Version Number: 01-2015

U.S. Department of Commerce
NOAA

Privacy Impact Assessment
for the
Aviation Weather Center (NOAA8861)

Reviewed by: _____, Bureau Chief Privacy Officer
Mark Graff

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

for Dr. Catrina D. Purvis LISA MARTIN Digitally signed by LISA MARTIN DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=LISA MARTIN, 0.9.2342.19200300.100.1.1=13001000105292 Date: 2018.08.06 13:41:44 -04'00' 07/27/2018

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

U.S. Department of Commerce Privacy Impact Assessment
National Weather Service / Aviation Weather Center

Unique Project Identifier: NOAA-8861

Introduction: System Description

The World Area Forecast System (WAFS) Internet File Service (WIFS) is provided by the United States National Weather Service (NWS) Aviation Weather Center (AWC) as a highly reliable Internet source of meteorological products. The purpose of 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. This service is available to all authorized customers. The Federal Aviation Administration (FAA) has an agreement with the United Kingdom Meteorological Office (UK-Met) which also produces similar products on a fee for service basis to the aviation community. Depending on the requester's legal address, the products may be obtained from the FAA via the AWC website at no cost. However, 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. The ICAO recognizes the use of the Internet to access aviation weather data in support of flight planning. The WIFS provides this capability.

Once the FAA approves a user state (country or organization) to access the WIFS system, the AWC will issue a user name and password which will be required to access the data. The ICAO, in Amendment 75 to Annex 3, recognizes the use of the Internet to access aviation weather data in support of flight planning. The WIFS provides this capability and serves an important function backing up the International Satellite Communications System (ISCS).

The WIFS is an integral part of the AWC's Consolidated Aviation Web Services (CAWS) system which has been certified by the FAA as a Qualified Internet Communications Provider (QICP). The CAWS system provides QICP certification and access to the real-time repository for the WIFS application via the HTTPS protocol. The primary open source product for access using the HTTPS protocol is the "GNU Wget package" (GNU is a recursive acronym for "GNU's Not Unix" and is pronounced "guh-NEW"). For the purposes of meeting the ICAO Document 9855 (Guidelines on the Use of the Public Internet for Aeronautical Applications) and the FAA's Advisory Circular 00-62 for the Qualified Internet Communications Provider (QICP) requirement, there are three geographically remote web farms that house the WIFS data.

The AWC is a Moderate Impact system.

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. *See also* U.S. Department of Commerce and NOAA official Privacy Act system of records listing: COMMERCE/NOAA-11. This listing sets forth the authority for the maintenance of the system as well as for the underlying collection of information.

The data requestor's address is shared with the FAA. No sensitive information is collected or shared.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

____ This is a new information system.
____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

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

Section 2: Information in the System

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

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

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

Work-Related Data (WRD)					
a. Occupation		d. Telephone Number	X	g. Salary	
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

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		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

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

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

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

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

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility		For administering human resources programs	
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): Name, email and address may be collected for those requesting data, so that they may open an account through which to receive the data.

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 determine eligibility to receive data, and to promote information sharing initiatives:

The purpose of 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.

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.

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			
Private sector			
Foreign governments			
Foreign entities			

Other (specify):			

*FAA

	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.

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. When the user registers his/her information, it is captured using HTTPS (encryption). The data is stored locally in a database. Last name is then e-mailed to AWC as notification of a new registration. AWC then collects this information in a word document and then uses Accellion to transmit data to FAA for review. All data between AWC and FAA is transmitted via Accellion.
	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: 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 his/her information, including product preferences, when accessing his/her 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.
	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 not overusing this service in accordance with the established UK-Met/FAA agreements.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 31, 2017 ☐ 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. (MODERATE)
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security and privacy controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
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.

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.

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). Commerce/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, 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.)*

	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 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: There is information by which a person may be identified.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	There is no sensitive data.
X	Context of Use	Provide explanation: If the PII is lost or compromised, would impact aviation weather warning communications.
	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 Accellion (Encrypted).
	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.
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.
X	No, the conduct of this PIA does not result in any required technology changes.