Privacy Impact Assessment

Core Service

Policy, E-Government and Fair Information Practices

- Version: 3.2
- Date: October 14, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA

United States Department
of Agriculture

Privacy Impact Assessment for the

Core Services

October 14, 2020

Contact Point

John Shideler
Program Manager, FPAC
970-295-5404

Reviewing Official

James Flickinger
Chief Information Security Officer, FPAC
United States Department of Agriculture
(816) 926-6010

Abstract

The Conservation Delivery Streamlining Initiative (CDSI) application suite of NRCS, including Core Services, helps the NRCS field staff and NRCS customers in delivering conservation services efficiently.

This PIA is being conducted to comply with Federal Information Security Management Act (FISMA) of 2014 (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101).

Overview

The Core Services project includes an initial list of over 200 candidate web services, which will be used to replace point-to-point connections from numerous legacy systems and will be designed to be scalable to support the growth of more services during the life of the system. Core Services includes several new components, as well as a re-architecture and re-development of existing services that are touched by, or interact with, CDSI.

Legal Authority: This system is regulated by privacy laws, regulations and government requirements, including the Privacy Act (5 U.S.C. §552a); the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101); the Paperwork Reduction Act of 1995 (44 U.S.C. §3501); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C.§3551 to §3559); Office of Management and Budget (OMB) Memos M-03-22, M-10-23, M-16-24, and M-17-12; and OMB Circular A-130, Appendix I.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

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

Core Services accesses the following information for Program Participants, Farmers, Ranchers and Producers:

- Full name or alias
- Street Address or email address
- SCIMS Customer ID that can be associated to a Social security number or tax identification number
- bank account numbers (last few digits only)
- case number (caseId, casename)

1.2 What are the sources of the information in the system?

Core Services may retrieve Privacy information from the following databases:

- National Planning and Agreements Database (NPAD) Database – The system of record for conservation technical plans and practices.
- NRCS Reference Tables (NRT) Database – The system of record for field office data and Document Management System (DMS) document types.
- USDA Farm Service Agency (FSA) Service Center Information Management System (SCIMS) Database – The system of record for NRCS client profile data.
- eContracts, econtractsLedger, eContractsPRT, FundManager, and Financial Management Modernization Initiative (FMMI) Databases – The system of record for ProTracts and FundManager data.
- SCIMS2 Database – The main source of core customer data which is then linked to other databases.

The Service Center Information Management System (SCIMS), maintained by FSA, Service Center Information Management System (SCIMS), CSAM ID # 1672, 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. This link allows the most current customer information to be printed on forms and letters. It also allows NRCS managers to generate reports on the race, sex, national origin, and disability of program applicants and participants.

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. Core Services does not modify or update any information in SCIMS.

1.3 Why is the information being collected, used, disseminated, or maintained?

Core Services uses the PII information obtained from the SCIMS database copy to associate a request to a specific client.

1.4 How is the information collected?

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

1.5 How will the information be checked for accuracy?

N/A. The accuracy of information will be the responsibility of the NRCS client applications and their System Owners (SO). The accuracy of information traversing through Core Services cannot be changed or updated.

The accuracy of PII obtained from SCIMS is not within the scope of Core Services. Core Services does not have the ability to update any information in SCIMS, nor does it have the ability to update the information in any other application database not maintained by NRCS.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The following regulations are applicable:

- Privacy Act (5 U.S.C. §552a)
- E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101)
- Paperwork Reduction Act of 1995 (44 U.S.C. §3501)

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There are moderate security concerns due to the amount of PII collected, processed, and traversed by the system. These risks are mitigated through Information Security Awareness Training and the implementation of controls discussed in Section 2.4.

Privacy risks are mitigated because access to the information is limited to appropriate NRCS personnel and partners through the use of the eAuth application, which provides user authentication for NRCS.

Other access requirements include the need for users to be on the USDA network backbone, using a Common Computing Environment (CCE) computer and via NRCS' role-based authorization.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Core Services does not directly collect any PII from any affected individual. Core Services receives API requests from various client applications and responds to the requests by performing business logic, running database queries, and using programmatic interfaces necessary to gather the requested information and will return the data to the user in JavaScript Object Notation (JSON) format.

2.2 What types of tools are used to analyze data and what type of data may be produced?

N/A - Core Services does not use data analysis tools; however, the data is formatted before being returned to the end user.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Core Services does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Core Services is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Core Services does not store PII; any PII stored is in the originating databases. The Core Services database is used to store administrative and transactional information for the services only.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Retention of application-specific data (in the originating databases) is required to meet business and organizational requirements for this information system. The risks associated with retaining application-specific information are mitigated by the controls discussed in Section 2.4.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Core Services shares and transmits USDA application data and metadata between several USDA internal systems to include client applications, back-end databases and adjacent systems. Core Services receives API requests from Conservation Desktop (CD), Mobile Planning Tool (MPT), and Conservation Client Gateway (CCG); Core Services also receives requests from RS and the IET, and retrieves information from NPAD, NRT, FSA SCIMS, eContracts, CRdb, IET_LMOD, and SCIMS2 databases to send back to the client applications.

In addition, Core Services also shares information with the following internal USDA systems:

- CA API Gateway – Used for threat protection, access control, and other sharedservices as defined during the architecture build out.
- DMS – Used for document storage and retrieval.
- eAuth – Used for authentication.
- zRoles – Provides active/disabled status for NRCS clients andentitlements/jurisdictions for NRCS employees.
- Geographic Information System (GIS) Web Services – Used to retrieve variousgeospatial map layers.

NRCS has access to a view of the SCIMS database. Access to the data is through established security rules via eAuth.

4.2 How is the information transmitted or disclosed?

The transmission of API requests and formatted data between the client applications and Core Services is accomplished by way of Port 443, HTTPS 4. Requests from outside the NRCS firewall are first received by the external-facing CA API Gateway appliance, serving as a single point of entry into the Core Services platform. In addition, the internal CA API Gateway directly services requests from within the agency firewall, for example the Conservation Desktop workstations or legacy systems that may call the Core Services application.

NRCS has access to a copy of the SCIMS database via replication. Access to the data is through established security rules via eAuth.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The eAuth and zRoles systems ensure that the proper authentication and authorization are granted so that only authorized individuals have access to the information.

Any residual risks are mitigated by the controls discussed in Section 2.4.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

N/A. Information is not shared with organizations external to the USDA.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

N/A. Information is not shared with organizations external to the USDA.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

N/A. Information is not shared with organizations external to the USDA.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Information is not shared with organizations external to the USDA. Any API requests that are received from the public-facing CA API Gateway will undergo an API filtering process before being passed onto the internal network. All API requests must have received user authorization from their client application to retrieve information from Core Services.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

Core Services is subject to the NRCS-1 SORN accessible at: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

6.2 Was notice provided to the individual prior to collection of information?

Core Services does not collect any information; this would be addressed by the system collecting the information.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

The information used by Core Services is based on the rules of the source database. Any PII information is obtained from the SCIMS system

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Any PII information used in Core Services is obtained from the SCIMS system. Members of the Public do not have access to this application. This item would be addressed by the system collecting the information.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Core Services is not responsible for eliciting consent for the use, or collection, of PII. The owners of the client applications are responsible for eliciting consent from its users. Any PII that is obtained from SCIMS.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Users of the client applications can request access to their information via the System Owner of the client application(s).

As published in SORN USDA/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

Any PII obtained from SCIMS would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Users of the client applications can request access to their information via the System Owner of the client application(s).

As published in SORN USDA/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

Any PII obtained from SCIMS would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

Users of the client applications can request access to their information via the System Owner of the client application(s).

As published in SORN USDA/NRCS-1: “Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.).”

Any PII obtained from SCIMS would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

Users of the client applications can request access to their information via the System Owner of the client application(s).

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Users of the client applications can request access to their information via the System Owner of the client application(s).

Any PII obtained from SCIMS would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

Residual privacy risks associated with the redress process for individuals are mitigated since individuals can use the relevant procedures discussed above to update their original public records.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

All API requests originate from a client application where the user will have already authenticated with e-Auth. Core Services will only need to validate that the user is authenticated successfully; Core Services will not perform authentication directly. The CA API Gateway will then query the zRoles system to verify that the requestor is permitted to access the service being requested. All users accessing Core Services will be logged in the Security Information and Event Management (SIEM) server.

8.2 Will Department contractors have access to the system?

Yes. Department contractors with a need-to-know will have access to Core Services as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Annual organizational Privacy Awareness Training is mandatory for all NRCS personnel. NRCS requires that every employee and contractor receive information security awareness training before being granted network and account access, per General Manual, Title 270, Part 409 - Logical Access Control and Account Management. Annual Security Awareness and Specialized Training is also required, per FISMA and USDA policy, and is tracked by USDA.

To remind users of their responsibilities (which they acknowledged during their Annual Security Awareness Training), the application reiterates that documents passed to DMS may contain sensitive information, and this information must not be disclosed to anyone unless the recipient has a direct need-to-know in the performance of their official duties.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. Core Services received an Authority to Operate (ATO) on 01/08/2018 which expires on 01/08/2021.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

NRCS complies with the FISMA of 2014. Assessment and Accreditation (A&A), as well as annual key control self-assessments and continuous monitoring procedures are implemented for Core Services per the requirements given in NIST SP 800-53 Revision 4.The system also provides technical safeguards to prevent misuse of data including the following:

- Confidentiality: Encryption is implemented to secure data at rest and in transit for Core Services [e.g., by Federal Information Processing Standards (FIPS)140-2 compliant HTTPS and end-user hard disk encryption]. The documents that are passed to, and maintained in, DMS are encrypted in transit.
- Integrity: Masking of applicable information is performed for Core Services(e.g., passwords are masked by eAuth).
- Access Control: Core Services implements least privileges and need-to-know to control access to PII [e.g., by Role-Based Access Control (RBAC)].
- Authentication: Access to the system and session timeout is implemented for Core Services (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: Logging is implemented for Core Services [there is a logging infrastructure including Application Audit Log Solution (AALS)]. Core Services logs events from various devices within its accreditation boundary to include web servers and database servers. NRCS logs data transactions from devices adjacent to the Core Services accreditation boundary to include the legacy databases and the CA API Gateway. Logged events will be stored in the NRCSSIEM server.
- Attack Mitigation: The system implements security mechanisms such as input validation.

Note: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5 and by the security controls discussed in Section 2.4. Remediation of privacy risks associated with internal/external sharing are addressed in Sections 4 and 5 respectively. Remediation of privacy risks associated with notice and redress are addressed in Sections 6 and 7 respectively.

Mitigation occurs through policies that address Separation of Duties (SOD) which ensures that system operators and system administrators have limited, if any, access to PII. In addition, NIST 800-53 Audit and Accountability (AU) audit controls are used to prevent data misuses.

All API requests originate from a client application where the user will have already authenticated with eAuth. Core Services will only need to validate that the user is authenticated successfully; Core Services will not perform authentication directly. The CA API Gateway will then query the zRoles system to verify that the requestor is permitted to access the service being requested. All users accessing Core Services will be logged into the SIEM server.

Core Services does not directly collect any PII from any affected landowner (i.e., member of the public), but Core Services does utilize PII within the system which is obtained from SCIMS, which is maintained by FSA (see Section 1.0 above). Any PII information is obtained from the SCIMS database, copied from the SCIMS system, which is maintained by FSA.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

Core Services is an NRCS application and is comprised of both front-end web applications and back-end compute/processing applications.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. Core Services utilizes Agency approved technologies and these technology choices do not raise privacy concerns.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

Yes. However, Core Services does not use third-party websites and/or applications.

10.2 What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

N/A. Core Services does not use third-party websites and/or applications.

10.3 What personally identifiable information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

N/A. Core Services does not use third-party websites and/or applications.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A. Core Services does not use third-party websites and/or applications.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A. Core Services does not use third-party websites and/or applications.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A. Core Services does not use third-party websites and/or applications.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A. Core Services does not use third-party websites and/or applications.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A. Core Services does not use third-party websites and/or applications.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A. Core Services does not use third-party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

N/A. Core Services does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A. Core Services does not use web measurement and customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Privacy risks are nominal. Core Services does not provide access, or link, to third-party applications. In addition, the system does not use web measurement or customization technology

Agency Responsible Officials

JAKE ZEBELL

Digitally signed by JAKE ZEBELL
Date: 2020.11.13 10:00:13 -07'00'

Jake Zebell
Core Services Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS

Digitally signed by LANITA THOMAS
Date: 2020.11.12 12:16:45 -05'00'

Lanita Thomas
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2020.11.05 12:20:24 -06'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture