Template Version Number: 01-2021

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

Privacy Impact Assessment for the
NOAA8881
National Weather Service - Central Region (NWSCR)

Reviewed by: Robin Burress for 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

Robin.Burress Digitally signed on 2025.06.09 13:35:04 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment

NOAA/NWS/CR General Support System

Unique Project Identifier: NOAA8881

Introduction: System Description

Provide a brief description of the information system.

The National Weather Service (NWS)) CR Local Area Network (LAN)/Wide Area Network (WAN) is a general support system that provides weather, hydrologic, and climate forecasts 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 other governmental agencies, the private sector, the public, and the global community. Issuance of warnings and forecasts is dependent on a complex interaction of many information resources. The system is designed and used to collect, process, and disseminate supplemental weather data which supports warning and forecast products. It also supports the supporting and administrative functions and supports the scientific & technical research and innovations activities of all offices within the Central Region including the regional headquarters.

Although there are a variety of hardware and operating systems, several of the activities are interconnected. The system provides direct and indirect mission support for the NWS as a Government agency. Mission Support infrastructure encompasses W AN/ LAN host computer systems and client-server systems. The system supports a variety of users, functions, and applications. Supported applications include word processing, spreadsheets, presentation graphics, database development and management, electronic mail, and image processing.

NOAA8881 site Weather Forecast Office (WFO) Louisville, KY employs a Unmanned Aircraft System (UAS) to support hydrologic functions as well as storm damage surveys.

Address the following elements:

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

General Support System.

(b) System location

National Weather Service Central Region Headquarters (NWSCRHQ) Kansas City, MO

Warning Decision Training Branch Norman, OK

Minneapolis, MN River Forecast Center

Pleasant Hill, MO River Forecast Center
Kansas City, Olathe, KS Center Weather Service Unit
Minneapolis, MN Center Weather Service Unit
Indianapolis, IN Center Weather Service Unit
Denver, CO Center Weather Service Unit
Chicago, IL Center Weather Service Unit
Aberdeen, SD Weather Forecast Office
Bismarck, ND Weather Forecast Office
Boulder, CO Weather Forecast Office
Central Illinois, Lincoln, IL Weather Forecast Office
Cheyenne, WY Weather Forecast Office
Chicago, IL Weather Forecast Office
Davenport, IA Weather Forecast Office
Des Moines, IA Weather Forecast Office
Detroit, MI Weather Forecast Office
Dodge City, KS Weather Forecast Office
Duluth, MN Weather Forecast Office
Goodland, KS Weather Forecast Office
Grand Forks, ND Weather Forecast Office
Grand Junction, CO Weather Forecast Office
Grand Rapids, MI Weather Forecast Office
Green Bay, WI Weather Forecast Office
Hastings, NE Weather Forecast Office
Indianapolis, IN Weather Forecast Office
Jackson, KY Weather Forecast Office
La Crosse, WI Weather Forecast Office
Louisville, KY Weather Forecast Office
Marquette, MI Weather Forecast Office
Milwaukee, WI Weather Forecast Office
Minneapolis, MN Weather Forecast Office
Northern Central Lower Michigan, Gaylord, MI Weather Forecast Office
North Platte, NE Weather Forecast Office
Northern Indiana, IN Weather Forecast Office
Omaha, NE Weather Forecast Office

Paducah, KY Weather Forecast Office

Pleasant Hill, MO Weather Forecast Office

Pueblo, CO Weather Forecast Office

Rapid City, SD Weather Forecast Office

Riverton, WY Weather Forecast Office

Sioux Falls, SD Weather Forecast Office

Springfield, MO Weather Forecast Office

St. Louis, MO Weather Forecast Office

Topeka, KS Weather Forecast Office

Wichita, KS Weather Forecast Office

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

NWSCR interconnects with the following Federal Information Security Management Act (FISMA) systems (ALL internal to NOAA):

NOAA0100 – Cyber Security Center
NOAA8102 – Automated Surface Observation System
NOAA8106 – Upper Air Observing System
NOAA8107 – Advanced Weather Interactive Processing System
NOAA8850 – Enterprise Mission Enabling System
NOAA8860 – Weather and Climate Computing Infrastructure Services

Other (non-FISMA):

Big Sioux River Flood Forecasting Center
Bureau of Reclamation – Billings Area Office
Bureau of Reclamation – Great Plains Regional Office
Colorado State University- Cooperative Institute for Research in the Atmosphere (CIRA)
Iowa Flood Center
North Dakota State Agricultural Communications
University of Wisconsin – Madison
United States Corps of Engineers (USACE) – Northwestern Division – Omaha
USACE – St. Louis Office
USACE – St. Paul District
USACE _ Rock Island
United States Geological Survey (USGS) – Illinois Water Science Center
Internet

* NOAA0100 is not a new interconnection. The PIA is being updated to accurately reflect an existing interconnection not previously documented

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

The NWSCR WAN/LAN databases consist of basic identifying information about employees and volunteers who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports, andperforming other related administrative tasks. In addition, WFOs and RFCs maintain local databases that contain information on volunteers who provide weather reports to them. The NOAA8881 site WFO Louisville, KY employs a Mavic 2 Enterprise drone that will be used to collect hydrologic data along with post storm damage surveys.

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

Information is retrieved using Government Funded Equipment (GFE) while at the official duty station and both GFE and Personally Owned Equipment while teleworking. Common Access Card (CAC) usage is enforced while at the duty station and when using the Virtual Private Network (VPN) from the teleworking location. Data on the UAS is captured on internal drive or Secure Digital (SD) card. It uses Advanced Encryption Standard (AES)-265 encryption and is password protected. The UAS is operated in a way (altitude/ hydrologic locations) where the capturing of PII is unlikely. As soon as the data has been transferred to a local Personal Computer (PC), the UAS footage is reviewed and any PII that was captured is deleted.

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

Only authorized personnel can transmit to and from NWSCR using secure methods. NWSCR uses OneNet which is a Trusted Internet Connection Access Provider. If PII needs to be emailed, NWSCR uses KiteWorks for encrypted transport. UAS data is transferred directly to a dedicated PC for PII review/deletion.

(g) Any information sharing

The WAN/LAN databases consist of basic identifying information (name, phone number, address) about employees and volunteers who are part of the regional workforce. The databases are maintained as a supplement to other employee records for purposes of developing statistical reports, and performing other related administrative tasks. N WSCR site WFO Louisville, KY uses a UAS for hydrologic surveys and post storm damage surveys. The UAS is used strictly over hydrologic resources and areas of storm damage. Any privacy data that is inadvertently collected will be immediately deleted.

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

	Type of Information Collected (Introduction h.)	**Applicable SORNs (Section 9.2)**	**Programmatic Authorities (Introduction h.)**

1.	Badging & CAC Issuance	COMMERCE/DEPT-18	Electronic Signatures in Global and National Commerce Act, Public Law 106-229
			5 U.S.C. 301
2.	Contact Information for the Public	NOAA-11	5 U.S.C. 301, Departmental Regulations
			15 U.S.C. 1512, Powers and duties of Department
3.	Building Entry/Access & Surveillance	COMMERCE/DEPT-25	5 USC 301
			Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
4.	Personnel Actions Including Training	OPM-GOVT-1	5 U.S.C. 1302, 2951, 3301, 3372, 4118, 5379, 8347
			Executive Orders 9397, as amended by 13478, 9830, and 12107

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

Moderate

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*		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. Sex		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Marital Status	
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	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	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify): Name /Position General Schedule (GS) Level/Series/Service Computation Date/Date of Grade/ Date of separation.					

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

Other Information (specify)
Latitude/Longitude for spotter reports.

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

Directly from Individual about Whom the information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone	X*	Email			
Other (specify): *PAS is posted on the Weather Observer website, https://www.weather.gov/coop/standards. Spotters may call in from time to time to change their information.					

Government Sources

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

Non-government Sources					
Public Organizations		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.

NWSCR does not process PII information and only stores the information. The information that is stored is collected directly from the individual via secure email transmission or in person. The individual providing the information validate that the information provided is accurate. The UAS is used for hydrologic observing and storm damage surveys and not used as a source for PII.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. • 0648-CS - awaiting OMB review and approval
	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): Cameras are in place at all offices. Data is recorded but the data does not include any sensitive PII. Data is only captured outside facility entries and other locations around like parking lots and upper air facilities where present.			

	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	
Other (specify): Although the UAS has the potential to collect PII via video surveillance, it is not the purpose of the device and any PII captured is immediately deleted. The UAS is operated in mainly remote locations and is always in the line of sight of the operator. UAS data locations are captured by GPS/satellite during the drone flight. Those location coordinates are then input into the metadata for each drone picture or video. Security cameras have been deployed for many years in NWSCR, however, the information wasn't previously added to the privacy documents. Data is recorded but the data does not include any sensitive PII. Data is only captured outside facility entries and other locations around like parking lots and upper air facilities where present. Data is stored locally on the Network Video Recorder (NVR). Stored data is only available to IT staff and management when working with law enforcement.			
	There are not any IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

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

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	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):			

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 CR WAN/LAN system maintains information concerning each member of the CR workforce (employees). This information is managed by the NWS Central Region Headquarters (CRH) Administration Personnel. Only the Workforce Manager and the CRH Information Technology (IT) Database Administrator have access to these workforce databases.

The administrative information maintained on these databases consists of:

- Name /Position /GS Level/Series/Service Computation Date/Date of Grade/ Date of separation
- Residential information (Address, phone numbers)
- Government email addresses
- Division/Organization Name
- Regional Office Location
- Optional text field with current/relevant personnel issues, for which inclusion of PII is prohibited.
- The information is maintained as a supplement to other employee records for purposes of tracking job vacancies, developing statistical reports, and performing other related administrative tasks.
- There are also local databases at the local WFO/RFC that maintain information on volunteers (members of the public) who provide them weather reports. The database holds the following information on these volunteers:
- First and last name
- Mailing address
- County
- Phone (home/cell)
- Email address
- Hours to be contacted for severe weather reports
- Possession of a rain gauge, anemometer, thermometer, snow stick, or weather station
- Brief description of location of spotter's personal residence
- Last time attended spotter class
- Community Weather Involvement Program Identification – (optional) not all offices use this. It's a locally assigned number from the field office.
- Latitude / Longitude

All of this information collected on volunteers is provided voluntarily and most people who sign up do so during a community outreach training program, known as "spotter talks." Spotter talks help the public prepare for the severe weather season. A locally-assigned staff is responsible for the maintenance of this database, with occasional help from 1 to 2 other staff members for data entry. This database information is accessible for viewing by all staff members in order to make calls for severe weather information.

NWSCR site WFO Louisville, KY uses a UAS to support hydrologic functions as well as storm damage surveys. Use of the UAS is covered by the Department of Commerce System of Records Notices (DOC SORN) and NOAA Policy. The UAS is operated mainly in remote areas and is always in sight of the operator.

Video surveillance is used as a deterrent. In case of a security incident, the footage may be used to assist in any investigation.

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 controls (i.e. Access Control (AC), Identification and Authentication (IA), Audit and Accountability (AU)) which limits access to the information as well as monitors the access to the information system. Access to information is granted on a "need to have" basis and the least privilege principle.

Users undergo annual mandatory security awareness and privacy training with includes the proper handling of information. Users acknowledge the rules of behavior to ensure they understand their responsibilities.

NWSCR site WFO Louisville, KY uses a Mavic 2 Enterprise drone. The data captured by the Mavic is encrypted and password protected. The UAS has the potential to collect PII inadvertently. The UAS is flown by line of sight but still has the potential to be downed outside control of the operators.

Insider threat could potentially expose privacy data.

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			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	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.

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: NOAA8102 – Automated Surface Observation System NOAA8106 – Upper Air Observing System NOAA8107 – Advanced Weather Interactive Processing System NOAA8850 – Enterprise Mission Enabling System NOAA8860 – Weather and Climate Computing Infrastructure Services *NOAA0100 – Cyber Security Center Mitigations include the use of system security controls which limits access to the information as well as monitors the access to the information system. Access to information is granted on a "need to have" basis and the least privilege principle. Authentication is verified by the use of CAC IDs and PIV Cards. Only employees with authority to maintain these databases are allowed access to the information. Other (non-FISMA): Big Sioux River Flood Forecasting Center Bureau of Reclamation – Billings Area Office Bureau of Reclamation – Great Plains Regional Office Colorado State University (CIRA) Iowa Flood Center North Dakota State Agricultural Communications University of Wisconsin – Madison USACE – Northwestern Division – Omaha USACE – St. Louis Office USACE – St. Paul District USACE _ Rock Island USGS – Illinois Water Science Center Internet Mitigations include the use of system security controls which limits access to the information as well as monitors the access to the information system. Access to information is granted on a "need to have" basis and the least privilege principle. Authentication is verified by the use of CAC IDs and PIV Cards. Only employees with authority to maintain these databases are allowed access to the information. * NOAA0100 is not a new interconnection. The PIA is being updated to accurately reflect an existing interconnection not previously documented

	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 workforce database, employees are notified at the time of recruitment that the collection of their information is mandatory as a condition of employment. For the Spotter Volunteers, notice is provided in the cooperative agreement form when information is collected. Updates to spotter information is given voluntarily over the phone initiated by the spotter. NWSCR does not use the UAS at site WFO Louisville, KY to capture images of individuals. In the rare even PII is captured, the PII would be immediately deleted. Signs are posted at the facility giving notification of security camera usage. Signs are posted in parking lots and at building entrances.
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For the workforce database, individuals may inform Human Resources (HR) staff, verbally or in writing, that they do not want their information added to the database; however, provision of the information is a condition of employment. For Spotter Volunteers, failure to provide this information will result in volunteers being precluded from working with NWS as part of the cooperative agreement to provide observations. NWSCR does not use the UAS at site WFO Louisville, KY to capture images of individuals. In the rare even PII is captured, the PII would be immediately deleted. Signage is posted in parking lots and building entrances where surveillance is being recorded, individuals who no longer want to be recorded may leave the area.
	No, individuals do not have an opportunity to decline to provide PII/BII.	

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For the workforce database, employees may choose not to consent to all uses (administrative, job vacancy tracking, statistical reports) by informing HR staff verbally or in writing; however, they are required to provide the information as a condition of employment. The only use of the information for volunteers is for contact purposes, which is explained in the cooperative agreement. No other uses are suggested or specified. Provision of the information and signing of the cooperative agreement implies consent to that use. Providing information is voluntary for Spotter Volunteers. However, failure to provide this information will result in volunteers being precluded from working with NWS as part of the cooperative agreement to provide observations. NWSCR does not use the UAS at site WFO Louisville, KY to capture images of individuals. In the rare even PII is captured, the PII would be immediately deleted.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Security cameras in place record 24/7. This data is only used when needed for further investigation of an event.

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For the workforce data, information is routinely updated as an employee's role or position changes. Employees cannot directly review the information, but may request to review their information and ask that it be updated, through their supervisors. Updates are made by the following authorized individuals: the Workforce Program Manager, the Travel Program and Workforce Support Assistant, and the Administrative Support Division (ASD) Chief (all outside of system boundaries). Providing information is voluntary for Spotter Volunteers. However, failure to provide this information will result in volunteers being precluded from working with NWS as part of the cooperative agreement to provide observations. NWSCR does not use the UAS at site WFO Louisville, KY to capture images of individuals. In the rare even PII is captured, the PII would be immediately deleted.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Security cameras in place record 24/7. This data is only used when needed for further investigation of an event.

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.
	Access to the PII/BII is being monitored, tracked, or recorded. **Explanation:**
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): 06/26/24 ☐ 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).*

Access to the system maintaining the PII is controlled via National Active Directory. Authentication is verified by the use of CAC IDs and PIV Cards. Only employees with authority to maintain these databases are allowed access to the information.

NWSCR site WFO Louisville, KY UAS stores data on a password protected internal hard drive. All data is overwritten once removed from the UAS. Any PII inadvertently collected is deleted before use.

Access to security camera footage is limited to those holding IT Admin credentials.

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/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies 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 OPM-GOVT-1 General Personnel Records
	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: NOAA Records Schedule Chapter 300 and 1300. NWSCR site WFO Louisville, KY UAS all data is overwritten on the internal Hard Drive (HD). Any PII collection is incidental, unintentional and not retained.
	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.)*

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: Name and contact information for volunteers, and names of employees, are in the system
X	Quantity of PII	Provide explanation: Limited amount of PII stored.
X	Data Field Sensitivity	Provide explanation: There is an optional text field for current/relevant personnel issues for which inclusion of PII is prohibited.
X	Context of Use	Provide explanation: NOAA881 site WFO Louisville, KY UAS data is used to observe hydrologic conditions as well as storm damage.
	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. NWSCR site WFO Louisville, KY UAS data is only transferred by the UAS operator to a local PC for use and deletion of any PII inadvertently obtained.
	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.)

Security cameras are in place at all facilities but none collect sensitive PII. NWSCR 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. NWSCR 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.

NWSCR site WFO Louisville, KY UAS has a low risk of threat to privacy since it is operated mainly where no PII exists (hydrologic locations/damage areas). The UAS is flown by line of sight.

Insider threat could potentially expose privacy data.

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.