Privacy Impact Assessment

Conservation Delivery Streamlining Initiative Conservation Desktop

Technology, Planning, Architecture, & E-Government

- Version: 3.0
- Date: October 12, 2011
- Prepared for: USDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

CDSI Conservation Desktop

August 19, 2011

Contact Point
Kathy Green
Branch Chief, USDA-NRCS-ITC
Information Technology Center
United States Dept of Agriculture
Natural Resources Conservation Service
2150 Centre Avenue, Building A
970-295-5647

Reviewing Official
Ray Coleman
Director of IT Security
United States Dept of Agriculture
Natural Resources Conservation Service
1400 Independence Ave. SW 20250; Rm. 6164-S
202-205-7712

Abstract

- NRCS Conservation Delivery Streamlining Initiative (CDSI) Conservation Desktop
- The primary purpose of the CDSI Conservation Desktop application is to provide streamlined financial assistance information regarding conservation programs to NRCS staff as well as provide an accessible set of information regarding conservation programs to the public.
- This Privacy Impact Assessment (PIA) is being conducted to comply with Federal Information Security Management Act of 2002 (FISMA) and the E-Government Act of 2002 (Public Law. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) Federal Law.

Overview

- Conservation Delivery Streamlining Initiative (CDSI) is a major application, owned by the United States Department of Agriculture (USDA), Natural Resources Conservation Service (NRCS).
- The primary purpose of the CDSI Conservation Desktop application is to provide streamlined financial assistance information regarding conservation programs to NRCS staff as well as provide an accessible set of information regarding conservation programs to the public. Although the information is related to financial data, there are no financial transactions that occur via the CDSI Conservation Desktop. NRCS staff will interact with a scheduled to-do list, also known as tasks, that may be assigned to an individual or their role via a web browser. Citizens and other users interact via the CDSI Client Gateway web application to view their profiles and request assistance. These assistance requests are turned into Tasks which are then viewable by NRCS staff within the CDSI Conservation Desktop FA Desktop web application. An internal user audience web application called CDSI Dashboard allows monitoring of business processes.

  The information provided is geospatial and tabular in nature. The primary purpose of each component is described below

  - CDSI CD FA Desktop: Via a web browser interface, the NRCS employee and affiliate users view a to-do list of tasks that are assigned directly to them or to their role. The tasks originate from the overall conservation process. Tasks arise from the financial assistance conservation process. Users are able to upload documents to a document management system via the web browser user interface. Access is through a web browser.

- CDSI CD Client Gateway: Create, modify, and validate assistance requests from clients. Access is through a web browser.
- CDSI Dashboard: Via a web browser interface, NRCS employees and contractors will monitor the health of the overall CDSI CD components.
- CDSI CD Logging System: Store and view system level trace log events. Used by other CDSI systems. No direct user access.
- CDSI CD Asynchronous Event Sequencing Engine System: Create, store, and execute sequences of task definitions. Used by other CDSI systems. No direct user access.
- CDSI CD Task Management System: Create, modify, and store metadata information regarding tasks to be performed. No direct user access.

- The application operates under the following legal authority: The Soil Conservation Act, April 1935.regulations per Federal Register /Vol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations. The conservation provisions in the Food, Conservation, and Energy Act of 2008 (2008 Farm Bill). Regulations per Federal Register /Vol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations; Federal Register / Vol. 74, No. 11 / Friday, January 16, 2009 / Rules and Regulations;, 7 CFR Part 652; 16 U.S.C. 590 a-f, q, q-1 and other applicable authorities. Circular No. A-97, “Rules and regulations permitting Federal agencies to provide specialized or technical services to State and local units of government under Title III of the Intergovernmental Cooperation Act of 1968 > Types of services that may be provided. > Technical information, data processing, communications and personnel management systems services which the Federal agency normally provides for itself or others under existing authorities.”

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?

1. **Financial**
   - Accounting Information Type
   - Payments Information Type - **(The NRCS *CDSI Conservation Desktop* application does not make payments. All payments are made via the National Finance Center (NFC)).**
   - Funds Control Information Type
   - Reporting and Information Information Type
2. **Natural Resources**
   - Water Resource Management Information Type
   - Conservation, Marine and Land Management Information Type
3. **General Information**
   - Refers to Business contact information of customers and partners (i.e., name, phone #, email address)

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

FSA SCIMS, NRCS Program and Application Data from ProTracts, and Microsoft Bing Maps Platform.

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

Data being collected by the CDSI Conservation Desktop application will be used to process NRCS grants.

1.4 How is the information collected?

Information is collected via secure internal web services. The exception to this is map images are retrieved (read only) from Microsoft Bing Maps Platform via public web services.

1.5 How will the information be checked for accuracy?

Client side validation and human user review process to validate data prior to committing to FSA (via FSA process).

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

- Federal Register /Vol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)

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

For the CDSI application, there is a risk that an un-authenticated user will gain access to the application.

Mitigation: Common mitigation is provided by the USDA-OCIO-eAuthentication application, which provides user Authentication for NRCS. When required by the application business, Role-based Access Control, granted through the NRCS Delegation of Authority and using eAuthentication to verify user authentication, the software utilities called 'ZRoles' or 'IASRoles' set application level permissions for access to the specific Child application. Other access requirements can include the need for users to be on the USDA network backbone, using a CCE computer.

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.

Data being collected by the CDSI Conservation Desktop application will be used to process NRCS grants.

- Example: The USDA Natural Resources Conservation Service (NRCS) provides technical and financial support via easements to help landowners with their wetland restoration efforts and purchase development rights to keep productive farms and ranchlands in agricultural uses. This support provides for the restoration of land and/or the purchase of land with the intent of doing restoration.

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

Custom internal tools (the project tools, FA Desktop, etc.) are utilized.

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

The Microsoft Bing Maps Platform supplies geospatial information including base map and image.

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.

This application is in compliance with the Federal Information Security Management Act of 2002 (FISMA), USDA Office of the Chief Information Officer (OCIO) Directives, and U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3 guidance. Security Certification and Accreditation (C&A) was completed for this application in 2011.

- Access Control (AC)
- Security Awareness and Training Policy and Procedures (AT)
- Identification and Authentication (IA)
- Media Protection (MP)
- Physical Access (PE)
- Personnel Security (PS)

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?

Data is not normally purged from the applications. It may be archived, as required by the sponsoring business. Per the NRCS System of Record Notice (SORN), “Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs”. Thus, PII information is retained indefinitely with the exception of financial data which is purged after session login.

The NRCS System of Record Notice is accessible at: http://www.ocio.usda.gov/NRCS-1.txt

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

Yes. SF-115 shall be submitted to NARA for approval. External approval has already been granted for records covered by the General Records Schedules (GRS). No external approval is required for the disposition of nonrecord materials. An informational copy of the SF-115, in both hard copy and electronic format, shall be provided to the Departmental Records Officer at the same time that the original is sent to NARA.

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

No records management (no NARA guidelines yet followed).
Risks may also include those related to technical disaster recovery. Human error such as leaked data exists. Hackers may intentionally attempt to break through system security.

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?

CDSI currently shares data with NFC via interaction with another application, Protracts and Fund Manager, and again, currently, does not share information with NFC directly. It is anticipated that in the future, CDSI will take over the bulk of interaction with NFC from these aforementioned applications (which are covered under a different PTA/PIA/C&A set).

The NRCS-to-FSA interaction via FSA SCIMS, with regards to PII, does not transmit PII, but the nature of FSA SCIMS data returns PII to NRCS, which is then not used in the CDSI application (it is not “read” by the CDSI system). The FSA SCIMS web service is an encrypted and controlled interaction.

4.2 How is the information transmitted or disclosed?

PII is not transmitted.

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.

Data will not be shared.

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?

Information is not shared externally to non-USDA organizations on a routine basis. In order to implement the confidentially requirements of Section 1619, NRCS has developed an "Acknowledgement of Section 1619 Compliance form for NRCS cooperators to sign, which legally binds them to comply with the confidentiality provisions set forth in Section 1619. Refer to NRCS Directive National Bulletin Title 130.9.3 – Acknowledgement of Section 1619 Compliance for Conservation Cooperators at http://directives.sc.egov.usda.gov/viewDirective.aspx?hid=25284

This Agreement form is available at: http://directives.sc.egov.usda.gov/25283.wba

Disclosure may be made to contractors or to technical service providers when a written authorization has been received by the agency from the owner, operator, producer or participant. Such disclosure shall be made subject to the purposes for which the contractor or technical service provider is hired.

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.

Yes. This is covered by the NRCS SORN "NRCS-1." Disclosure may be made to contractors or to technical service providers when a written authorization has been received by the agency from the owner, operator, producer, or participant. Such disclosure shall be made subject to the purposes for which the contractor or technical service provider is hired. System access is restricted to authorized NRCS employees

and conservation district employees working to assist with the implementation of natural resources programs. NRCS field employees are authorized to access system records of owners, operators, producers, or participants in their service are or outside of their service area if the owner, operator, producer, or participant has authorized access. Conservation district employees are authorized to access system records of their district owners, operators, producers, or participants in their service area or outside of their service area if the owner, operator, producer or participant has authorized access. Conservation district employees are authorized to access system records of their district owners, operators, producers, or participants only in their official capacity as district employees. In order to implement the confidentiality requirements of Section 1619, NRCS has developed an "Acknowledgement of Section 1619 Compliance" form for NRCS cooperators to sign, which legally binds them to comply with the confidentiality provisions set forth in Section 1619.

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

System access is restricted to authorized NRCS employees and conservation district employees working to assist with the implementation of natural resources programs. The electronic data retrieval system is secured by the USDA Common Computing Environment user authentication process and USDA eAuthentication login and password protection. Offices are locked during non-business hours.

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

The electronic data retrieval system is secured by the USDA Common Computing Environment user authentication process and USDA eAuthentication login and password protection. Offices are locked during non-business hours. Some applications may also have user roles using the NRCS zRoles or USDA ICAM EEMS (enterprise entitlement management system) systems.

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

Refer to Appendix A: USDA Natural Resources Conservation Service, Privacy Policy. This policy is accessible by individuals from any NRCS public website.

If the individual has eAuthentication approval, upon accessing the application, the USDA OCIO eAuthentication banner states:

**********WARNING**********

• You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

• Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

• By using this information system, you understand and consent to the following:

o You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.

o Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

o Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except USDA's Chief Information Officer.

****

Per the NRCS System of Record Notice (SORN) at http://www.ocio.usda.gov/NRCS-1.txt and Freedom of Information Act website at http://www.nrcs.usda.gov/about/foia/, General Manual Part 408, SUBPART C, 408.45 'Notice of Privacy Act System of Records - Owner, Operator, Producer, or Participant Files - USDA/NRCS – 1:

(6) Notification Procedure:
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, D.C. 20013, who will refer it to the appropriate field office. A request for pertaining to an individual should contain: name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.).

In order to implement the confidentiality requirements of Section 1619: 'Information Gathering' of the 2008 Farm Bill, NRCS has developed an "Acknowledgment of Section 1619 Compliance" form for NRCS cooperators (land owners, operators, and Technical Service Providers) to sign, which legally binds them to comply with the confidentiality provisions set forth in Section 1619.

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

Yes.

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

Yes. Individuals consent to the particular use of their information by becoming a participant in a specific NRCS conservation program. Participation is at the discretion of the individual. The NRCS program rules and regulations, which are explained to the individual, determine the specific information required to participate in the specific NRCS program(s) for which the individual enlisted.

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

Notice is provided via both the aforementioned banner and SORN. While more mitigation could take place, only non-PII data is collected. CDSI uses anonymous usage statistics via Google Analytics; non-PII data is collected via Google Analytics. This "non-PII data" is not inconsistent with 1.1 (registration information may be shown to participant and can be changed, then SCIMS would update the information) because PII is collected only for registration purposes and only NRCS staff/administrators (with background checks and training) have access to that PII.

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?

Individuals have access to their profile information. In turn, they may change their profiles via the U.I. update feature.

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

Information may be changed via a backend, formal process involving a "Farm Service Agency" (FSA) procedures.

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

Individuals may change their profiles via the update feature of the website. The update button is on the same page and adjacent to their information.

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

Individuals may correct inaccurate data via the permission ability to change their profiles.

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

Privacy risks are mitigated since only the individual has access to their profile—the public does not have access. System administrators would have security background checks.

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?

Role-based access control (RBAC) via application; database administrator (DBA) account via NRCS Operations.

8.2 Will Department contractors have access to the system?

Yes, both system administrators and system operators will have access. However, via separation of duties, data is better protected.

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

New USDA employee/contractor "on board" security training via AgLearn is required.

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

Yes, C&A has been completed. Now, CDSI is merely awaiting the authority to operate (ATO).

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

Separation of duties (mentioned in 8.2) applies. As such, a form of checks and balances exists which applies to the auditing process. Also, NIST 800-53 A.U. audit controls are used to prevent data misuses.

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?

Mitigation occurs through separation of duties policies which ensures both system operators and system administrators have limited, if any, access to PII. Identification numbers keep customer PII ephemeral. CDSI does not retain social security numbers. Also, NIST 800-53 A.U. audit controls are used to prevent data misuses.

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?

The system is comprised of 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.

The project utilizes Agency approved technologies and the technology choice does not raise security 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"?

CDSI interacts with one third-party website, Microsoft Bing Maps Platform. CDSI pulls read-only data from Microsoft Bing Maps Platform rather than pushing data out. Thus, no PII is exposed to or from third party Websites.

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

N/A, since no PII is exposed to or from third party Websites per 10.1.

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

N/A, since no PII is exposed to or from third party Websites per 10.1.

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

Based on USDA PII definition, intent exists only to collect non-PII data from third party Websites. This "non-PII data" is not inconsistent with 1.1 (registration information may be shown to participant and can be changed, then SCIMS would update the information) because PII is collected only for registration purposes and only NRCS staff/administrators (with background checks and training) have access to that PII.

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?

Based on USDA PII definition, intent exists only to collect Non-PII data from third party Websites.

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

N/A, since agency use of third party Websites only involves non-PII data.

If so, is it done automatically?

N/A, per above 10.6 answer.

If so, is it done on a recurring basis?

N/A, per above 10.6 answer.

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

With the focus on non-PII data, only CDSI system administrators and system operators.

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?

With the focus on non-PII data, 10.8 is not applicable.

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)?

No, per Section 10 above replies, PII is not involved such that no SORN modification is necessary.

10.10 Does the system use web measurement and customization technology?

No, the system does not use this technology.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A, per Section 10.10.

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, per Section 10.10.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A, per Section 10.10.

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. CDSI's focus is on non-PII data. However, data is always subject to human error. There is the unlikely event that data which falls within the PII definition may be erroneously engaged. The security/privacy training administrator/operator would dispose of such rarely encountered PII immediately. Disaster recovery related error may occur. This "non-PII data" is not inconsistent with 1.1 (registration information may be shown to participant and can be changed, then SCIMS would update the information) because PII is collected only for registration

purposes and only NRCS staff/administrators (with background checks and training) have access to that PII.

Responsible Officials

PM: Mat Keller, Component/Office: NRCS ITC

United States Department of Agriculture

Approval Signature

Ray Coleman

Digitally signed by Ray Coleman
DN: cn=Ray Coleman, o=USDA, ou=NRCS, email=ray.coleman@wdc.usda.gov, c=US
Date: 2011.10.13 09:36:02 -04'00'

Ray Coleman
Senior Official for Privacy
Director of IT Security
United States Dept of Agriculture
Natural Resources Conservation Service
1400 Independence Ave. SW 20250; Rm. 6164-S
202-205-7712