

Privacy Impact Assessment Review of Open Obligations Tool (ROOT) Application

Technology, Planning, Architecture, & E-Government

- Version: 2.01
- Date: July 3, 2013
- Prepared for: USDA OCIO TPA&E



United States Department
of Agriculture





Privacy Impact Assessment for the Review of Open Obligations Tool (ROOT) Application

July 3, 2013

Contact Point

Kent Matsutani

Natural Resources Conservation Services

970-295-5477

Reviewing Official

Lian Jin

Chief Information Security Officer (Acting)

United States Department of Agriculture

(202) 720-8493



Abstract

This Privacy Impact Assessment (PIA) addresses the Review of Open Obligations Tool (ROOT) application.

The ROOT application provides a tool that is used on a quarterly basis to complete, review, and certify checklists that track open obligations that have been extracted from the Financial Management Modernization Initiative (FMMI).

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 Review of Open Obligations Tool (ROOT) audit application has been written to provide quarterly audit support to the Financial Management Division (FMD).

ROOT is used to filter data on all currently open NRCS obligations in FMMI. Once the NRCS user completes the ROOT determination for a specific obligation, any de-obligation or obligation must occur in the financial application that is set up for that particular transaction (e.g., ProTracts).

IMPORTANT: ROOT does not process any financial transactions. ROOT does not transmit any information to FMMI, and ROOT will never have an interface into FMMI.

The information received from FMMI is to be considered Sensitive but Unclassified (SBU).

Per the PTA, the FMMI information contains one element of Personally Identifiable Information (PII), which is a "Vendor Name" that can also be an individual's name in some circumstances. No PII information of any sort is directly collected from customers (i.e., the public) or the users of ROOT. ROOT logs the names of users who complete the checklists and make the determination for each obligation.

ROOT does not provide any user interface functionality that allows any information to be retrieved by reference to any type of personal identifier.

The system supports an approximate 3600 end users during a review/certification period. Only NRCS employees and NRCS Affiliates will be allowed to access the system. ROOT is a web-based application protected by Level 2 eAuthentication.

Authority to operate ROOT was previously provided via the ATO granted in 2010.

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?

- ROOT uses and maintains Personally Identifiable information (PII) information obtained from the Financial Management Modernization Initiative (FMMI).
- The PII that is used (displayed) by ROOT is strictly limited to the “Vendor Name” that is associated with open obligations. This “Vendor Name” is PII because it can be an individual’s name in some circumstances
- Note that ROOT explicitly does not directly “collect” any PII from any individual.

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

- ROOT receives information related to open obligations from FMMI.

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

- ROOT is used on a quarterly basis to complete, review, and certify checklists that track open obligations that have been extracted from FMMI.
- Note that ROOT explicitly does not directly “collect” any PII from any individual.

1.4 How is the information collected?

- N/A – ROOT does not directly “collect” any PII from any individual or any other third party sources.

1.5 How will the information be checked for accuracy?

- PII is checked for accuracy when ROOT is used on a quarterly basis to complete, review, and certify checklists that track the open obligations that have been extracted from FMMI.

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

- ROOT does not directly “collect” any PII from any individual.

- 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.

- ROOT does not directly “collect” any PII data from any individual.
- The only PII data in the application that poses nominal privacy risks is the “Vendor Name,” which can be an individual’s name in some circumstances as discussed above in this PIA.
- 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 Level 2 user authentication for NRCS.
- 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 that is displayed by ROOT is strictly limited to the “Vendor Name” that is associated with open obligations.

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 the PII that is maintained in ROOT.

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) as reflected in CSAM, USDA Office of the Chief Information Officer (OCIO) Directives, and National Institute of Standards and Technology (NIST) guidance, including applicable controls provided in these NIST Special Publication 800-53 Revision 3 control families:
 - Access Control (AC)
 - Security Awareness and Training Policy and Procedures (AT)
 - Identification and Authentication (IA)
 - Media Protection (MP)
 - 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.

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?

- N/A – ROOT does not “share” PII with any internal USDA organization.

4.2 How is the information transmitted or disclosed?

- N/A – ROOT does not “transmit” or “disclose” PII with any internal USDA organization.

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.

- N/A – ROOT does not “share” PII with any internal USDA organization.
- Privacy risks are minimal. The PII that is displayed by ROOT is strictly limited to the “Vendor Name” that is associated with open obligations.
- Any residual risks are mitigated by the controls discussed in Section 2 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.

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 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 – no notice is provided, because no PII is collected from any individual by this application.

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

- N/A – no PII is collected from any individual by this application.

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 – no PII is collected from any individual by this application.

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 – no procedures are required. The vendors associated with obligations are not allowed access to ROOT.

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

- N/A – no procedures are required. ROOT does not provide a means to update or change (i.e., “correct”) the Vendor Name that is associated with obligations.

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

- N/A – no notification is provided related to procedures to allow individuals to correct their PII, because no PII is collected from any individual 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.

- There are no privacy risks specifically associated with the redress process for this application. There is no risk that an individual would need to correct their PII.
- No PII is collected from any individual by this application.

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 ROOT 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 to ROOT 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?

- 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/Privacy Awareness and Specialized Training are also required, per FISMA and USDA policy, and this training is tracked by USDA.

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

- Yes.

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). Assessment and Accreditation, as well as annual key control self-assessments, and continuous monitoring procedures are implemented for this application per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3.
- NRCS complies with the specific requirements for “auditing measures and technical safeguards” provided in OMB M-07-16:
 - Encryption that is performed outside of the accreditation boundary of this application (e.g., by NITC) is discussed in Section 8.6 below. Given the limited sensitivity and scope of the information retained, this application does not encrypt any PII.
 - Masking of applicable information is performed outside of the accreditation boundary of this application (e.g., passwords are masked by eAuth). Given the limited sensitivity and scope of the information retained, this application does not mask any PII (e.g., “Vendor Name” is not masked).

- Controlled access to PII is implemented outside the accreditation boundary of this application (e.g., via multi-factor authentication for remote access). Given the limited sensitivity and scope of the information retained, this application does not control (limit) access to PII via RBAC, as discussed elsewhere in this PIA.
- Timeout for remote access is implemented outside of the accreditation boundary of this application (e.g., by eAuth), so this application does not need to implement timeout for remote access to PII due to inactivity.
- System audit logs are implemented outside of the accreditation boundary of this application. This includes internal audit logs that are used to ensure that administrative functions and activities are being logged and monitored (e.g., modifications, additions, and deletions of privileged accounts per the NITC SLA). Given the limited sensitivity and scope of the information retained, this application does not implement system audit logs related to PII integrity, nor does this application implement a Security Information and Event Management (SIEM) log management system.

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?

- ROOT explicitly does not “collect” or “share” (internally or externally) any PII.
- Specific privacy risks are mitigated by specific security controls including enforcement of “need to know” and “least privilege” via RBAC as discussed above, as well as the implementation of Department approved encryption measures for data at rest and data in transit (per NIST SP 800-53 Revision 3 and using FIPS 140-2 compliant algorithms).
 - To mitigate the risk of “data at rest” being lost or stolen, all CCE laptops that access this application are protected with whole disk encryption.
 - To mitigate the risk of “data in transit” being intercepted / stolen, this application uses HTTPS encryption.
 - Given the limited sensitivity and scope of the information retained, encryption is not implemented within the application database.
- All security controls provided by external information systems are reviewed and monitored for compliance annually by NRCS Security as a part of the NRCS continuous monitoring program. Security controls provided by external information systems are identified in SLAs and ISAs, including the following:
 - To mitigate the privacy risk of back-up media (e.g., tapes) being lost or stolen, all back-ups are encrypted per the NITC Service Level Agreement.
 - To mitigate the privacy risk of data being retained longer than required, application-specific data will be erased/deleted using NIST-compliant disposal methods (per the NITC Service Level Agreement) when the

agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes. See Section 3.

- Residual privacy risks associated with the sensitivity and the scope of PII that is maintained in this application are mitigated by the technical security controls discussed in Section 2.

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?

- This is a legacy application that is 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

kent.matsutani@usda.gov

Digitally signed by kent.matsutani@usda.gov
DN: cn=kent.matsutani@usda.gov
Date: 2013.07.03 08:33:57 -06'00'

Kent Matsutani/Project Manager Date
NRCS

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



7-3-2013

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.