Privacy Impact Assessment (PIA)

Review of Open Obligation Tool (ROOT)

Technology, Planning, Architecture, & E-Government

- Version: 3.1
- Date: August 19, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

Review of Open Obligation Tool (ROOT)

August 19, 2020

Contact Point

Sudha Sriparameswaran
FPAC Program Manager Supervisor
817-509-3260

Reviewing Official

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

Table of Contents

Abstract

The Review of Open Obligations Tool (ROOT) application is a system of the Natural Resources Conservation Service (NRCS). ROOT is a tool that is used on a quarterly basis to complete, review, and certify checklists that track open obligations extracted from Financial Management Modernization Initiative (FMMI) financial transactions. FMMI is an advanced, web-based core financial management system that complies with Federal accounting and systems standards. FMMI is being supported by the USDA Office of the Chief Financial Officer (OCFO), at the USDA National Finance Center.

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 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-FundManager).

ROOT does not process any financial transactions and ROOT does not transmit any information to FMMI. No PII is collected from customers (i.e., the public).

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?

ROOT is used to filter data on all currently open NRCS obligations in FMMI.

The PII that is used (displayed) by ROOT is limited to the Vendor Name associated with open obligations and could be considered PII because the Vendor Name could be an individual's name in some circumstances, used in conjunction with the FMMI Document Number, and/or the Legacy Obligation Number, and/or the Obligation Number associated with that vendor.

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. ROOT does not directly collect any PII from individuals.

1.4 How is the information collected?

PII is collected from the FMMI system. ROOT does not collect any PII directly.

1.5 How will the information be checked for accuracy?

The PII is checked for accuracy when ROOT is used on a quarterly basis to complete, review, and certify checklists that track open obligations. The Chief Financial Officer (CFO) conducts a review beginning in the third month of each quarter of the open balances. Completion of the review process actions will be monitored by the CFO.

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.

The only PII that poses nominal privacy risk is the vendor name, which can be an individual's name in some circumstances, used in conjunction with the FMMI Document Number, and/or the Legacy Obligation Number, and/or the Obligation Number associated with that vendor, as discussed above.

Privacy risks are mitigated because access to the information is limited to appropriate NRCS personnel and partners through the use of the eAuthentication (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.

Please see Sections 2 and 8 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.

ROOT is used on a quarterly basis to filter data on all currently open NRCS obligations extracted from FMMI to complete, review, and certify checklists that track open obligations extracted from 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.

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

N/A. Data is not analyzed.

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

N/A. ROOT does not use commercial or publicly available data.

2.4 <u>Privacy Impact Analysis:</u> 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 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?

Application specific information is retained while the application remains in production. For ROOT, the retention period may vary depending on business purpose, but typically is no longer than 25 years.

All information contained will be retained in compliance with NARA Guidelines, which vary on average in years from less than one year to more than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017.

Per the NRCS-1 System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs."

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

Yes. Per NARA Code of Federal Regulations - 36 CFR 1220, Subchapter B – Records Management and USDA OCIO Department Regulation 3080-001 accessible at: http://www.ocio.usda.gov/document/departmental-regulation-3080-001

NARA Approval: NARA approval is required for all official records schedules. 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 non-record 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.

Electronic Records: Electronic records should be scheduled in the context of entire information systems, along with appropriate documentation and related indexes, and provide the necessary elements:

- *All input records or source documents.*
- *All information recorded on electronic media.*
- *All output records.*
- *The documentation associated with the system.*
- *Any related indexes.*

As with audiovisual and microform records, permanent electronic records should not be proposed for long-term storage at Federal records centers but should be transferred directly to the National Archives.

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

The primary privacy risk is that a data breach could result in the release of information on vendors. This is mitigated by limited access to the data, nonportability of the data and controlled storage of the data located in controlled facilities.

Retention of application-specific data 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?

ROOT obtains information related to open obligations from FMMI; however, ROOT does not share PII with any internal USDA organizations.

4.2 How is the information transmitted or disclosed?

ROOT is used to filter data on all currently open NRCS obligations in FMMI.

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.

For administrator access, 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 external organizations.

5.2 Is the sharing of Personally Identifiable Information (PII) outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a System of Records Notice (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 external organizations.

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

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

N/A. Information is not shared with external organizations.

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

Privacy risks are mitigated by not sharing information with organizations external to the USDA. Any residual risks are mitigated by the controls discussed in Section 2.4.

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?

Yes. This application 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?

Yes. The NRCS Privacy Policy is published on the USDA website and the privacy policy for FMMI which is published on the USDA National Finance Center website.

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

No. PII is only obtained from FMMI.

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

No. PII is only obtained from FMMI.

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.

Notice is given via the privacy policy for FMMI which is published on the USDA National Finance Center website.

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?

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.)."

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

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.)."

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

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.)."

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

N/A. Refer to Section 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.

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.)."

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?

Administrative access to ROOT is determined via a Level 2 eAuth ID and password on a valid need-to-know basis, determined by requirements to perform applicable official duties. ROOT has documented AC Procedures, in compliance with FISMA and USDA directives. Refer to Section 2.4 for further information.

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?

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 Document Management System (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 (C&A) been completed for the system or systems supporting the program?

Yes. ROOT received an ATO on 12/07/2017.

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 ROOT 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 ROOT [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 ROOT (e.g., passwords are masked by eAuth).*
- *Access Control: ROOT 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 ROOT (e.g. by eAuth and via multi-factor authentication for remote access).*
- *Audit: Logging is implemented for ROOT [there is a logging infrastructure including Application Audit Log Solution (AALS)]. ROOT 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 ROOT accreditation boundary to include the legacy databases and the CA Application Programming Interface (API) Gateway. Logged events will be stored in the NRCS Security Information and Event Management (SIEM) 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 <u>Privacy Impact Analysis:</u> 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.

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?

ROOT is an NRCS application hosted on devices using Commercial-off-the-Shelf (COTS) hardware and software configured in accordance with USDA baseline configurations for servers and web portals.

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

No. ROOT 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 Technologies" 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 third-party websites and/or applications?

N/A. ROOT 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 third-party websites and/or applications?

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

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

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

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

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

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

N/A. ROOT 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 third-party websites and/or applications?

N/A. ROOT 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 third-party websites and/or applications be shared - either internally or externally?

N/A. ROOT 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 third-party websites and/or applications require either the creation or modification of a SORN?

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

10.10 Does the system use web measurement and customization technology?

N/A. ROOT 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. ROOT 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 third-party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

ROOT does not use third-party websites and/or applications. In addition, the system does not use web measurement or customization technology.

Agency Responsible Official

ANGELA SIEG

Digitally signed by ANGELA SIEG
Date: 2020.09.25 10:45:08 -05'00'

Angela Sieg
ROOT Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS

Digitally signed by LANITA THOMAS
Date: 2020.11.03 13:25:46 -05'00'

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

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2020.10.23 08:52:00 -05'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture