Version Number: 01-2021

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

Privacy Impact Assessment
for the
NOAA8880
NWS Alaska Region General Support System

Reviewed by: Mark Graff Bureau Chief Privacy Officer

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

GRAFF.MARK.HYRUM.1514447892 Digitally signed by GRAFF.MARK.HYRUM.1514447892
Date: 2023.10.23 08:10:10 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA/NWS/Alaska Region General Support System

Unique Project Identifier: NOAA8880

Introduction: System Description

Provide a brief description of the information system.

The National Weather Service (NWS) Alaska Region GSS (NOAA8880) provides weather, hydrologic, and climate forecast 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 productions, including forecasts and waring is dependent on a complex interaction of many information resources and systems. This system (NOAA8880) 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, scientific & technical research, and innovation activities of employees within the organization.

NOAA8880 supports the NWS offices with the Alaska Region. Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct and indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Network (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, research and development, and collaboration.

Address the following elements:

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

The National Weather Service (NWS) Alaska Region (NOAA8880) is a General Support System (GSS) that provides weather, hydrologic, and climate forecast 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.

NOAA8880 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, scientific & technical research, and innovation activities of employees within the organization.

(b) System location

NOAA8880 maintains offices across the state of Alaska.

Alaska Region Headquarters – Anchorage, AK

Weather Forecast Offices
WFO AFC – Anchorage, AK
WFO AFG – Fairbanks, AK
WFO AJK – Juneau, AK

River Forecast Centers
Alaska-Pacific RFC – Anchorage, AK

Center Weather Service Units
CWSU ZAN – Anchorage, AK

Weather Service Offices
WSO ANN – Metlakatla, AK
WSO BRW – Barrow, AK
WSO BET – Bethel, AK
WSO CDB – Cold Bay, AK
WSO AKN – King Salmon, AK
WSO OTZ – Kotzebue, AK
WSO MCG – McGrath, AK
WSO OME – Nome, AK
WSO SNP – Saint Paul Island, AK
WSO YAK – Yakutat, AK

Other Offices
Dutch Harbor NWR – Dutch Harbor, AK
National Tsunami Warning Center – Palmer, AK

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

NOAA8880 maintains system interconnections with:

NOAA:
NOAA8106 (Upper Air Observing System)
NOAA8107 (Advanced Weather Interactive Processing System)
NOAA8850 (NWS Enterprise Mission Enabling System
NOAA8860 (Weather and Climate Computing Infrastructure Services)
NOAA8865 (NOAA Tsunami Warning System)

NOAA0100 (NOAA Cyber Security Center)

Non-NOAA:
Juneau Airport Wind System (JAWS) Data Distribution Service (FAA)
Alaska Lightning Detection System (ALDS) Alaska Fire Service (BLM)

No sensitive information is shared outside of NOAA8880.

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

NOAA8880 supports the NWS offices within the Alaska Region. Although there are a variety of hardware and operating systems, all the activities are interconnected. The system provides direct and indirect mission support for the NWS as a Government agency.

Mission Support infrastructure encompasses Wide Area Networks (WAN), Local Area Network (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, research and development, and collaboration.

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

Only authorized employees and contractors have access to the NOAA8880 information system. Access is based on a need-to-know and user must use CAC to log in to the Government Furnished Equipment (GFE).

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

NOAA8880 transmits data via LAN/WAN connectivity.

(g) Any information sharing

FAA shares weather data via the Juneau Airport Wind System (JAWS) Data Distribution Service. Information is inbound to NOAA8880 only.

No sensitive information is shared outside of NOAA8880.

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

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.

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

NOAA8880 is a 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):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

X__ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License	X	j. Financial Account	X
b. Taxpayer ID		g. Passport	X	k. Financial Transaction	X
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	X
d. Employee ID	X	i. Credit Card *	X	m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

The SSN is collected on standard federal forms, e.g. OF-306. The statutory authority is 5 U.S.C. Sections 1302, 3301, 3304, 3328 and 8716.

* Credit cards, financial account, and financial transaction relates to government purchase cards and activities only.

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	X *
b. Maiden Name	X	i. Place of Birth	X	p. Medical Information	X
c. Alias		j. Home Address	X	q. Military Service	X
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship	X	n. Religion			
u. Other general personal data (specify): * For payroll purposes.					

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	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	X *
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): GS level/series, division/organization name, regional office name/location. * Associated with Government credit card purchases.					

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	X	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	
b. IP Address	X	d. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

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):					

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.

Accuracy of information is ensured via proper handling and storage methods as well as through proper access control which restricts information access to only approved individuals. Access controls enable data consistency, accuracy, and trustworthiness. In person and telephone information is obtained directly from the person the information pertains to and is provided voluntarily. Government specific information is obtained from existing sources from which the individual has the opportunity to request to be updated through their supervisor.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
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	X
Video surveillance	X	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			
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)		For web measurement and customization technologies (multi-session)	
Other (specify): Information on volunteers is utilized to obtain reports of 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 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 of Birth
- Place of Birth
- Home contact information
- 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 in use by all offices. 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.

Video surveillance imagery is captured at points of ingress and egress at facilities to ensure safety and security. Financial transaction information is collected in regard to federal purchase card transactions.

* 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.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to the privacy of sensitive information residing in the NOAA8880 information system include insider threats, employees with excessive access permissions, and accidental information disclosure. Controls that have been put in place to reduce the likelihood of occurrence include initial and refresher training on the appropriate handling of sensitive information, periodic reviews of user access permissions, security background investigations, timely removal of system access for terminated employees, and maintaining/proper disposal of information, in accordance with NOAA Record Controls Schedule.

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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

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

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NOAA8106 – Upper Air Observing System NOAA8107 – Advanced Weather Interactive Processing System NOAA8850 – Enterprise Mission Enabling System NOAA8860 – Weather and Climate Computing Infrastructure Services NOAA8865 – NOAA Tsunami Warning System NOAA0100 – NOAA Cyber Security Center Juneau Airport Wind System (JAWS) Data Distribution Service (FAA) Alaska Lightning Detection System (ALDS) Alaska Fire Service (BLM) Network segmentation and boundary protection prevent PII/BII leakage; the interconnections are only allowed to pass certain types of traffic, some only unidirectional. Access to information is also granted only on a "need to know" basis. Access controls are instituted through the use of role-based security groups, enforcing the principle of least privilege and separation of duties. Authentication to the information system is controlled via the use of two-factor authentication and DoD Common Access Cards (CAC). System logs are audited by security staff and automatically transferred to an off-site Security Operations Center for storage and further analytics.
	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 the volunteer database, users are notified on the volunteer cooperative agreement form (see PAS in Appendix). For the workforce database, individuals are notified by the Office of Human Capital Services (OHCS) via email, that the collection of PII is mandatory as a condition of employment. Individuals are notified of video surveillance via posted signs on the grounds in additional to signage at points of ingress/egress that video recording is occurring.
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: 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. Individuals have the opportunity to decline to provide PII via video surveillance by not entering areas where signage is posted and video imagery is captured.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For the volunteer 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. Signage is posted at all points of ingress/egress at the facilities where imagery is captured. Individuals are informed that the purposes if for facility security and safety. Individuals consent to this use by continuing to access these locations.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the volunteer database, users may request to review their data form, 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 form, and ask that it be updated through, their supervisors. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program & Workforce Support Assistant, or the Administrative Management Division (AMD) Chief.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: There is no opportunity for individuals to update the video images recorded for safety & security purposes.

Section 8: Administrative and Technological Controls

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

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:** PII/BII is tracked on paper records and stored in HR controlled spaces.

X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 2023-05-31 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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).*

Folder/file permissions are enforced to control access to sensitive information. This is restricted to only individuals that have a need to know. All mobile devices are encrypted using Bitlocker (Windows laptops) and Mobile Device Manager (mobile phones). It is prohibited to transport sensitive information on mobile devices without authorization which reduces the risk of unauthorized disclosure. Multi-factor authentication (CAC/PIV card) is enforced and access to PII/BII is limited to those with a need to know.

Section 9: Privacy Act

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

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: • **NOAA-11**, Contact information for members of the public requesting or providing information related to NOAA's mission. • **COMMERCE/DEPT-1**: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons • **COMMERCE/DEPT-18**: Employees Personnel Files Not Covered by Notices of Other Agencies • **COMMERCE/DEPT-13**: Investigative and Security Records • **COMMERCE/DEPT-25**, Access Control and Identity Management System
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: Chapter 1300 National Weather Service Records Disposition Schedule, General Records 3.1 General Technology Management Records 3.2 Information Systems Security Records 4.1 Records Management Records 4.2 Information Access and Protection Records 5.1 Common Office Records 5.2 Transitory and Intermediary 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	X	Deleting	X
Other (specify):			

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

11.1 Indicate the potential impact that could result to the subject individuals and/or the

organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	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 level. *(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 is stored.
X	Data Field Sensitivity	Provide explanation: Human resources information is stored, including SSNs.
X	Context of Use	Provide explanation: Data is collected only for the stated purpose.
	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.)

NOAA8880 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, which include the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Management Division (AMD) Chief. NOAA8880

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. There is also a potential for insider threat. However, NWS only collects the least amount of information necessary to accomplish its mission.

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.