



USDA Privacy Impact Assessment

Fiscal Year 2025

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project	3
Mission Area System/Program Contacts	3
Abstract	4
Overview.....	4
Section 1: Authorities and Other Requirements	5
Section 2: Information Characterization	6
Section 3: Information Uses	7
Section 4: Notice	8
Section 5: Data Retention	9
Section 6: Information Sharing.....	10
Section 7: Redress.....	11
Section 8: Auditing and Accountability.....	12

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Water and Climate Information System (WCIS)
Program Office	National Water and Climate Center
Mission Area	Farm Production and Conservation (FPAC) /Natural Resources Conservation Service (NRCS)
CSAM Number	986
Date Submitted for Review	-

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Samantha Jones	202-221-9289
Information System Security Manager	Karl Hill	816-823-1496
System Project/Program Manager	Mathew Cervantes	573-465-0188

Abstract

The Water and Climate Information System (WCIS) support the United States Department of Agriculture (USDA) Snow Survey and Water Supply Forecasting (SSWSF) and Soil Climate Analysis Network (SCAN) Programs. The SSWSF program manages a comprehensive network of manually measured snow courses and automated Snow Telemetry (SNOTEL) monitoring sites throughout the West, ingests and stores the data collected by those sites, and uses the data to forecast streamflow runoff that will occur when snow melts. The SCAN program supports natural resource assessments and conservation activities through comprehensive, nationwide moisture and climate data collection. WCIS stores the information collected by the networks managed by both programs across all 50 states and several US territories. The PIA is being conducted because this system contains PII.

Overview

WCIS is owned by USDA's National Water and Climate Center (NWCC), in support of the SSWSF and SCAN programs within NRCS. The business purpose of the information technology (IT) system is to aggregate daily weather-related information. WCIS supports people and land by providing science-based technical assistance to all clients to enable natural resource planning and decision-making. This supports NRCS' mission to ensure national forests and private working lands are conserved, restored, and made more resilient while enhancing water resources. WCIS supports mission-essential functions at 12 federal agencies, as well as thousands of farmers, state and local governments, companies, and more. Only names and email addresses of USDA employees are stored in WCIS. No personal information about other individuals is stored in WCIS for any purpose.

It is estimated that approximately 120 are within WCIS. The snow, water, and climate data stored in WCIS are available to the public through several applications, both manually and programmatically. An account is not required to access this data, and individual information is not stored within the system. The ability to edit data in WCIS is limited to USDA employees in the Snow Survey and Water Supply Forecasting program and the SCAN program who have an account for that purpose. WCIS account holders can see the name and username of other WCIS account holders. The system is hosted online, and PII is only visible to WCIS account holders who are logged on through USDA authentication. NRCS is granted annual appropriations specifically for the operation of a Snow Survey and Water Supply Forecasting Program. WCIS is an essential component of that program and central to its efficient and effective operation.

The legal authorities operating the IT system include the following:

1. Soil Conservation and Domestic Allotment Act (16 USC 590a et seq).
2. Food Security Act of 1985 (Public Law 99-198).
3. Agriculture Improvement Act of 2018 and the American Relief Act, 2025.

Section 1: Authorities and Other Requirements

These questions identify all statutory and regulatory authorities for operating the project, application, or system, including the authority for collection, which SORN applies, if an ATO has been completed, and if there is Paperwork Reduction Act coverage:

What legal authorities and/or agreements permit the collection of information by the project, application, or system?

The legal authority to collect this information are:

- 1. Soil Conservation and Domestic Allotment Act (16 USC 590a et seq).
- 2. Food Security Act of 1985 (Public Law 99-198).
- 3. Agriculture Improvement Act of 2018 and the American Relief Act, 2025.

NRCS is granted annual appropriations specifically for the operation of a Snow Survey and Water Supply Forecasting Program. WCIS is an essential component of that program, and central to its efficient and effective operation. The only PII collected by WCIS is that of employees of the USDA/NRCS.

Has Authorization and Accreditation (A&A) been completed for the project, application, or system?

- Security Plan Status: Completed, New Security Plan underway
- Security Plan Status Date: August 30, 2024
- Authorization Status: Authorized To Operate
- Authorization Status Date: July 11, 2023
- Authorization Termination Date: July 11, 2026
- Risk Review Completion Date: June 17, 2025
- FTPS 199 Classification of the System: Moderate

Which System of Records Notices (SORNs) apply to the information?

None. Under the Privacy Act (5 U.S.C. § 552a(a)(5)), a "system of records" exists when records are retrieved by an individual's name or other personal identifier. WCIS does not organize or retrieve records by name, email, IP address, or any other personal identifier. WCIS uses only aggregated and identified datasets for reporting, segregates optional email addresses in a transient, time-limited store used solely for one-time follow-up, not for retrieval of records about an individual. Therefore, no SORN is required. If future changes enable retrieval by a personal identifier, a SORN analysis will be conducted before deployment.

Is the collection of information covered by the Paperwork Reduction Act?

No.

Section 2: Information Characterization

These questions define the scope of the information requested and collected, as well as the reasons for its collection as part of the project, application, or system being developed:

What information is collected, used, disseminated, or maintained in the project, application, or system?

Biographical Information:

- Name (Including Nicknames)
- Business Email Address

What are the sources of the information in the project, application, or system?

The information is supplied directly from the SSWSF and SCAN programs.

How is the information collected?

The information is collected from the program participants of the programs.

Does the project, application, or system use information from commercial sources or publicly available data? If so, explain why it is used.

No PII is collected or used from commercial sources or publicly available data.

How will the information be checked for accuracy? How often will it be checked?

USDA employees requiring access will confirm whether their access has been granted. WCIS accounts are terminated when an employee leaves the program, and a report of WCIS user accounts is reviewed monthly to confirm old accounts have been closed.

Does the project, application, or system use third-party websites?

Yes

What is the purpose of the use of third-party websites?

Data collected by partner agencies, such as the Bureau of Reclamation, is programmatically ingested to WCIS to improve the overall data set's comprehensiveness. No PII is collected through this process.

What PII will be made available to the agency with third-party websites?

N/A

List the privacy risks and mitigations related to the characterization of the information.

Privacy Risk: The information collected contains sensitive PII, which, if disclosed, would cause an unwarranted invasion of personal privacy.

Mitigation: The information is only disclosed to those responsible for the administration of the program or other entities that have legal authority to access the information. Users are required to authenticate their identity prior to accessing the information, and access is restricted based on user role.

Section 3: Information Uses

These questions delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated, and/or maintained will support the project, application, or system's business purpose.

Names are used to track which USDA employees have WCIS accounts and which staff have taken data management actions in the system.

Does the project, application, or system use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No

List the privacy risks and mitigations related to uses of the information.

Privacy Risk: Access to the data is monitored to ensure safeguarding against unauthorized access and use.

Mitigation: Access to names is determined by the owner of the information, user roles, and restricted access. Additionally, access will only be granted to the PII upon appropriate legal authority.

Section 4: Notice

These questions are intended to provide notice to the individual of the scope of information collected, the right to consent to use of the information, and the right to decline to provide information.

How does the project/program/system provide notice to individuals before collection?

Individuals are provided notice through a Privacy Act Statement presented on WCIS data submission interfaces, forms, or web pages at the point of collection, as well as through a publicly available WCIS privacy notice. Although WCIS is not a Privacy Act System of Records because it does not retrieve records by personal identifiers and therefore does not require a SORN, notice is still provided consistent with 5 U.S.C. § 552a(e)(3).

What options are available for individuals to consent, decline, or opt out of the project?

Participation in WICS is voluntary. Individuals may decline to provide information by choosing not to submit data or engage with WICS. There are no penalties for non-participation. Because WCIS does not retrieve records by personal identifiers, a formal opt-out process is not applicable; instead, individuals exercise choice at point of collection.

List the privacy risks and mitigations related to notice.

Privacy Risk: Individuals are provided notice through a Privacy Act Statement presented on WCIS data submission interfaces, forms, or web pages at the point of collection, as well as through a publicly available WCIS privacy notice.

Mitigation: Participation in WICS is voluntary. Individuals may decline to provide information by choosing not to submit data or engage with WICS.

Section 5: Data Retention

These questions outline how long information will be retained after the initial collection.

What information is retained and for how long?

Although there is no SORN, the management of retention and disposal is handled with utmost care and in strict accordance with USDA Regulation 3080-001, ensuring the security and privacy of all data.

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, indicate the name of the records retention schedule.

The retention schedule has been approved by the USDA records office and NARA. The [Records Schedule Number](#) is NI-114-08-001.

List the privacy risks and mitigations related to data retention.

Privacy Risk: The information contained in the records is sensitive, which could cause a privacy breach if not properly safeguarded.

Mitigation: Access and destruction of the information will only occur upon establishment of proper legal authority to access the data, pursuant to the Privacy Act, Section 1619 of the Farm Bill, and the appropriate SORN(s) covering the information.

Section 6: Information Sharing

These questions define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared, received, and/or transmitted? What information is shared, received, and/or transmitted, and for what purpose? How is the information transmitted?

No PII is shared with other internal organizations or systems.

List the privacy risks and mitigations related to internal information sharing and disclosure.

Privacy Risk: Unauthorized access to sensitive data could pose a risk to existing data and disclosure to unauthorized parties.

Mitigation: Information is electronically transmitted and encrypted, and access is only granted based on a user's role and active/inactive status.

With which external organizations (outside USDA) is information shared, received, and/or transmitted? What information is shared, received, and/or transmitted, and for what purpose? How is the information transmitted?

No PII is shared with external organizations or systems.

List the privacy risks and mitigations related to external information sharing and disclosure.

Privacy Risk: N/A

Mitigation: N/A

Section 7: Redress

These questions address the individual's ability to ensure the accuracy of the information collected about him or her.

What are the procedures that allow individuals to gain access to their information?

Should an individual wish to gain access to their information, they will need to make a written request to the system owner or the FPAC FOIA Officer to authenticate their identity and identify the records they request access to in WCIS.

What are the procedures for correcting inaccurate or erroneous information?

Individuals must make a written request to the system owner, information system owner or Privacy Officer, authenticate their identity, identify the portion(s) of the record that needs to be corrected, and describe whether their information is inaccurate or erroneous. Upon receipt and review of the request, if it is verified that a correction needs to be made, the record will be corrected, and a sample of the document with the correction will be transmitted to the individual who made the request.

Requests to correct a record should be sent directly to the local or state FSA Office. All requests (1) must be in writing, (2) clearly identify the information that needs correction, (3) provide a reason why the information is incorrect, and (4) state what the correction should be.

How are individuals notified of the procedures for correcting their information?

In addition to normal notification through the SORN process, field technicians provide correction procedures to individuals upon request.

If no formal redress is provided, what alternatives are available to the individual?

Individuals may contact their administrative point of contact to obtain access to their information.

List the privacy risks and mitigations related to redress.

Privacy Risk: The system information provided by participants is important to be accurate, as it has an impact on their program participation. Incorrect information may adversely affect the participant or other individuals, resulting in denial of service or incorrect payments.

Mitigation: Individuals are provided with access to their information electronically to check for accuracy of their submission(s). Additionally, program staff will verify submitted information with the individual as well as previously collected data.

Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

How is the information in the system/project/program secured?

WCIS employs a defense-in-depth strategy. The system is protected by a web application firewall and restrictive networking. The application server is configured using Center for Internet Security hardened images, and all components employ endpoint protection and real-time monitoring for malicious activity. Access to the system is role-based and requires multi-factor authentication for all accounts. All data transfer and storage utilize Federal Information Processing Standard (FIPS 140-2) compliant encryption.

What procedures are in place to determine which users may access the program or system/project, and are they documented?

Access to PII is determined by user role and restricted access. Access to PII is granted by appropriate legal authorities. Applicable users and roles are documented in the System Security Plan.

How does the program review and approve information sharing requirements?

Organizations outside of USDA request access to information, and a data sharing agreement is created and routed through the Grants and Agreements Office for review. The Grants and Agreements Office will ensure all stakeholders, including but not limited to, the FPAC Privacy Officer, a Senior Agency Official, and a receiving organization official, review and sign the agreement that lays forth the standards and rules for handling USDA PII.

Describe what privacy training is provided to users, either generally or specifically relevant to the program or system/project.

Annual organizational training, including USDA Information Security Awareness Training & Acknowledgment of Rules of Behavior, is mandatory for all federal and contractor staff working with WCIS.