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

Detail	Information
System/Project Name	Core Services (CS)
Program Office	Information Solutions Division
Mission Area	(FPAC)/Natural Resource Conservation Services (NRCS)
CSAM Number	2308
Date Submitted for Review	7/21/2025

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/Program Managers	Krystal Casey	000-000-0000

Abstract

Core Services (CS) supports USDA's Natural Resources Conservation Service (NRCS) programs. The Environmental Quality Incentives Program (EQIP) is NRCS' flagship conservation program that helps farmers, ranchers, and forest landowners integrate conservation into working lands. The CS shares and transmits the information collected to help support the Agency's mission and technology assets, while avoiding the need to manage multiple competing and overlapping functions. The PIA is being conducted because this system shares and transmits PII.

Overview

Core Services (CS) is owned by the information Solutions Division branch within USDA's NRCS. The business purpose of the information technology (IT) system is to share and transmit USDA application data and metadata between several USDA internal systems to include client applications, back-end databases and adjacent systems. This relates to NRCS's mission to provide conservation solutions so that agricultural producers can protect natural resources and feed a growing world. The system, which users include NRCS employees, was created to help NRCS see the value of common business processes and data in helping to reduce costs and lost resources attributable to redundant functions and duplicated efforts.

Roughly 1.4 million individuals are active and have an active case file within the Conservation Desktop application. Roughly 22,000 of those were active in the last year, whose data would have been shared and transmitted by the Core Services (CS) system during that time. Roughly 1.8 million customers are active in SCIMS2 and could be returned in search results. There are roughly 22,000 active non-USDA customers.

Core Services (CS) is currently comprised of 6 applications, which include (1) CS, (2) CS-API, (3) Conservation Resources (CR), (4) CPII, (5) Feature Flag Service (FSS) and (6) CDSI Services.

The legal authorities to operate the IT system include the following:

- Soil Conservation and Domestic Allotment Act (16 USC 590a et seq.)
- Food Security Act of 1985 (Public Law 99-198)
- Conservation Title of the Farm Bill (various sections across different farm bills).
- Environmental Quality Incentives Program (EQIP): Established under the Farm Security and Rural Investment Act of 2002 (Public Law 107-171).
- Conservation Reserve Program (CRP): Authorized under the Food Security Act of 1985 and subsequent farm bills.
- Conservation Stewardship Program (CSP): Established under the Food, Conservation, and Energy Act of 2008 (Public Law 110-246).

The completion of this PIA will not result in changes to business processes or technological changes.

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?

- Soil Conservation and Domestic Allotment Act (16 USC 590a et seq.)
- Food Security Act of 1985 (Public Law 99-198)
- Conservation Title of the Farm Bill** (various sections across different farm bills).
- Environmental Quality Incentives Program (EQIP): Established under the **Farm Security and Rural Investment Act of 2002 (Public Law 107-171).
- Conservation Reserve Program (CRP): Authorized under the Food Security Act of 1985 and subsequent farm bills.
- Conservation Stewardship Program (CSP): Established under the Food, Conservation, and Energy Act of 2008 (Public Law 110-246).

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: May 1, 2025
- Authorization Status: Authorized to Operate
- Authorization Status Date: December 1, 2023
- Authorization Termination Date: December 1, 2026
- Risk Review Completion Date: December 1, 2023
- FTPS 199 Classification of the System: Moderate

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

The following SORN covers CS: Natural Resources Conservation Service SORN-1.

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?

Identifying Numbers:

- Social Security Number
- Truncated or Partial Social Security Number
- File or Case ID Number
- Taxpayer Identification Number
- Business Taxpayer Identification Number (Sole Proprietor)
- Customer Identification Number

Biographical Information:

- Name (Including Nicknames)
- Business Mailing Address (Sole Proprietor)
- Ethnicity
- Business Phone or Fax Number (Sole Proprietor)
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Race
- Nationality
- Personal Email Address
- Business Email Address

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

Core Services may share or transmit Privacy information from the following databases:

- National Planning and Agreements Database (NPAD) Database – The system of record for conservation technical plans and practices, includes customer data for non-USDA customers. NPAD has views that provide access to the following which are sources of PII information:
- SCIMS2, a read-only copy of the USDA Farm Service Agency (FSA) Service Center Information Management System (SCIMS) Database – The system of record for NRCS client profile data.

The Service Center Information Management System (SCIMS), maintained by the Farm Service Agency (FSA) Farm Program Common Management System (FPCMS), is the database of customer information that is shared by the three Service Center Agencies, FSA, NRCS, and Rural Development. SCIMS is a repository for USDA business entity and conservation compliance information. Access to SCIMS customers allows the selection of customers for

Conservation Desktop processes and allows the most current customer information to be used on forms and documents. NRCS has a view of the SCIMS database and access to the data from SCIMS for NRCS users is via NPAD and through eAuthentication (eAuth). NRCS users do not have direct access to SCIMS. The landowners may provide information to SCIMS, which is the source of the PII. All information is obtained through a view of the database. CS does not modify or update any information in SCIMS.

How is the information collected?

Information is not stored on the Core Services platform; information only traverses it.

CS obtains landowner information from the SCIMS database copy, using the customer's SCIMS ID. NRCS users do not have direct access to SCIMS. All information is obtained through a database copy.

CS obtains customer information for non-USDA customers from NPAD using the customer's Client ID. Conservation Desktop manages non-USDA customer data.

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

N/A

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

The accuracy of information will be the responsibility of the NRCS client applications, including underlying systems, like SCIMS, and their System Owners (SOs).

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

No

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

N/A

What PII will be made available to the agency though the use of third-party websites?

N/A

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

Privacy Risk: Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Mitigation: Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

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.

CS obtains landowner information from the SCIMS database copy, using the customer's SCIMS ID. This allows the most current information to be on UI forms and used in documents. The PII attributes also support selection of the correct customer for use within consuming system processes. NRCS users do not have direct access to SCIMS. All information is obtained through a database copy.

Information about customers may be collected when they request brief technical assistance. This allows NRCS to gauge the extent of support they provide to farmers and ranchers. Customers that seek brief technical assistance may eventually request additional technical and financial assistance from NRCS and transition to being a USDA/SCIMS customer.

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: Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Mitigation: Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

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 prior to collection?

The CS system transmits and shares information and does not interact directly with the individuals that provide information. This is handled by FPCMS the source system.

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

This is handled by FPCMS source system and not handled by CS directly.

List the privacy risks and mitigations related to notice.

Privacy Risk: Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Mitigation: Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

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?

All records found in CS are retained for 10 years and deleted only after the information is no longer needed for administrative, legal, audit or other operational purposes.

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 Numbers are NC1-114-08-002 & NC1-114-83-01 which includes SCIMS interfaces.

List the privacy risks and mitigations related to data retention. Follow this format:

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

Mitigation: Data Retention Policy: Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes.

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?

The CS System shares and transmits USDA application data and metadata between several USDA internal systems to include client applications, back-end databases and adjacent systems.

The CS System receives API requests from

- Conservation Desktop (CD)/Conservation Assessment & Ranking Tool (CART)
- Farmers.gov

The CS System retrieves data from the NPAD database which includes views into data from SCIMS2 database.

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: Electronic transmission of the data is 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?

N/A

List the privacy risks and mitigations related to external information sharing and disclosure. Follow this format:

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.

Note: The CS System shares and transmits data but is not the system of record for the data. The answers here apply to the system of record and are included to provide clarity that there is redress for individuals.

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 FPAC FOIA Officer; to authenticate their identity and identity the records they request access to Core Services (CS).

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 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 a 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. Follow this format:

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?

The CS system is integrated with the agency's authorization system, zRoles, which manages roles for NRCS staff. In addition, to support Farmers.gov requests, the CS System is also integrated with FSA RAP (Representative Authority for Producers) system to ensure the requesting user is authorized to access the requested customer's information. Consumers identify the user and customer, where appropriate, for whom the call is being made which is used to retrieve the authorization information. Users must also be authenticated using the USDA eAuthentication system. Access to Core Services (CS) and Core Services API (CS-API) is also controlled using an API Gateway.

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 user and roles are documented in the System Security Plan.

How does the program review and approve information sharing requirements?

Any time organizations outside of USDA requests access to information, a data sharing agreement is created and routed through the Grants and Agreements Office for review. The Grants and Agreements Office ensure all stakeholders, to include, but not limited to the FPAC Privacy Officer, a Senior Agency Official, and receiving organization official, review and sign the data sharing 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 CS.