the collection of their information is mandatory as a condition of employment. For the Spotter Volunteers, notice is provided in the cooperative agreement form when information is collected.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the workforce database, individuals may inform HR staff verbally or in writing, that they do not want their information added to the database; however, provision of the information is a condition of employment. All information is voluntary for Spotter Volunteers, as part of the cooperative agreement to work with NWS on providing observations. There is a Privacy Act Statement on the Web site.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For the workforce database, employees may choose not to consent to all uses (administrative, job vacancy tracking, statistical reports) by informing HR staff verbally or in writing; however, they are required to provide the information as a condition of employment. The only use of the information for volunteers is for contact purposes, which is explained in the cooperative agreement. No other uses are suggested or specified. Provision of the information and signing of the cooperative agreement implies consent to that use.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the workforce data, information is routinely updated as an employee's role or position changes. Employees cannot directly review the information, but may request to review their information and ask that it be updated, through
---	---	--

		<p>their supervisors. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Management Division (AMD) Chief.</p> <p>The local manager who recruited the volunteers updates their information when notified by them to do so. Updates are not solicited but the instructions for submitting updates are in the cooperative agreement.</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	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: NOAA8882 utilizes Active Directory and additional Enterprise tools to monitor and track activity.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>3/28/2019</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting 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 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 the system maintaining the PII is controlled via Active Directory. Authentication is verified by the use of CAC IDs and PIV Cards. Only employees with authority to maintain these databases are allowed access to the 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, number, and link. (list all that apply): COMMERCE/DEPT-13. Investigative and Security Records COMMERCE/DEPT-18. Employee Personnel Files Not Covered By Notices of Other Agencies NOAA-11. Contact information for members of the public requesting or providing information related to NOAA's mission.
	Yes, a SORN has been submitted to the Department for approval on (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 – Weather, 1307-05. Chapter 300 – Personnel
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same 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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Name and contact information for volunteers, and names of employees, are in the system.
X	Quantity of PII	Provide explanation: Limited amount of PII stored.
X	Data Field Sensitivity	Provide explanation: There are no sensitive data fields other than optional text field with current/relevant personnel issues (where completed).
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Secured database managed by federal employees with limited user privileges.
	Other:	Provide explanation:

Section 12: Analysis

- 12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

NOAA8882 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. The workforce data is available to only authorized individuals. NOAA8882 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.