Privacy Impact Assessment

Electronic Forms (eForms)

Rural Development (RD)

- Date: July 18, 2016
- Prepared for: RD

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	07/18/16	ISSS/SN	Transitioned to new template

Abstract

eForms is a web-based system created to lessen the public paperwork burden mandated by the Paperwork Reduction Act. eForms gives customers, producers, partners, and others access to forms and account information related to USDA programs. eForms consists of the following modules:

- **Forms:** Portal that allows public access to forms for FSA, GIPSA, and RD. Forms can only be view and printed without an eAuth ID; however, to submit a form an eAuth ID is required. Public Forms Search Site allows for the search and retrieval of public burden forms used by FSA, GIPSA, and RD. To be able to save forms Level 2 eAuth is required. http://forms.sc.egov.usda.gov
- **FormsAdmin** is a service center application that allows employees to retrieve forms/packages from customers who submit from MyForms. Level 2 eAuth protected web application providing FSA, GIPSA, and RD Employee processing of electronic service requested submitted through MyForms. https://formsadmin.sc.egov.usda.gov
- **MyForms:** Web application that allows public access (with eAuth ID) to access for FSA, GIPSA, and RD. Forms can be saved and submitted electronically to service centers. Public facing Level 2 eAuth protected web application providing electronic service request submission to federal servicing offices. https://myforms.sc.egov.usda.gov

  USDA employees collect, process, generate and store PII in the form of Borrower and Management Agent Identification Numbers, Social Security Number (SSN), debt payment information, client names, lender names, and addresses as well as the employee's Name, eAuth ID, phone numbers, duty station and agency.

Overview

eForms is a web-based system created to lessen the public paperwork burden mandated by the Paperwork Reduction Act and as part of the regulatory reform efforts to increase their use of electronic means of information collection and, where feasible, to decrease the frequency of reporting by the public by 50%. eForms gives customers, producers, partners, and others access to forms and account information related to USDA programs. After activating their account, customers may complete and submit documents online to local USDA Service Centers or Area Offices.

eForms allows for the search and retrieval of public burden forms used by FSA, GIPSA, and RD.

- **FormsAdmin** is a Level 2 eAuth protected web application providing FSA, GIPSA, and RD Employee processing of electronic service requested submitted through MyForms.
- **MyForms** is a Level 2 eAuth protected web application providing electronic service request submission to federal servicing offices.

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?

Forms, FormsAdmin, MyForms:

Customer Information: Borrower and Management Agent Identification Numbers, SSN, debt payment information, client names, lender names, and addresses.

Employee Information: Name, eAuth ID, phone numbers, duty station and agency.

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

Forms, MyForms

County Servicing Offices for FSA, GIPSA, and RD programs.

FormsAdmin

Internal RD servicing offices employee names are added to Forms Admin to administer and review the information in MyForms

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

Forms, FormsAdmin, MyForms: provide an electronic service for the customer

The information is collected to provide an electronic service for the customer per the Paperwork Reduction Act and Section 10708 of the 2002 Farm Bill.

1.4 How is the information collected?

Forms, MyForms: electronic interactions to County Servicing Offices.

FormsAdmin: Users are entered via RD internal secure application

1.5 How will the information be checked for accuracy?

Forms, FormsAdmin, MyForms: Manual inspection of electronic form information by authorized USDA Service Center employees is leveraged to verify accuracy of that data set. Other system data sources are viewed as authoritative sources and maintain a separate verification process for the data they provide.

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

Paperwork Reduction Act and Section 10708 of the 2002 Farm Bill.

Consolidated Farm and Rural Development Act (7 U.S.C. 1921 et. seq.); and Title V of the Housing Act of 1949 as amended (42 U.S.C. 1471 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.

Risks: Minimal risk; eForms gives customers, producers, partners, and others access to forms and account information related to USDA programs. No data is produced.

Mitigation: Applications are located behind the NITC secure midrange infrastructure. See the System Security Plan (SSP) security controls: Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM). These applications are behind eAuthentication (eAuth) with a Level 2 access authority. Users of the system are required to complete annual privacy act training to ensure the proper handling of privacy data.

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.

eForms gives customers, producers, partners, and others access to forms and account information related to USDA programs. After activating their account, customers may complete and submit documents online to local USDA Service Centers or Area Offices.

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

Manual inspection by RD government staff is used to analyze the data. No data is produced.

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

N/A

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.

The National Institute of Standards and Technology (NIST) 800-53 controls for the eForms system are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1-8, 11, 12, 14, 17, and 19-22), Identification and Authentication (IA-1-8) and Systems and Communication Protection (SC-1,2, 4, 5, 7, 8, 10, 12, 13, 15, 17-23, 28, and 39) controls are in place to prevent unauthorized access. The Authority and Purpose (AP-1 and 2), Accountability, Audit, and Risk Management (AR-1-8), Data Quality and Integrity (DI-1 and 2), Data Minimization and Retention (DM-1, 2, and 3), Individual Participation and Redress (IP-1-4), Security (SE-1 and 2), Transparency (TR-1-3), and User Limitation (UL-1 and 2) controls are in place to protect privacy.

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?

Data is not retained.

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

Data is not retained.

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

Minimal risk associated, since there is no data retention.

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?

FSA, and RD all provide additional electronic form templates and configuration data for the system.

Forms, MyForms: USDA Grain Inspection, Packers and Stockyard Administration (GIPSA) purpose is to manage the business processes around the Account Management System.

UniFi provides forms for agencies.

PLAS is an accounting system providing transaction processing.

4.2 How is the information transmitted or disclosed?

The NIST 800-53 controls for the eForms system are discussed in detail in the System Security Plan and specifically the System and Communication (SC) controls are in place to provide integrity and confidentiality

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 NIST 800-53 controls for the eForms system are discussed in detail in the System Security Plan and specifically the System and Communication (SC) controls are in place to provide integrity and confidentiality.

Interconnection Service Agreement (ISA) and Memorandum of Understanding (MOU) agreements are in place [in Cyber Security Assessment and Management (CSAM)] and maintained by the Information Systems Security Staff (ISSS).

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?

MyForms: Federation of Appalachian Housing Enterprise (FAHE) – FAHE employees log into website, uploads loan application information package from their desktop. This provides assistance to the rural community by submitting electronic loan application packages to USDA Rural Housing service through the MyForms.

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.

A SORN is not required for eForms, it does not share information with the public.

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

Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU) agreements are in place CSAM and maintained by the ISSS.

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

No risks identified. Interconnection Security Agreements (ISA) agreements are in place CSAM and maintained by the ISSS.

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.

.1 Does this system require a SORN and if so, please provide SORN name and URL.

No

6.2 Was notice provided to the individual prior to collection of information?

Yes, County Based Agency electronic service requests.

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

Yes, individuals willingly participate in the application.

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

Yes, individuals willing participate in the application.

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.

Individuals willingly participate in providing information for the completion of loan and grant requirements. Users complete privacy forms when they apply for loans or grants and consent to the use of their data before this information is provided.

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?

Users, employees, managers, system administrators and developers have access to the data in the system. Access is controlled by UserID and password. Access rights are granted to designated individuals only when their supervisor or the site system manager approves a written request.

Privileges granted are based on job functions and area of authority (e.g. State office user with authority for their state only).

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

During the course of the review, if any information found to be missing, incorrect, or out-dated, comments are added to the packet and the form is reassigned to an editable state (Returned) for participant correction.

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

Information is disseminated through annual POC training.

Users are notified of the ability to update their information when they sign their consent form to use the service.

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

Individuals have access, redress, and amendment rights under the Privacy Act and the Freedom of Information Act.

Contact:

Administrator, Rural Housing Service, USDA, 1400 Independence Avenue, SW, Room 5014, South Building, Stop 0701, Washington, DC 20250-0701;

Administrator, Rural Business-Cooperative Service, USDA, 1400 Independence Avenue, SW, Room 5045, South Building, Stop 3201, Washington, DC 20250-3201;

Administrator, Rural Utilities Service, USDA, 1400 Independence Avenue, SW, Room 4501, South Building, Stop 1510, Washington, DC 2050-1510.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

No additional risks are associated with the redress process.

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?

eAuth Level 2 is required to access Forms Admin and MyForms.

Generally, the National Institute of Standards and Technology (NIST) 800-53 controls for Common Call Components are discussed in detail in the System Security Plan and specifically the Access Control (AC), Identification and Authentication (IA) and Systems and Communication Protection (SC) controls are in place to prevent unauthorized access. Access control is also addressed in the individual systems desk procedures.

Desk Procedures document the process for establishing, activating, and modifying IDs. This process is defined by System Owners. System Owners define Groups and account types. System Point of Contact assigns group membership and determines Need-to-know validation. The POC is responsible for verifying user identification; the User Access Management Team relies on a POC supplying the correct UserID and password to UAM to identify themselves. UAM tickets are the tool used to track authorized requests by approving Point of Contact (POC).

RD reviews reports from HR on a Bi-weekly basis. The organization employs automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are not used or authorized. Guest and Anonymous accounts are not managed by ISS UAM Team. POCs (empowered by RD IT managers) are responsible for notifying UAM Team if access or roles need to be modified and periodically reviewing and certifying established access.

8.2 Will Department contractors have access to the system?

Yes

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

The NIST 800-53 controls for the eForms system are discussed in detail in the System Security Plan and specifically the Awareness and Training (AT) controls are in place to provide privacy training. RD requires annual Information Security and Awareness (ISAT) training for all employees and contractors. RD is responsible for ensuring all new employees and contractors have taken the Department Security Awareness Training as developed by OCIO-Cyber Security (CS). Training must be completed with a passing score prior to access to a RD System. All RD employees/contractors are required to complete Computer Security Awareness Training and USDA Privacy Basics on an annual basis.

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?

The NIST 800-53 controls for the eForms system are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls are in place to prevent misuse of data.

RD has an Application Auditing and Monitoring Policy in place that defines the following auditable events: server startup and shutdown, loading and unloading of services, installation and removal of software, system alerts and error messages, user logon and logoff attempts (both successful and unsuccessful), granting of elevated privileges (root access success and failure), modifications of privileges and access controls, all root commands (success and failure), and sensitive files accessed, modified and added. These controls, including full compliance, inheritance and risk acceptance descriptions, are available in CSAM.

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?

Risk is mitigated by collecting auditable events: date and time of the event, the component of the information system where the event occurred, type of event, user/subject identity, and the outcome (success or failure) of the event.

The NIST 800-53 controls for the Shared Services system are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls are in place to prevent misuse of data. At a minimum, the following information will be collected for each of the auditable events: date and time of the event, the component of the information system where the event occurred, type of event, user/subject identity, and the outcome (success or failure) of the event.

Audit logs will be reviewed by security personnel every two weeks and suspicious activity will be investigated. Suspicious activity includes, but not limited to: modifications or granting of privileges and access controls without proper request submitted, consecutive unsuccessful log-on attempts that result in a user being locked, multiple unsuccessful log-on attempts without lock out by the same User Identification (UserID), modifications or attempted modification of sensitive files without authorization and within the applications repeated attempts to access data outside a user's privilege.

Per the General Records Schedule 20, Section 1C, the following items will be deleted/destroyed when the agency determines they are no longer needed for administrative, legal audit or other operational purposes: electronic files and hard copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files and cost-back files used to assess charges for system usage.

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?

eForms is a custom application from Commercial off the shelf and Government developed software.

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

No, eForms does not employ technologies which would 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?

eForms does not use 3rd party websites

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

eForms does not use 3rd party websites

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

eForms does not use 3rd party websites

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?

eForms does not use 3rd party websites

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

eForms does not use 3rd party websites

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

eForms does not use 3rd party websites

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?

eForms does not use 3rd party websites

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)?

eForms does not use 3rd party websites

10.10 Does the system use web measurement and customization technology?

N/A

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

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.

eForms does not use 3rd party websites

Responsible Officials

MICHAEL SUTTON Digitally signed by MICHAEL SUTTON
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=MICHAEL SUTTON, 0.9.2342.19200300.100.1.1=12001000317363
Date: 2016.10.12 10:40:30 -05'00'

Michael Sutton
Chief, Enterprise Technologies Branch

Approval Signature

Signed For

EUGENE TEXTER Digitally signed by EUGENE TEXTER
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=EUGENE TEXTER, 0.9.2342.19200300.100.1.1=12001000317346
Date: 2016.10.12 10:06:04 -05'00'

Diego Maldonado
Information Systems Security Program Manager
United States Department of Agriculture