Privacy Impact Assessment
Enterprise Content Management (ECM)

Rural Development (RD)

- Date: Mar, 2017
- Prepared for: RD

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	July 16, 2014	Natasha Williams	FY14 Continuous Monitoring. Document was reviewed and the only updates for the system owner.
1.1	April, 2015	Natasha Bradley	FY15 review
1.2	May, 2016	JH	FY 16 review
1.3	June, 2016	JMK	New Template and updates
1.4	March, 2017	TGW	Updated SORN to RD-2

Abstract

ECM receives, collects, imports, interprets, documents and track incoming correspondence and content from public, individual, private, political sources and internal sectors from the beginning of the inquiry up to and including its resolution and response back to the originator. All collected data is then scanned into ECM by USDA personnel.

Overview

ECM documents are scanned or added electronically into the system from a USDA scanning location or user's workstation. When scanning, the operator performs a quality control check. The operator enters some basic document index information. Document indexes categorize the document and forward it to the group responsible to set-up the folder for the action to be performed. The system then transfers the documents to the centralized document repository (Oracle database) at USDA. Once the document is stored, the system starts the workflow process.

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?

Name, address Information, personal identification number, miscellaneous identification numbers and handwriting or an image of the signature.

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

The below items are the ECM sources of DATA:

- **Content Analysis Module (CAM)** is used by USDA agencies and offices to view public comments solicited by USDA on the 2007 Farm Bill.

- **Acquisition Approval Requests (AAR)** module utilizes ECM's workflow abilities to route requests through the approval process and uses ECM to store the associated documentation that accompanies the AAR.

- **Acquisition Management Module (AMM)** is used by the Forest Service (FS) to manage and document approval of acquisition requests for their procurement staff.

- **Agriculture Foreign Investment Disclosure Act** (**AFIDA) Module** is used to track foreign interests in United States Agriculture land.

- **ASBCF Miscellaneous Payments** is used by the Forest Service to store documents related to payments made outside of Integrated Acquisition System (IAS).

- **Correspondence Management Module (CMM)** helps USDA employees at any organizational level manage correspondence and other documents from initial receipt through completion and archival storage.

- **Controller Operations Division (COD) Telephone/Utility Module** is an ECM module implemented to process USDA telephone and utility invoices. National Finance Center (NFC) employees use the module to manage the approval and payment processing of telephone and utility bills.

- **Content Analysis Module** was used to sort and categorize feedback from the Farm Bill of 2008. Public comments were routed to the appropriate Agency for review and response.

- **Customer Service Call Management (CSCM)** is used to track incoming telephone calls made to National Agricultural Statistics Service (NASS) and keep a running record of telephone inquiries made to that Agency. Specifically CSCM tracks the subject inquired about, who was inquiring about the subject and the resolution to the telephone inquiry**.**

- **Deputy Chief Financial Officer (DCFO) Receipts Module** was developed for the Office of the Chief Financial Officer, Receipts Unit, and this module automates the processing of receipts with the integration of fax server functionality that allows for the employees in the Receipt Unit to telework.

- **Direct Loan & Grant Branch (DLGB) Module** was developed for the USDA Office of the Chief Financial Officer (OCFO), DLGB in St. Louis to process and track various correspondence items relating to Community Facilities and Multi-Family Housing programs.

- **electronic Personnel Security Folder (ePSF) Module** was developed for the Office of Homeland Security (OHSEC) Personnel and Document Security Division (PDSD) to digitize existing paper investigation records, adjudicate new subject investigations and manage the retention of the employee investigation files according to PDSD regulations.

- **Farm Loan Program (FLP)** is used by the Farm Service Agency (FSA) to manage their internal work assignments using ECM FLO to track payments and for general tasking of employees. FLO allows management to track documents, record actions taken, and utilize archival storage of the documents.

- **Federal Grain Inspection Service** (**FGIS) Module** is used as a document repository to store handbooks, policies and procedures for conducting business.

- **Invoice Processing Module (IPM)** is used by USDA agencies and offices are utilizing the ECM Invoice Processing Module to store all USDA invoices in a centralized repository. Currently, managers use the module to manage the approval and payment processing of invoices.

- **General Use Module (GUM)** is used by USDA agencies and offices to manage administrative processes. For example, RD uses GUM to track payments and tenant certifications, maintain a running case record for their accounts, and for general tasking of employees. GUM allows management to track documents, record actions taken, and utilize archival storage.

  The OCIO uses GUM to manage requests for information technology waivers and similar documents at all stages, from initial application through final decision and archival storage. Applicants and OCIO managers can track the status of these items at all stages of the business process.

- **Packers, Stockyards Automated System (PSAS)** is used by the USDA's Packers and Stockyards Program (P&SP) under Grain Inspection, Packers and Stockyards Administration (GIPSA) to track tasks and documents related to the various regulatory activities that their mission calls to be conducted on businesses in the livestock and poultry industries. These activities take the form of registrations, audits, investigations and enforcements with standard workflows that have been defined for each.

- **Grants Review Module** is used by Rural Utilities to process loan and grant requests for broadband access. ECM is used as a document repository and workflow for routing the requests to reviewers for scoring.

- **Office of the General Counsel (OGC) Case Management Module** was developed for the USDA OGC to track and update all of their legal cases and back-file documents and casework.

- **Performance Appraisal Module** is used by Food and Nutrition Service to store copies of old performance appraisals. After they are scanned into ECM the hard copy

of the appraisal can be accessed electronically at any time. This help free up physical space at their headquarters office.

- **Rural Business Service (RBS) Module** is used by RBS Alternative Agriculture Research to store BCPAR documentation.

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

ECM is a document repository; that allows USDA to manage business documents, including correspondence.

1.4 How is the information collected?

ECM receives, collects, imports, interprets, documents and track incoming correspondence and content from public, individual, private, political sources and internal sectors from the beginning of the inquiry up to and including its resolution and response back to the originator. All collected data is then scanned into ECM by USDA personnel.

1.5 How will the information be checked for accuracy?

ECM is a document repository. End users are responsible for the data they upload. Any possible data corruption is reported to the ECM Tier 3 Support to troubleshoot.

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

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 since ECM is a document repository

Mitigation: Data is stored in a secure environment 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).

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.

Responding to inquiries, processing invoices and processing day to day work.

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

N/A – Information is provided.

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

N/A, Internal use only. All collected data is then scanned into ECM by USDA personnel

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 ECM system are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1-8, 11, 12, 14, and 19-22), Identification and Authentication (IA-1-7) and Systems and Communication Protection (SC-1, 2, 4, 7, 8, 10, 12, 13, 17, 18, 23, 28, and 39) controls are in place to prevent unauthorized access. The Authority and Purpose (AP-1-2), Accountability, Audit, and Risk Management (AR-1-8), Data Quality and Integrity (DI-1-2), Data Minimization and Retention (DM-1-3), Individual Participation and Redress (IP-1-4), Security (SE-1-2), Transparency (TR-1-3), and User Limitation (UL-1-2) 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 currently retained permanently

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.

There are minimal risks with the length of time data is retained because data access is only granted by the owner of the document.

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?

Hyperion – information is used to create reports

4.2 How is the information transmitted or disclosed?

Information is transmitted through an Oracle Database connection.

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.

There are minimal privacy risks because data access is granted by the owner of the document.

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?

Office of Personnel Management (OPM) – eDelivery system providing an inbound data only feed and documents to ECM via Connect Direct Secure Plus.

US Bank – provides inbound data feed only and documents in ECM via Connect Direct Secure Plus.

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.

ECM does not share personally identifiable information outside the Department.

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

ECM does not share personally identifiable information outside the Department.

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

ECM receives data from external sources but once it is scanned into ECM it can only be accessed by internal sources.

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.

ECM is covered under SORN RD-2

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

End users are responsible for the data they provide, they have the opportunity to not provide the data.

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

End users are responsible for the data they upload; they have the opportunity to not upload data.

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

N/A

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.

N/A. End users are responsible for the data they upload.

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?

In order to gain access to ECM, users must have a level 2 e-authentication account, be attempting to access ECM from a USDA computer and must have been added to the application by an ECM administrator who determines what groups and access to which modules they are entitled to receive.

To be granted the administrative roles of Agency Group Administrator, Privileged User, Module Administrator, Security Officer, Records Manager and Application Administrator a user's access must be upgraded by a Security Officer.

In ECM, some privileges and defaults are anchored to a specific point in the organizational hierarchy and then apply to all levels (organizations, groups and users) below. When group default security settings are created, they are anchored to a specific organization and apply to all organizations below unless overridden by a lower level group security default.

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

Formal requests for correction of USDA information must be submitted by letter, fax, or e-mail to the Information Quality Official(s) of the USDA agency or office that disseminated the information (henceforth in these procedures, the term "USDA agency" shall mean "USDA agency or office"). For requests for correction concerning information on which USDA seeks public comment, submit the correction request during the comment period.

After the responsible USDA agency has made its final determination pertaining to a request for correction of information, that agency will respond to the requestor in writing by letter, e-mail, or fax, normally within 60 calendar days of receipt. The response will explain the findings and the actions the agency will take (if any) in response to the complaint.

If the request requires more than 60 calendar days to resolve, the agency will inform the complainant within that time period that more time is required, and the reasons for the delay, and an estimated decision date.

Customers and employees may contact **USDA Rural Development Primary FOIA Contact Information:**

USDA Rural Development
FOIA/Privacy Act/Torts Unit
1400 Independence Avenue, SW, Stop 0742
Washington, DC 20250-0706
TELEPHONE (202) 690-5394
Email: Ssd.foia@wdc.usda.gov

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

Persons who wish to file a Request for Reconsideration should submit the request by letter, fax, or e-mail to the Reconsideration Official identified in the final determination of the request for correction that the requestor receives from USDA. For requests for reconsideration that involve *influential* scientific, financial, or statistical information, or regulatory information, USDA will designate a panel of officials to perform this

function. Typically, such a panel would include a Reconsideration Official from the USDA agency that made the initial determination and two from other USDA agencies.

Persons requesting reconsideration should submit written material to support their case for reconsideration, as well as a copy of the information originally submitted to support the request for correction and a copy of USDA's response. Requests for Reconsideration must be filed with the appropriate designated Reconsideration Official (postmarked, shipped by an overnight delivery service, faxed, or sent by e-mail) within 45 days after the date that the USDA agency transmitted its decision on the original request for correction. Requests for Reconsideration that are filed after the 45-day deadline may be denied as untimely.

Depends on which Agency, each Agency has their own specific policies in place.

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

If the requestor disagrees with the USDA agency's denial of the request or with the corrective action the agency intends to take, the requestor may file a Request for Reconsideration with the USDA agency. The USDA agency that processed the request for correction will provide instructions in its final determination communication to the requestor for the procedure to request reconsideration of USDA's decision.

In cases where the agency disseminates a study, analysis, or other information prior to the final agency action or information product, requests for correction will be considered prior to the final agency action or information product in those cases where the agency has determined that an earlier response would not unduly delay issuance of the agency action or information product and the complainant has shown a reasonable likelihood of suffering actual harm from the agency's dissemination if the agency does not resolve the complaint prior to the final agency action or information product.

The individual would write a letter to the Secretary which will be processed in ECM

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?

National Institute of Standards and Technology (NIST) 800-53 controls for ECM 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. UAM tickets are the tool used to track authorized requests by approving Point of Contact (POC).

Currently 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?

RD requires annual Information Security and Awareness training for all employees and contractors. RD is responsible for ensuring all new employees and contractors have taken the Department Security Awareness Training developed by Office of Chief Information Officer-Cyber Security. Training must be completed with a passing score prior to access to a RD system.

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?

NIST 800-53 controls are discussed in detail in the SSP including the Audit and Accountability (AU) controls in place to prevent misuse of data.

RD has a NIST Audit and Accountability Policy, Standards, and Procedure 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: Human factor: extracting information and using this information erroneously.

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 are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls which 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 I c 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?

ECM is a document repository with workflow capabilities; it allows USDA to manage business documents, including correspondence, effectively and efficiently

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

No

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, guidance has been reviewed by all parties.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

ECM 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 3rd party websites and/or applications.

ECM does not use third party websites and/or applications.

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

ECM does not use third party websites and/or applications.

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?

ECM does not use third party websites and/or applications.

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

ECM 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 3rd party websites and/or applications?

ECM 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 3rd party websites and/or applications be shared - either internally or externally?

ECM 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 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

ECM does not use third party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

ECM does not use web measurement and customized 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

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.

ECM does not use third party websites and/or applications.

Responsible Official

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: 2017.03.17 10:00:31 -05'00'

Michael Sutton
Chief, Enterprise Technologies Branch

Approval Signature

DIEGO MALDONADO

Digitally signed by DIEGO MALDONADO
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=DIEGO MALDONADO, 0.9.2342.19200300.100.1.1=12001001325122
Date: 2017.03.17 11:20:16 -05'00'

Diego Maldonado
Information Systems Security Program Manager