Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
National Weather Service (NWS) Alaska Region
General Support System (GSS)
(NOAA8880)

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

for Dr. Catrina D. Purvis 07/18/2019
Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

Version Number: 01-2015

NWS Alaska Region GSS (NOAA8880)

Unique Project Identifier: 006-000351100 00-48-02-00-01-00

Introduction: System Description

NOAA8880 is a General Support Services system that supports NWS offices within the Alaska Region. The servers for the NOAA8880 are in Anchorage, Alaska. 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 users, functions, and applications. Supported applications include weather forecaster supporting web applications, word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

The NWS Alaska Region (AR) Wide Area Network (WAN)/Local Area Network (LAN) databases consist of basic identifying information about employees. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports and performing other related administrative tasks. The system also collects and maintains information on volunteers who provide weather reports to system personnel.

The PII/BII in this system is not shared outside the bureau except in law enforcement cases. The information is not available to the general public, other NWS Regions, or other NOAA components. General information is available only to employees of the NWS Alaska Region. Specific information about individual personnel is available only to authorized NWS Alaska Region Headquarters Administration Staff. The volunteer databases are accessible to forecast staff so they can contact volunteers for severe weather information.

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.
- 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.
- From DEPT-1: Title 5 U.S.C., Title 31 U.S.C. 66a, 492, Title 44 U.S.D. 3101, 3309.
- From DEPT-13: 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.

- FROM DEPT-18: 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 impact 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 with no changes that 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	X
b. Taxpayer ID		f. Driver's License	X	j. Financial Account	X
c. Employer ID		g. Passport	X	k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	X
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	X	m. Religion	

b. Maiden Name		h. Place of Birth	X	n. Financial Information	X*
c. Alias		i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): N/A					

*For payroll.

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

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): N/A					

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	X
g. Other system administration/audit data (specify): Standard system infrastructure and configuration data.					

Other Information (specify)
N/A

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			
Other (specify):N/A					

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

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

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	X
Other (specify):			

	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	X
Video surveillance		Electronic purchase transactions	X
Other (specify):			

	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	
For litigation	X	For criminal law enforcement activities	X
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): Weather Data Dissemination			

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 Alaska Region Headquarters maintains PII concerning federal employees in the Alaska Region workforce. This information is managed by the NWS Alaska Region Headquarters Administration Personnel.
The information maintained includes:
Name
Age, Gender, date and place of birth, home contact information and email address
Position, GS Level/Series, Division/Organization Name, Regional Office Name/Location, work history
Financial information, medical information, military service information

This information is maintained to aid in maintenance of organization structures, supplementing management of employee records, and providing statistical data. The information is not shared with any third parties or unauthorized personnel.

There are also local databases at the local Weather Forecast Office/River Forecast Center (WFO/RFC), within the boundaries of the system, which 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
Telephone number (home/cell)
Email address

- 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

Non-sensitive PII in these databases is provided on a voluntary basis: volunteers sign up and provide the information during spotter talks* that the NWS conducts in preparation for the severe weather season. These databases are accessible to forecast staff so they can contact volunteers for severe weather information. The information is collected from members of the public.

*** On-site spotter training classes are conducted annually in various locations in the system area. The spotter training class is designed for people new to severe storm spotting, as well as those that need refresher training. The training is comprised of all of the information that spotters need to be effective and stay safe. Information on the trainings is posted on the applicable NWS Web site.**

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):			

*For law enforcement purposes

	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): N/A			

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 volunteer database, users are notified on the volunteer cooperative agreement form (see PAS). For the workforce database, individuals are notified by NOAA Workforce Management via email, that the collection of PII 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: Prospective volunteers may choose not provide the non-sensitive PII, by not completing the volunteer form, and thus will not become volunteers. For the workforce database, individuals may decline having their PII added to this database by providing a written request to the Chief, Administrative Division, when they start work within the office; however, this action will affect their employment status.
	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 database, the information is provided on a purely volunteer basis and users provide the PII to participate in the program which constitutes consent to use of 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. When users click the "Submit" button on any of the Web forms found on our site, they are indicating voluntary consent to use of the information they submit for the stated purpose." For the workforce database, written consent to only particular uses of PII must be submitted to the Chief, Administrative Division. However, failure to consent to all particular uses may affect employment status.
	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: Specify how: For the volunteer database, users may request to review their data from, and send updates if needed, to their local station manager. For the workforce database, PII is routinely updated as an employee's role or position changes. Employees may request their information from, and ask that it be updated through, their supervisors. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Management Division (AMD) Chief.
	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.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff 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: PII/BII is tracked on paper records and stored in HR controlled spaces.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 28, 2018 ☐ 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 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).
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.

Access to the system maintaining the PII is controlled by access via Active Directory and the use of Common Access (CAC)/Personal Identity Verification (PIV) cards. Only employees with authority to maintain this database 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 and number: The following SORNS apply to the information on this system: NOAA-11, Contact information for members of the public requesting or providing information related to NOAA's mission; DEPT-1 :Attendance, Leave, and Payroll Records of Employees and Certain Other Persons; DEPT-18: Employees Personnel Files Not Covered by Notices of Other Agencies DEPT-13, Investigative and Security Records:
	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 General Records Schedule (GRS) 20, issued by National Archives and Records Administration (NARA)
	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	X	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.

	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.

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

X	Identifiability	Provide explanation: Individuals may be identified.
X	Quantity of PII	Provide explanation: Limited amount of PII stored.
X	Data Field Sensitivity	Provide explanation: Human resources information is stored, including SSNs..
X	Context of Use	Provide explanation: Employee information only.
	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 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.

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

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.