Version Number: 01-2020

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

Privacy Impact Assessment for the
NOAA8861
Aviation Weather Center, AWC

Reviewed by: Mark H. 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

Jennifer Goode 06/03/2021

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

U.S. Department of Commerce Privacy Impact Assessment
NOAA8861 Aviation Weather Center

Unique Project Identifier: NOAA8861

Introduction: System Description

The Aviation Weather Center (AWC), located in Kansas City, MO, enhances aviation safety by issuing accurate warnings, forecasts and analyses of hazardous weather for aviation interests. The Center identifies existing or imminent weather hazards to aircraft in flight and creates warnings for transmission to the aviation community. The Center also originates operational forecasts of weather conditions predicted to affect domestic and international aviation interests during the next 24 hours. The AWC collaborates with universities, governmental research laboratories, Federal Aviation Administration facilities, international meteorological watch offices and other National Weather Service components to maintain a leading edge in aviation meteorology hazards training, operations and forecast technique development.

Warnings of flight hazards, such as turbulence, icing, low clouds and reduced visibility remain most critical for the protection of life and property over the United States from the earth's surface up to Flight Level (FL) 240. Above FL 240, the AWC provides warnings of dangerous wind shear, thunderstorms, turbulence, icing, and volcanic ash for the Northern Hemisphere from the middle of the Pacific Ocean eastward to the middle of the Atlantic Ocean. Additionally, above FL 240, the AWC forecasts jet stream cores, thunderstorms, turbulence and fronts for the Northern Hemisphere from the east coast of Asia eastward to the west coast of Europe and Africa. Through international agreement, the AWC also has responsibility to back up other World Area Forecast Centers with aviation products distributed through the World Area Forecast System.

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

The Aviation Weather Center (AWC) is a general support system.

(b) System location

The Aviation Weather Center is located in Kansas City, MO.

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

The Aviation Weather Center interconnects with 557th Weather Wing. AWC utilizes NOAA8860 managed circuits and routers for all network connectivity. NOAA8860 owns and manages the circuit and hardware physically present at the 557th Wx Wing, AWC workstations are connected to this communications platform in a closed and locked room. There is an air gap between all NOAA and USAF equipment, the two organizations do not overlap or connect.

NOAA8861 Advanced Weather Interactive Processing System (AWIPS), and NOAA8860 - Weather and Climate Computing Infrastructure Services (WCCIS).

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

AWC ingests data into the operations network servers using DBNET and LDM. Once data is ingested it is processed by the AWC data processing servers and stored on the storage servers for use by the Linux Forecaster workstations and Development Linux Workstations. All ingested data enters through the local site router and/or firewalls. All incoming data is restricted and controlled.

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

Forecasters are able to retrieve and render the data on demand, display the data for analysis, and develop the AWC suite of products, e.g., scheduled guidance and outlook products and event driven watch and special products. These products cover a time period from a few days to within a few minutes. With such a time range and a mixture of important and routine products, it is important for AWC to have multiple distribution pathways. The AWC distribution pathway from highest preference to lowest preference is:

1. Product Distribution Service (PDS) to the AWC local PDS server.
2. PDS to any other National Center PDS.
3. AWC local access to the NWS Gateway via the redundant socket servers.
4. AWC PDS servers which in turn places text products into the AWIPS environment via AWIPS firewall for distribution to the AWIPS WAN.

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

The AWC ingests data into the operations network servers using DBNET and LDM. Once data is ingested it is processed by the AWC data processing servers and stored on the storage servers for use by the Linux Forecaster workstations and Development Linux Workstations. All ingested data enters through the local site router and/or firewalls. All incoming data is restricted and controlled.

(g) Any information sharing conducted by the system

The Aviation Weather Center collaborates with universities, governmental research laboratories, Federal Aviation Administration facilities, international meteorological watch offices and other National Weather Service components to maintain a leading edge in aviation meteorology hazards training, operations and forecast technique development. The data requestor's address is shared with the FAA. No sensitive information is collected or shared.

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

The legal authority for information collection addressed in this PIA is:

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

The Aviation Weather Center is categorized as a Moderate 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.

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

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 (version 01-2019 or later).

Section 2: Information in the System

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

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		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:					

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

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify): No physical address is needed but an overall zip code or country code is required to determine eligibility for AWC products and services as part of International Civil Aviation Organization (ICAO) agreements. The FAA determines the eligibility based on information submitted					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	f. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

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

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X

Telephone		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	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

Information accuracy is ensured by employing proper handling techniques and storage methods as well as utilizing access control methods that restrict access to only authorized individuals.

Information is also verified for accuracy and authenticated by the FAA upon receipt.

Access controls enable data consistency, accuracy, trustworthiness and on a need to know basis.

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	
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	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		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).

To promote information sharing initiatives:

The purpose of the World Area Forecast System (WAFS) Internet File Service (WIFS) is to provide timely delivery of critical aviation-related weather information to support air traffic management and flight operations in over 80 countries, and regional meteorological telecommunications between the United States and nations in the Caribbean and Central America. The WIFS will become the primary service at that time. Information is collected from members of the public.

To improve Federal services online:

Through improved, expedited dissemination of accurate critical aviation safety weather-related data, NOAA improves both existing aviation safety, as well as Federal Services to Federal Agency partners for the understanding of meteorological phenomenon and datasets necessary for future improved safe aviation.

For administrative matters:

The data collected is used for statistical analysis. Additionally, the information is helpful to identify groups of individuals who may be interested in helping AWC develop future products or to improve existing products. Information is collected from members of the public.

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 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 safeguards that limit access to the information and monitor the access to the information system. Access to information is granted on a "need to know" basis and the least privilege principle. Users undergo the NOAA annual mandatory IT Security Awareness and Privacy Training that 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			
Federal agencies	X*		
State, local, tribal gov't agencies			
Public	X**		
Private sector	X**		
Foreign governments			
Foreign entities			
Other (specify):			

* - FAA
** - Only weather data is shared with the Public and Private Sector. No PII is shared.

	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?

X	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.

	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.

X	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: FAA system to ensure ICAO agreements. PII transmitted between 8861 and FAA is encrypted and sent via Kiteworks.
	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://aviationweather.gov/wifs/registration/index .	
	Yes, notice is provided by other means.	Specify how:
	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: Individuals may decline to provide the information by not completing a request, but then they will not be registered.

	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: The Privacy Policy states that completion of the requested information implies consent to the uses described on the registration form.
	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: An individual may update their information, including product preferences, when accessing their account.
	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: AWC tracks login information for each account to determine if backup users (backup to UKMET) are overusing this service in accordance with the established UK-Met/FAA agreements.
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): July 31, 2020 ☐ 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).*

The address of the requester must be collected by the AWC and sent via encrypted file transfer to the FAA for analysis based on the UK-Met/FAA agreements before access can be granted as part of the International Civil Aviation Organization (ICAO) agreement.
AWC ingests data into the operations network servers using DBNET and LDM. Once data is ingested it is processed by the AWC data processing servers and stored on the storage servers for use by the Linux Forecaster workstations and Development Linux Workstations. All ingested data enters through the local site router and/or firewalls. All incoming data is restricted and controlled.

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)*: COMMERCE/NOAA-11, Contact Information for Members of the Public Requesting or Providing Information Related to NOAA's Mission. 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: System Access Records: the disposition authority is DAA-GRS-2013-0006-003. Disposition Instruction: Temporary. Destroy when business need ceases.
	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		Overwriting	
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, and does not have to be 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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: There is information by which a person may be identified.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: There is no sensitive data.
X	Context of Use	Provide explanation: If the PII is lost or compromised, it would impact aviation weather warning communications. However, there would likely be no adverse effects experienced by the individual if their data was lost or compromised.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: PII is collected via an external website (HTTPS) and stored in a database that is not publicly accessible. All internal data transmitted to the FAA is done via Kiteworks.
	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.)

AWC collects only the minimum required information necessary for the purpose in which it is intended. In addition, AWC participates in a mandated annual Assessment and Authorization (A&A) exercise that evaluates, tests, and examines security controls to 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.