Privacy Impact Assessment
Receipt for Services (RFS)

Technology, Planning, Architecture, & E-Government

- Version: 1.10
- Date: September 2, 2014
- Prepared for: USDA OCIO TPA&E

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

Receipt for Services (RFS)

2 September 2014

Contact Point
Matthew Keller
Natural Resources Conservation Service
970-295-5591

Reviewing Official
Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture
202-720-8493

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

The Receipt for Services (RFS) is a system of the Natural Resources Conservation Service (NRCS).

RFS system is specifically designed to allow NRCS, FSA and RD employees to provide a receipt to customers for any service provided by USDA to the customer. The 2014 Farm Bill language requires that a receipt be provided to USDA customers, unless they deny the receipt.

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 overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

The Receipt for Services System (RFS) is a system of the Natural Resources Conservation Service (NRCS).

The purpose of the Receipt for Services (RFS) application is to meet a 2014 Farm Bill requirement passed by Congress that provides for a receipt to be issued for any service or denial of service from USDA agencies. This receipt is required to be provided on the date of service to all customers unless they elect not to receive it. This changes the current process because the Farm Bill verbiage requires the receipt to be provided unless the customer opts out, whereas prior to the 2014 Farm Bill, the customer needed to specifically request the receipt.

The USDA employee collects minimal PII information to generate and send the customer a receipt for services. The PII information collected and maintained by RFS includes contact information for customers who request services from NRCS, RD, or FSA. The information is shared by employees of NRCS, RD, and FSA.

The PII information maintained by RFS is used to manage generate a receipt and track the number and type of services requested by office.

RFS maintains the minimal contact information (name, address and email) PII in the RFS application.

The RFS application is seeking Authority to Operate in 2014.

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?

- The PII that is collected, used and maintained by RFS includes contact information for customers who receive services. It may specifically include: name, street address, email address and SCIMS ID (owned by FSA).
- RFS stores the receipt address, if provided. It is not the official repository of that information; SCIMS is,
- RFS does not disseminate PII information to any other system. It calls into SCIMS for customer address and email, but does not disseminate that information to another system.

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

- PII data (customer email and/or address) are brought into RFS from the SCIMS search.
- RFS does not process any financial transactions, and will never share any type of PII with FMMI.

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

- The information is collected, used and maintained in order to provide a receipt to the customer and determine the number and type of services by office.
- RFS does not disseminate PII information to any other system.

1.4 How is the information collected?

- PII data is collected by NRCS personnel into forms.

1.5 How will the information be checked for accuracy?

- Information in RFS is reviewed for accuracy and is verified through manual review and comparison with existing agency data throughout the approval process. This is done by NRCS personnel who have the requisite knowledge and responsibility for the data.
- The accuracy of PII obtained from SCIMS is not within the scope of RFS. RFS does not have the ability to update any information in SCIMS.

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

- RFS does not directly "collect" any PII from any landowner. (Entered by employee.)
- 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.

- RFS does not directly "collect" any PII from any landowner.
- The only PII data in the application that poses privacy risks is the minimal amount of PII that is used to provide a receipt to landowners. (Name, and mail or email address.) This is discussed in the PIA Overview and Section 1.1.
- Privacy risks are mitigated because access to the information will be limited to appropriate USDA employees by USDA-OCIO-eAuthentication application, which provides user authentication for NRCS. USDA employees of NRCS, FSA, and RD have access to RFS. Access to SCIMS is outside the

accreditation of RFS. If they do not have access to SCIMS, then SCIMS will deny them access.
- 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.

- This information is used to provide receipts to customers and determine number and types of service by office.

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

- N/A – RFS does not use any type of tools to analyze PII. RFS only produces summary reports for number and type of service by office. No PII data is 'produced' for analysis and PII data is not manipulated or reformatted. PII is only used to generate the receipt.

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

- N/A – RFS does not use commercial or publicly available data.

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)
  - Audit and Accountability (AU)
  - Security Awareness and Training Policy and Procedures (AT)
  - Identification and Authentication (IA)
  - Media Protection (MP)

- Physical Access (PE)
- Personnel Security (PS)
- Risk Assessment (RA)
- 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 in the RFS database. Per NARA General Records Schedule 20, CPD 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 – or after three (3) years from when the information was originally collected.

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.

- The primary privacy risk is that a data breach could result in the release of information on members of the public. This is mitigated by limited access to the data, non-portability of the data and controlled storage of the data in controlled facilities.
- 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 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?

- RFS information is shared between NRCS, RD and FSA within the USDA organization. In many USDA offices there is one NRCS employee and one FSA employee co-located in an office. In such a scenario if the NRCS employee is out sick or is working in the field, then the FSA employee would typically provide basic NRCS information and assistance to customers who may visit the office. In this scenario the FSA employee would provide the service and would generate the receipt for NRCS. Per the 2014 Farm Bill NRCS, RD, and FSA are required to provide receipts to customers, unless the customer declines.

4.2 How is the information transmitted or disclosed?

- N/A – NRCS, RD, and FSA will use the RFS application to provide receipts.

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 PII information is minimal.
- Privacy risks are mitigated by limiting access to authorized personnel via the eAuthentication application.
- 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?

- PII information is not transmitted or disclosed to external organizations. A receipt that may contain minimal PII is generated by the employee and provided to the customer identified in the receipt.

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.

- Minimal contact information (name, address, email) is collected. It is provided only to the customer.
- This information is covered by the following SORNs:
  - NRCS-1
  - FSA-2
  - FSA-14
  - RD-1

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.

- PII information is not transmitted or disclosed externally. Privacy risks are mitigated by virtue of NOT sharing PII with organizations external to USDA.
- 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?

- RFS provides receipts for programs or functions that USDA already offers to customers. In general the system doesn't collect any new data in order to generate a receipt and customers may be allowed to opt out of obtaining a receipt from USDA.

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

- Yes. Receipts can be generated under the name "Guest". Furthermore, the contact information (street address, zip, email) are always optional information for the receipt.

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

- The customer can decide whether or not they want a receipt for services.

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.

- Because no PII is collected from any individual landowner by this application, "Notice" does not need to be provided to any landowners. Minimal PII is obtained from SCIMS, not landowner.
- There is no risk that any landowner would be unaware of "collection," because a receipt cannot be mailed or emailed without contact information.

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 customers are not allowed to gain access to RFS, so any PII information in RFS is not directly available to the customers (i.e., members of the Public) via this application.
- Note that the applicable procedures to allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS (owned by the Farm Service Agency), which is the source of some of the PII used by this application. An individual may make a request to correct information through RFS. However, any actual information correction takes place in SCIMS.

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

- N/A – No procedures are required. The customers are not allowed to gain access to RFS, so any PII information in RFS is not directly available to them

(i.e., members of the Public) to update or change (i.e., "correct") any inaccurate or erroneous PII information.

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

- N/A – no notification is provided related to procedures to customers to correct their PII, because customers are not allowed to gain access to RFS. – See 7.1.

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

- N/A – See 7.1.

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 a customer would need to correct their PII, because the PII is used exclusively to provide them with a receipt.
- Residual privacy risks associated with the redress process for individual landowners 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?

- Access to the RFS 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?

- No.

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.
- For all three agencies (NRCS, RD, and FSA), Annual Security 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?

- RFS is seeking an Authorization to Operate (ATO) via an A&A that is currently in progress, to be completed in 2014.

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.
- NRCS complies with the specific requirements for "auditing measures and technical safeguards" provided in OMB M-07-16:
    - Confidentiality: Encryption is implemented in transit for this application (e.g., by FIPS 140-2 compliant HTTPS and end-user hard disk encryption.
    - Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).
    - Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC). The USDA HR systems populate employee status in the eAuth record. We obtain and use this value from the eAuth record in order to grant access. The employee must also be from NRCS, FSA, or RD.
    - Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
    - Audit: Logging is implemented for this application (e.g. by logging infrastructure).
    - Attack Mitigation: The system implements security mechanisms such as input validation.

- Encryption that is performed outside of the accreditation boundary of this application is discussed in Section 8.6 below. Given the limited sensitivity and scope of the information retained, this application does not encrypt any PII in the application database.
- 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., the "landowner's 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 eAuthentication 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.

Notice: For the privacy notice control, please see Section 6 which addresses the notice. For the privacy redress control, please see Section 7 which addresses redress.

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?

- RFS explicitly does not directly "collect" any PII from any landowner, or "share" (internally or externally) any PII, but does utilize PII within the system which is obtained from other sources (see Section 1.0 above). Data extracts containing PII are not regularly obtained from the system; therefore, privacy risk from this area is limited and addressed through IT Data Extract process controls.
- Since the RFS does not share any information with other systems, 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 above. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5 respectively.

- The documents that are passed to and maintained in RFS are encrypted in transit. PII information can be shared back to the customer via the receipt.

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?

- RFS is an NRCS GOTS application that is seeking an Authorization to Operate (ATO), as discussed in Section 8.4.

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 - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

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

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

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 - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

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 - 3rd party websites / applications are not used.

10.10 Does the system use web measurement and customization technology?

- No. 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 <u>Privacy Impact Analysis</u>: 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. RFS does not provide access or link to 3rd Party Applications. In addition, the system does not use web measurement and customization technology.

Responsible Officials

Matthew Keller — Date 9/3/2014
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

Mr. Lian Jin — Date 9/3/2014
Acting Chief Information Security Officer
United States Department of Agriculture
This signature certifies that the PTA analysis and PIA determination due diligence has been conducted pursuant to Department guidance and NIST regulations.