Privacy Impact Assessment

Review Open Obligation Tacking (ROOT) audit application

Revision: 1.1

Natural Resources Conservation Service

Date: October 2009

Document Information

Owner Details	
Name	Frank Geter
Contact Number	(970) 295-5540
E-mail Address	Frank Geter@ftc.usda.gov

Revision History			
Revision	**Date**	**Author**	**Comments**
1.0	13 November 2008	Ray Coleman	Initial Draft
1.1	8, October 2009	Barbara Pursley	Updated document contact information

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**

Table of Contents

DOCUMENT INFORMATION II

TABLE OF CONTENTS III

1 SYSTEM INFORMATION 1

2 DATA INFORMATION 2

2.1 Data Collection 3

2.2 Data Use 4

2.3 Data Retention 6

2.4 Data Sharing 6

2.5 Data Access 7

2.6 Customer Protection 8

3 SYSTEM OF RECORD 9

4 TECHNOLOGY 9

5 COMPLETION INSTRUCTIONS 10

1 System Information

System Information	
Agency:	Natural Resources Conservation Service
System Name:	Review Open Obligation Tracking (ROOT)
System Type:	☐ Major Application ☐ General Support System ☒ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	The Review of Open Obligations Tool (ROOT) application provides NRCS employees a tool for data entry and tracking, recording and certifying open obligations on financial transactions from FFIS, ProTracts and Fund Manager. In November 2008 ROOT was developed to support a one-time audit of NRCS program and financial transactions. The audit focused on transactions completed during the first quarter of Fiscal Year 2009. The audit was completed between November 20th and December 31, 2008. (approximately 185,000 obligation documents with a total dollar value of over $3.2 billion). In February 2009 – The NRCS CIO and CFO determined the ROOT application should be enhanced to support long-term audit of NRCS financial transactions on a quarterly basis, beginning with second quarter Fiscal Year 2009 data (March 2009). Additionally, ROOT is a web-based application protected by eAuthentication. Only NRCS employees and NRCS Affiliates will be allowed access to the system. The system will track which NRCS employee answered each question (user name, eauth id, and date/time stamp) and anytime a record is saved to the database an audit log will be written. The system supports approximately 3600 end-users during a quarterly review/certification period. The information contained in the FFIS is considered sensitive but contains no Personally Identifiable Information (PII).
Who owns this system? (Name, agency, contact information)	Frank Geter, Development Branch Chief, USDA-NRCS, Frank.Geter@ftc.usda.gov, (970) 295-5540
Who is the security contact for this system? (Name, agency, contact information)	Chuck Hart, Information System Security Manager, USDA-NRCS, Chuck.Hart@ftc.usda.gov, (970) 295-5550
Who completed this document? (Name, agency, contact information)	Ray Coleman, Systems Security Analyst, USDA NRCS Contractor, ray.coleman@ftc.usda.gov, 970-2955-5570.

2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	**Categories of Data** **(Data type are derived from NIST SP 800-60)** **Program Monitoring**: • Program Monitoring involves the data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies. **Personal Identity and authentication:** • Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. **Travel:** • Travel involves the activities associated with planning, preparing, and monitoring of business related travel for an organization's employees. **Funds Control:** • Funds Control includes the management of the Federal budget process including the development of plans and programs, budgets, and performance outputs as well as financing Federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other financing mechanisms. Funds control management includes the establishment of a system for ensuring an organization does not obligate or disburse funds in excess of those appropriated or authorized. **Reporting and Information:** • Reporting and Information includes providing financial information, reporting and analysis of financial transactions. Financial reporting includes the activities necessary to support: management's fiduciary role; budget formulation and execution functions; fiscal management of program delivery and program decision making; and internal and external reporting requirements.

No.	Question	Response
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	☐ Yes ☒ No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	☒ Yes ☐ No
4	Sources of the data in the system.	Source of data will be the FFIS and NRCS employees
4.1	What data is being collected from the customer?	N/A, data will not be collected from customers (Public)
4.2	What USDA agencies are providing data for use in the system?	The National Finance Center (NFC) and the Natural Resources Conservation Service
4.3	What state and local agencies are providing data for use in the system?	N/A, data will not be collected from any state and local agencies
4.4	From what other third party sources is data being collected?	N/A, data will not be collected from any third party sources
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	☒ Yes ☐ No – If NO, go to question 6. Data will be collect from NFC
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	N/A, data will not be collected from customers (Public)
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	State Conservationist will be responsibility for ensuring data is verified for accuracy, relevance, timeliness, and completeness.
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	The ROOT application will inherit the data collection controls from NFC and FFIS. ROOT DBA performs manual validation on data extracts.

2.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	N/A, data will not be collected from customers (Public)
7	Will the data be used for any other purpose?	☐ Yes ☒ No – If NO, go to question 8.

No.	Question	Response
7.1	What are the other purposes?	
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President	☒ Yes ☐ No
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	☐ Yes ☒ No – If NO, go to question 10.
9.1	Will the new data be placed in the individual's record (customer or employee)?	☐ Yes ☐ No
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	☐ Yes ☐ No
9.3	How will the new data be verified for relevance and accuracy?	
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	N/A, data will not be collected from customers (Public)
11	Will the data be used for any other uses (routine or otherwise)?	☐ Yes ☒ No – If NO, go to question 12.
11.1	What are the other uses?	None
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	☐ Yes ☒ No – If NO, go to question 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	
13	Are processes being consolidated?	☐ Yes ☒ No – If NO, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	☐ Yes ☒ No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	
14.2	What are the procedures for purging the data at the end of the retention period?	
14.3	Where are these procedures documented?	
15	While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	Data will be retained within ROOT application as long as a current obligation is open. Once and obligation is closed all information will be archived at management discretion.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No

2.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	☐ Yes ☒ No – If NO, go to question 18.
17.1	How will the data be used by the other agency?	
17.2	Who is responsible for assuring the other agency properly uses the data?	
18	Is the data transmitted to another agency or an independent site?	☐ Yes ☒ No – If NO, go to question 19.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	
19	Is the system operated in more than one site?	☐ Yes ☒ No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	• State Conservationist • District Conservationist • Support Staff • Senior Executive Staff • Application administrators • ITC application support staff
21	How will user access to the data be determined?	Access to the ROOT application is determined via a valid eAuthentication ID and password (level II) and a valid need to know
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☐ Yes ☒ No
22	How will user access to the data be restricted?	Access to the ROOT application will be restricted user with a valid eAuthentication user ID and password (level II) and a valid need to know
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No The ROOT application uses eAuthentication, auditing and USDA warning banner to detect and deter browsing and unauthorized user access.
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	☒ Yes ☐ No

2.6 Customer Protection

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	NRCS
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	If incident response assistance is needed Customers and employees can contact the NRCS Security Response Team via the following numbers: • Lost and Stolen equipment NRCS 800 number (1-888-926-2373) and/or e-mail address (nrcs.security@usda.gov). • Personal Identifiable Incidents – 877-744-2968 (PII-2YOU) • NRCS/CD - (202) 757-8111 or (703) 200-3008
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	☒ Yes – If YES, go to question 27. ☐ No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	
27	Consider the following: ▪ Consolidation and linkage of files and systems ▪ Derivation of data ▪ Accelerated information processing and decision making ▪ Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	☐ Yes ☒ No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	
28	How will the system and its use ensure equitable treatment of customers?	N/A, data will not be collected from customers (Public)
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	☐ Yes ☒ No – If NO, go to question 30
29.1	Explain	

3 System of Record

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	☐ Yes ☒ No – If NO, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov.)	
30.3	If the system is being modified, will the SOR require amendment or revision?	☐ Yes ☐ No

4 Technology

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?	☐ Yes ☒ No – If NO, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	

5 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE FOR CYBER SECURITY.

Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Review Open Obligation Tool (ROOT) Audit Tools

(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

Frank Geter

System Manager/Owner
OR Project Representative
OR Program/Office Head.

Date

Agency's Chief FOIA officer
OR Senior Official for Privacy
OR Designated privacy person

Date

Agency OCIO

Date