

Privacy Impact Assessment Conservation Measurement Tool (CMT) Application

Technology, Planning, Architecture, & E-Government

- Version: 2.0
- Date: June 7, 2013
- Prepared for: USDA OCIO TPA&E





Privacy Impact Assessment for the Conservation Measurement System

June 7, 2013

Contact Point

Deb May
USDA NRCS Fort Collins
970-518-7415

Reviewing Official

Lian Jin
Acting CISO
United States Department of Agriculture
(202) 720-8493

Abstract

The Conservation Measurement Tool (CMT) component is a planning tool that is invoked from within the ProTracts application (CMT cannot be used as a stand-alone application).

CMT evaluates Conservation Stewardship Program (CSP) applications using a point-based system to measure a relative environmental benefit.

A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the 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

The NRCS Conservation Measurement Tool (CMT) evaluates and ranks Conservation Stewardship Program (CSP) applications using a point-based system to measure a relative environmental benefit. The tool evaluates existing and proposed new activities to calculate conservation performance points that will be used for ranking and payment purposes. Each operation is evaluated based on the operation's merits. The CMT is size neutral, which means that similar operations (despite the size of each operation) have the same potential to accrue a similar number of points.

All scoring for the relative environmental benefit impact is measured by question, enhancement and/or conservation practice responses. Each measure is rooted in the Conservation Practice Physical Effects (CPPE) scoring tables using a numeric scoring system (e.g., -5 to +5). Points for twenty-eight identified micro resource concerns and eight macro resource concerns have been established nationally for each question and additional activity.

Each land use is evaluated independently to determine: program stewardship eligibility requirements met, land use annual payments, and/or supplemental payment (where applicable). The ranking score evaluation is an aggregate reflection of activities on all land uses.

CMT cannot be used as a stand-alone application, because CMT is a planning tool that is invoked from within the ProTracts application.

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?

- CMT uses and maintains contract data (containing PII) obtained from ProTracts.

- Note that CMT does not collect or disseminate PII from SCIMS directly.
- CMT uses web services to obtain this data from ProTracts using SCIMS ID.
- SCIMS PII is not stored within the application database (aside from Name, Address and SCIMS ID), noting that the application aggregates (i.e., displays) SCIMS PII within the application user interface.

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

- Natural Resources Conservation Service (NRCS). CMT uses web services to obtain SCIMS data from ProTracts, using SCIMS ID.
- Service Center Information Management System (SCIMS), from the Farm Service Agency (FSA)

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

- To facilitate compliance with financial requirements related to ranking of CSP applications.

1.4 How is the information collected?

- CMT uses web services to obtain this data from ProTracts using SCIMS ID.
- Data is not collected from any other third party sources.
- Data is not collected from customers by this application.

1.5 How will the information be checked for accuracy?

- The PII obtained from ProTracts is validated prior to it being provided to CMT. This PII data is trusted.

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.

- The only PII data in the application that poses privacy risks is the contract data obtained from ProTracts, including Name and associated transitory personal SCIMS data. Per the PTA, the following data elements are stored in the CMT

database: name, address, and SCIMS ID. However, NRCS has built in adequate security and privacy controls to minimize the residual risk. Privacy risks are reduced due to existence of security and privacy controls (see Section 1.7, 2.4 and 8.6).

- Privacy risks are mitigated because access to the information will be limited to appropriate NRCS personnel and partners by the use of the USDA-OCIO-eAuthentication application, which provides user authentication for NRCS. Role-Based Access Control (RBAC) provides access enforcement. Other access requirements include the need for users to be on the USDA network backbone, using a CCE computer.
Please see Section 2.4 and Section 8.6 for a further discussion of security controls that are in place to mitigate privacy risks.

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.

- The PII is required to facilitate compliance with financial requirements related to ranking of CSP applications, as described in the Overview.

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

- N/A – no tools are used to analyze PII data and no type of data is produced from the PII. The PII is used for contract information purposes only.

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

- N/A – no commercial or publicly available data is used.

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.
 - Access Control (AC)
 - Security Awareness and Training Policy and Procedures (AT)

- Physical Access (PE)
- Personnel Security (PS)
- System and Communication Protection (SC)
- System and Information Integrity (SI)

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?

- Application-specific information is retained while the application remains in production.
- Per NARA General Records Schedule 20, application-specific information has been authorized by the NRCS Records Manager for erasure or deletion when the agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes.
- 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, any PII information that is retained will be retained for sufficient periods of time (approximately 10 years) to ensure compliance with the Farm Bill and any other applicable legislation and regulations.

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 is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed in Section 1.7 and Section 2 above.

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?

- NRCS. PII information is only shared with the invoking application (ProTracts) via web service calls, for the purpose of ranking CSP applications. See question 1.7 which reflects authentication exists, as an enforcement mechanism, to ensure request is coming from a legitimate source.

4.2 How is the information transmitted or disclosed?

- N/A - PII information is not transmitted or disclosed internally.

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 privacy risks related to internal information sharing are minimal, given the minimal extent of PII information that may be transmitted or disclosed.
- Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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 - PII information is not transmitted or disclosed externally. See question 1.7 which reflects authentication exists, as an enforcement mechanism, to ensure request is coming from a legitimate source.

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 - PII information is not transmitted or disclosed externally.

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

- N/A - PII information is not transmitted or disclosed externally.

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

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

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?

- N/A – Limited, if any PII is collected from any individual by this application. PTA reflects “Name” and “Address.” SCIMS ID is outside the accreditation boundary of this application.

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

- N/A – Limited, if any PII is collected from any individual by this application. See 6.1.

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

- N/A – Limited, if any PII is collected from any individual by this application. See 6.1.

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 does not need to be provided to individuals. There is no risk that an individual would be unaware of “collection,” because no PII is collected from any individual by this application.

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?

- N/A – Applicable procedures to allow individuals to gain access to their information are maintained by SCIMS, which is the primary source of the PII used by CMT, which uses web services to obtain this SCIMS data from ProTracts using SCIMS ID.

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

- N/A – Applicable procedures for correcting inaccurate or erroneous information are maintained by SCIMS, which is the source of the PII used by this application.

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

- N/A – Applicable notification is provided by SCIMS, which is the source of the PII used by this application.

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

- N/A – See 7.3

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 associated with redress that is available to individuals are mitigated since individuals can use SCIMS procedures to update their original records in SCIMS.

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?

- Access to the CST application is determined via a valid eAuthentication ID and password (level II) on a valid “need to know” basis, determined by requirements to perform applicable official duties. The application has documented Access Control Procedures, in compliance with FISMA and USDA directives. See Section 2.4.

8.2 Will Department contractors have access to the system?

- Yes. Department contractors, with a need to know, will have access this application as part of their regular assigned duties.

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

- NRCS requires that every employee and contractor receives 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, and Privacy training, is also required, per FISMA and USDA policy, and is tracked by USDA.

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

- Yes. CMT was previously accredited as component of ProTracts, in 2010.

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

- NRCS complies with the “Federal Information Security Management Act of 2002” (FISMA). Certification and Accreditation, Annual Key Control self-assessments, and Continuous Monitoring procedures are implemented per law following the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3 for applications.

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?

- Specific privacy risks should be mitigated by specific security controls including enforcement of “need to know” and “least privilege” via RBAC discussed above, as well as the implementation of Department approved encryption measures for data at rest and data in transit (NIST 800-53 Revision 3 and using FIPS 140-2 compliant algorithms). Given the limited sensitivity and scope of the information retained, encryption is not implemented within the application database. However, all CCE laptops that access this application are protected with whole disk encryption to mitigate the risk of data at rest being lost or stolen. In addition, back-ups must be encrypted and application-specific data must be disposed of in accordance with NIST-compliant disposal methods when this data is no longer needs to be retained, per the Service Level Agreement with NITC. Another mitigation control is to implement Information Input Validation controls (e.g., to

include NIST 800-53 SI-10) according to industry best practices and NIST 800-53 controls specifications.

- Additional privacy risks associated with the sensitivity and scope of information that is maintained in this application are mitigated by the controls discussed in Section 2.4 and 8.5 above.

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?

- CMT is an application hosted on devices using common COTS hardware and software configured in accordance with USDA baseline configurations for servers and web portals. This application is not undergoing new development activities at this time.

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

- No. The project 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.

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

- N/A - 3rd party websites / applications are not used.

- 10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.**
- N/A, see 10.2.
- 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, see 10.2.
- 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, see 10.2.
- 10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?**
- N/A, see 10.2.
- 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, see 10.2.
- 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, see 10.2.
- 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, see 10.2.
- 10.10 Does the system use web measurement and customization technology?**
- N/A - The system 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, see 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. No PII is exposed to or from 3rd party Websites per Section 10.2 above.

Responsible Officials

deb.may2@usda.gov Digitally signed by deb.may2@usda.gov
DN: cn=deb.may2@usda.gov
Date: 2013.06.07 17:27:07 -06'00'

Deb May
NRCS

Date

United States Department of Agriculture

This signature certifies that the above PIA responses are provided to the best of my knowledge and understanding.

Approval Signature

michael.sheaver@usda.gov Digitally signed by michael.sheaver@usda.gov
DN: cn=michael.sheaver@usda.gov
Date: 2013.06.11 14:45:31 -04'00'

Mr. Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture

Date

This signature certifies that the PTA analysis and PIA determination due diligence has been conducted pursuant to Department guidance and NIST regulations.