Privacy Impact Assessment

Enterprise Content Management (ECM)

Policy, E-Government and Fair Information Practices

- Date Prepared: September 14, 2020
- Prepared for: USDA 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	Nil	New Template and updates
1.4	March, 2017	TGW	Updated SORN to RD-2
1.5	November, 2017	SAC	FY18 Review, updated FOIA Liaison
1.6	September, 2020	CC/IO	Updated system information

Abstract

The USDA relies on its information technology systems, including the Enterprise Content Management (ECM), to accomplish its mission of providing cost-effective and reliable services to the USDA, other Federal agencies, and the public at large.

Enterprise Content Management (ECM) is a DISC based mission-critical system with a FIPS 199 security rating of "moderate". ECM receives, collects, imports, interprets, documents and tracks 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. ECM allows USDA to manage business documents, including correspondence, effectively and efficiently. ECM currently includes 20 functional components/modules. These components all use RD's Enterprise Shared Services hardware and software infrastructure. However, each presents a different user interface that has been customized and fine-tuned to meet a specific set of business requirements. Over the next several years, additional ECM components will be available to meet other RD business needs.

Overview

ECM is an application component of the USDA RD initiative for Information Technology (IT). This system is designed to receive, collect, import, interpret, document and track incoming correspondence and content from public, individual, private, and political sources. All users to the system will be authenticated through eAuthentication over the USDA Intranet. All collected data is then scanned into ECM by USDA personnel. This application and its components are created using JAVA and Stellent Content Manager.

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.

The workflow process routes the document through necessary processing steps that may include the following:

- Set-up a new folder with the scanned document;
- Set-up a new folder with an electronically added document, adding a processing code to the folder to trigger the workflow;
- Create the workflow list of tasks and assignees;
- Route the folder through the workflow tasks for processing

The actual tasks that are performed depend on the requirements of the document. The Folder Owner determines the actual workflow tasks and assignees necessary to process the work. The system provides capabilities that allow each individual to manage their workflow tasks using

their inbox. Workflows can be monitored to see the current status and help ensure timely completion.

In addition to accessing the system to process correspondence, authorized users may search the system for documents and folders. Searches can be performed on the document or folder indexes. Alternatively, full-text searches can be performed to find all documents that contain specific words or phrases.

Features and Benefits

ECM currently includes the following modules, which are the sources of the information in ECM. These modules all use RD's Enterprise Shared Services hardware and software infrastructure. However, each presents a different user interface that has been customized and fine-tuned to meet a specific set of business requirements. Over the next several years, additional ECM modules will be available to meet other RD business needs.

The modules consist of:

Acquisition Approval Requests (AAR)

The AAR module was developed for the Department OCIO's Office. All Information Technology procurements over $25,000 require a Departmental Approval. The AAR module is used to track the approval of these procurements. This module is not actively collecting new information.

Acquisition Management Module (AMM)

The Forest Service uses AMM to manage and document approval of acquisition requests for their procurement staff. Acquisition requests are tracked at all stages, from initial application through final decision and archival storage. Procurement managers can track the status of these items at all stages of the business process. This module is not actively collecting new information.

Agriculture Foreign Investment Disclosure Act Module (AFIDAM)

The AFIDA group from FSA uses the AFIDAM to track foreign ownership of agriculture land in the United States. This module is not actively collecting new information.

Albuquerque Service Center Budget and Finance Miscellaneous Payments (ASCBFMP)

The ASCBF is used by the Forest Service to store documents related to payments made outside of the Integrated Acquisition System. This module is not actively collecting new information.

COD Telephone/Utility Module

An ECM module will be implemented to process RD telephone and utility invoices. Currently, National Finance Center (NFC) employees use the module to manage the approval and payment processing of telephone and utility bills. Future phases will follow the invoices

through all stages of the business process and may include a flat file transmission of data to a NFC application. This module is not actively collecting new information.

Content Analysis Module (CAM)

ECM's powerful, versatile features are also proving useful for specialized non-correspondence applications. RD agencies and offices, for example, are using the CAM to view public comments solicited by RD on the 2008 Farm Bill. CAM users can view the database of comments according to key issues and then "drill down" to access each actual comment. This module is not actively collecting new information.

Correspondence Management Module (CMM)

The CMM helps RD employees at any organizational level manage correspondence and other documents from initial receipt through completion and archival storage. The system's strong workflow capabilities enable documents to be routed within or among RD agencies and offices for collaborative input or review, and a robust security scheme ensures that information is available only to authorized personnel. Easy-to-use search and report features are helping executives, managers, and other users find and display the information they need quickly and efficiently. This module is actively collecting, storing and processing new information.

The Correspondence Management Module can:

- Support and streamline intra-agency and interagency correspondence and document management processes, whether at RD headquarters or a field office, within a secure environment.
- Offer ease of access to users while, as a Web-based application, eliminating the need to install or support desktop client software.
- Provide a computer-based work environment, eliminating document loss and reducing time required for document review and revision.
- Support a "less paper" environment while improving service.
- Detect and Categorize possible duplicates of correspondence and Campaign Mail through enhanced content analysis.

Customer Service Call Management Module (CSCMM)

National Agriculture Statistics Service uses the ECM CSCMM to track telephone requests for specific statistics. This module is not actively collecting new information.

Deputy Chief Financial Officer Receipts Module (DCFORM)

The DCFO receipts module was developed for the Office of the Chief Financial Officer, Receipts Unit, 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. This module is actively collecting, storing and processing new information.

Direct Loan & Grant Branch Module (DLGBM)

The DLGBM was developed for the USDA Office of the Chief Financial Officer. The DLGB in St. Louis processes and tracks various correspondence items relating to Community Facilities and Multi-Family Housing programs. This module is actively collecting, storing and processing new information.

Farm Loan Program Module (FLPM)

The Farm Services Agency (FSA) uses the FLPM to process and track the payments made to the FLP. This module is actively collecting, storing and processing new information.

Federal Grain Inspection Service Module (FGISM)

FGIS uses this module to store FGIS handbooks and other legacy documentation to prepare for the upcoming retirement wave. This module is not actively collecting new information; however, the information has been updated.

General Use Module (GUM)

RD agencies and offices are utilizing the ECM GUM 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.

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. This module is actively collecting, storing and processing new information.

Grants Review Module (GRM)

The GRM is used for the processing and scoring of Rural Utility Service grant applications. This module is not actively collecting new information.

Invoice Processing Module (IPM)

RD agencies and offices are utilizing the ECM IPM to store all RD invoices in a centralized repository. Currently, managers use the module to manage the approval and payment processing of invoices. Future phases will follow the invoices through all stages of the business process from initial submission through final decision and archival storage. Vendors will be able to electronically submit their invoices and check on the status of those invoices. This module is not actively collecting new information.

Office of the General Counsel Case Management Module (OGCCMM)

Implemented in July 2012 the module was developed for the RD Office of the General Counsel (OGC) to track and update all of their legal cases and back-file documents and casework. Unique features of this module include a tickler reminder system, special position specific security enhancement, drag and drop document capability, and a document repository specifically developed for back-file documents at OGC. This module is actively collecting, storing and processing new information.

Packers Stockyards Automated Systems (PSAS)

RD's PSAS under the Grain Inspection Packers and Stockyards Agency (GIPSA) is utilizing the PSAS module 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. In addition, the PSAS module allows for the maintenance of data concerning the various businesses being regulated. These data elements are used in support of the regulatory activities and include general information about the businesses as well as annual business volume, facilities, scales and bonding. Viewed on the user level, PSAS comes across as two modules GIPSA and AMS. Logically they are PSAS. This module is actively collecting, storing and processing new information.

Performance Appraisal Module (PAM)

The PAM is used by Food and Nutrition Service (FNS) to store and access employee performance appraisals. This allowed FNS to free up physical space in their offices. This module is actively collecting, storing and processing new information.

Personal Security Folder Module (ePSFM)

The electronic-PSFM is used by the Office of Homeland Security & Emergency Coordination Personnel and Document Security Division to store background checks on all RD employees and contractors. This module is actively collecting, storing and processing new information.

Rural Business Module (RBM)

The Rural Business Service uses this module to track and process Alternative Agriculture Research grants and Agency outreach. This module is not actively collecting new information.

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?

Data Elements: Name, address information, personal identification number, Biometric data, Criminal History, Employment History, miscellaneous identification numbers and handwriting or an image of the signature.

Individuals: USDA employees, contractors, and the general public.

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

The below modules are the internal ECM sources of data:

- Acquisition Approval Requests (AAR) is used by the Office of the Chief Information Officer (OCIO) in Washington DC to Manage Information Technology acquisition requests greater than $25,000.00. The 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.
- Albuquerque Service Center Budget and Finance Miscellaneous Payments (ASCBFMP) is used by the Forest Service to store documents related to payments made outside of the Integrated Acquisition System.
- COD Telephone/Utility Module is an ECM module implemented to process USDA telephone and utility invoices. National Finance Center (NFC) employees used the module to manage the approval and payment processing of telephone and utility bills. Future phases will follow the invoices through all stages of the business process and may include a flat file transmission of data to an NFC application.
- Content Analysis Module (CAM) 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. Feedback would have been provided by members of the public and special interest groups.
- Correspondence Management Module (CMM) helps USDA employees at any organizational level manage correspondence and other documents as a result of inquiries from public citizens and members of Congress from initial receipt through completion and archival storage. The system's strong workflow capabilities enable documents to be routed within or among USDA agencies and offices for collaborative input or review, and a robust security scheme ensures that information is available only to authorized personnel.
- Customer Service Call Management (CSCM) was 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 what the subject inquired about, who was inquiring about the subject and the resolution to the telephone inquiry.
- DCFO Receipts Module was developed for the Office of the Chief Financial Officer, Receipts Unit, 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 Module (DLGBM) was developed for the USDA Office of the Chief Financial Officer (OCFO), Direct Loan & Grant Branch in St. Louis to process and track various correspondence items relating to Community Facilities and Multi-Family Housing programs.
- Farm Loan Program Module (FLPM) is used by the Farm Service Agency (FSA) to manage their internal work assignments. They are 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.
- 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.
- 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.
- 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.
- OGC Case Management Module was developed for the USDA Office of the General Counsel (OGC) to track and update all of their legal cases and back-file documents and casework.
- Packers, Stockyards Automated System (PSAS) is used by the USDA's Packers and Stockyards Program (P&SP) under 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.
- Performance Appraisal Module (PAM) is used by Food and Nutrition Service (FNS) 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 helps to free up physical space at their headquarters office.
- Personal Security Folder Module (ePSFM) 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.
- Rural Business Service (RBS) Module is used by RBS Alternative Agriculture Research to store BCPAR documentation.

ECM only receives inbound data from these external sources: OPM, DCSA and U.S. Bank.

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 tracks 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. The sources of the information are the modules listed above. The public does not have direct access to ECM; all data is received by USDA personnel from the original source and then scanned into ECM by USDA personnel**.**

1.5 How will the information be checked for accuracy?

ECM is a document repository. Users with approved role-based access would be responsible for the accuracy of the data that they upload in ECM. 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?

Privacy Act of 1974 (5 U.S.C. Sec. 552a); Freedom of Information Act, as amended (5 U.S.C. Sec. 552); 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); Debt Collection Act of 1982, Pub. L. 97-365 (5 U.S.C. 5514; 31 U.S.C. 3701 et seq.); Debt Collection Improvement Act of 1996, Pub. L. 104-134 (5 U.S.C. 5514; 31 U.S.C. 3701 et seq.); 31 U.S.C. 7701 (Taxpayer Identifying Number); USDA Departmental Regulation (DR) 3080-001; Records Management; NARA General Records Schedules Transmittal 31.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

RISK: ECM is a document repository. The initial assessment of privacy risk would be performed by the administrators who manage the data at its collection.

MITIGATION: Data is stored in a secure environment behind the DISC 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.

ECM is a document repository. Data is stored in ECM in designated folders. Users with approved access to the designated folders can access the data in ECM and create ad hoc reports, as necessary. The data could be used to respond to inquiries, process invoices and process day to day work. Data received from the DLGB module will be stored in ECM and may also be shared with the Electronic Customer File (ECF) application. Additionally, reports are generated on a frequent basis using Hyperion.

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

N/A. No tools are used to analyze data.

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

All collected data is internal to the USDA and is 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, 12, 14, 17, 20 and 21), Identification and Authentication (IA-1-7) and Systems and Communication Protection (SC-1, 2, 4, 5, 7, 8, 10, 12, 13, 17, 20-23, 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?

All information will be retained in compliance with NARA Guidelines, according to the NARA General Records Schedules (GRS).

The SORN RD-2 specifies policies and practices for retention and disposal of Rural Development's records.

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

Yes, the retention period has been approved.

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

RISK: Access to the data is controlled by designated administrators, as such, the risk associated with the length of time that the data is retained is minimal.

MITIGATION: Data Integrity controls (DI 1-2) are used to protect data from accidental or malicious alteration and destruction providing assurance to the user the information meets expectations for quality and it has not been altered. 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 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?

Information is shared with the system Business Intelligence (BI): Hyperion & Tableau Reporting System application, for the preparation of reports. Name, Address Information, Personal identification number, Biometric data, Criminal History, Employment History, miscellaneous identification numbers and handwriting or an image of the signature are all data elements that could be shared for the purpose of creating reports. The reports would be provided to the designated administrators of the modules. Information from the DLGB module is also shared with the system Common Call Components (CCC): Electronic Customer File (ECF) application.

4.2 How is the information transmitted or disclosed?

Information is transmitted through an Oracle Database connection. ECM application services are only accessible to an internal USDA audience and are not available to the public. The sources of the information are the modules listed above. All data is received by USDA personnel from the original source(s) and then scanned into ECM by USDA personnel. The public does not have direct access to ECM.

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.

RISK: Access to the data is controlled by designated administrators, as such, the risk associated with the sharing of the data is minimal.

MITIGATION: The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality. The security and control of PII is the responsibility of the System Owner and RD employees. Risk is mitigated with the implementation of RD Technology Office NIST policies, standards and procedures. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure.

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?

Defense Counterintelligence and Security Agency (DCSA) - Memorandum of Understanding (MOU) between DCSA and USDA Headquarters/Personnel and Document Security Division (USDA HQ/PDSD) – DCSA will perform a background investigations process and will transmit any investigative case materials to USDA using the eDiscovery system. eDiscovery system to provide an inbound data only feed and documents to ECM via Connect Direct Secure Plus.

Office of Personnel Management (OPM) – Interconnection Security Agreement (ISA) between USDA RD and OPM. Background investigations process previously carried out by National Background Investigations Bureau (NBIB), as part of OPM, was transferred to DCSA. ISA required between USDA RD and OPM, as OPM legacy IT systems housing investigative records are owned and operated by OPM, and DCSA requires ISA for each connection utilized for eDelivery, for as long as DCSA receives IT background investigation IT services from OPM. DCSA has a service level agreement with OPM for the continued use and support of the OPM IT systems in support of background investigations conducted by DCSA.

US Bank – Interconnection Security Agreement (ISA) between USDA RD (ECM) and US Bank. ECM provides one-way data transmission STOP files to US Bank.

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, other than to the organizations listed in 5.1.

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, other than to the organizations listed in 5.1.

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

RISK: The risk to external information sharing would be the unauthorized disclosure of correspondence, however, ECM does not share (transmit) personally identifiable information outside the Department, other than to the organizations listed in 5.1.

MITIGATION: ECM receives inbound data from external sources but once it is scanned into ECM it can only be accessed by internal sources. An ISA is in place between USDA RD (ECM) and US Bank, documenting the connections between the systems and how the security of the two systems will be maintained. An MOU is in place between USDA HQ/PDSD and DCSA, documenting the responsibilities between the parties and how the data will be transmitted to ECM. An ISA will be in place between USDA RD and OPM, documenting the connections between the systems and how the security of the two systems will be maintained. The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality. Also, the data is stored in a secure environment behind the DISC secure mainframe infrastructure.

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, Enterprise Content Management. (http://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records)

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

Notice was provided to individuals by the initial source systems prior to collection or processing of the information. ECM is a document repository and is not involved in the initial collection of information from the individuals.

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

Notice of opportunity and/or right to decline to provide information was provided to individuals by the initial source systems prior to collection or processing of the information. ECM is a document repository and is not involved in the initial collection of information from the individuals.

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

Consent of the individuals for particular uses of the information would have been obtained by the initial source systems, if required, prior to collection or processing of the information. ECM is a document repository and is not involved in the initial collection of information from the individuals.

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.

RISK: Notice was provided to individuals by the initial source systems prior to collection or processing of the information. The initial assessment of privacy risk would be performed by the administrators who manage the data at its collection.

MITIGATION: Individuals do not have direct access to the system as users. Notice of the purposes and uses for the collection of the information is provided in the SORN RD-2.

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?

The public does not have direct access to ECM; all data is received by USDA personnel from the original source and then scanned into ECM by USDA personnel. In order for a user 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.

Individuals are notified of the procedure to gain access to their information in the Notification Procedure section as outlined in the SORN RD-2. Notification Procedure: Individuals who want to know whether this system of records contains information about them, who want to access their records, or who want to contest the contents of a record, should make a written request to the Office of the Chief Information Officer, Enterprise Technologies Branch, Branch Chief, 4300 Goodfellow Blvd., St. Louis, MO 63120. Individuals must furnish the following information for their records to be located and identified:

A. Full name or other identifying information necessary or helpful in locating the record;

B. Why you believe the system may contain your personal information;

C. A statement indicating the type of request being made (i.e., access, correction, or amendment) and whether a personal inspection of the records or a copy of them by mail is desired;

D. Signature.

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

Individuals are notified of the procedure to gain access to and contest their information in the Notification Procedure, Record Access Procedures and Contesting Record Procedures sections as outlined in the SORN RD-2. See Notification Procedure information in 7.1. Record Access Procedures: Individuals wishing to request access to their records should follow the Notification Procedures. Individuals requesting access are also required to provide adequate identification, such as a driver's license, employee identification card, social security card, or other identifying document. Additional identification procedures may be required in some instances. Contesting Record Procedures: Individuals requesting correction or amendment of their records should follow the Notification Procedures and the Record Access Procedures and also identify the record or information to be changed, giving specific reasons for the change.

In general, 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 also contact:

USDA Rural Development Primary FOIA Contact Information:

Lolita Barnes
FOIA Liaison
1400 Independence Ave., SW
Washington, DC 20250
Tel. 202-692-0004
Email: lolita.barnes@usda.gov

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

Individuals are notified of the procedure to gain access to and contest their information in the Notification Procedure, Record Access Procedures and Contesting Record Procedures sections as outlined in the SORN RD-2. See Notification Procedure information in 7.1. Record Access Procedures: Individuals wishing to request access to their records should follow the Notification Procedures. Individuals requesting access are also required to provide adequate identification, such as a driver's license, employee identification card, social security card, or other identifying document. Additional identification procedures may be required in some instances. Contesting Record Procedures: Individuals requesting correction or amendment of their records should follow the Notification Procedures and the Record Access Procedures and also identify the record or information to be changed, giving specific reasons for the change.

In general, 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?

See SORN RD-2.

However, in general, 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. The requestor may also refer to the RD-2 SORN for additional information regarding Notification Procedure, Record Access Procedures and Contesting Records Procedures.

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 accounts are not managed by RD Technology Office's 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, the current ATO is valid till 28 October, 2022.

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 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: Human factor: extracting information and using this information erroneously.

MITIGATION: RD has the following controls in place - 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. Audit logs will be reviewed by the DISC Security Division as necessary or as requested 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. RD will comply with the NARA General Records Schedule 31 for the deletion or destruction of information that is no longer needed for administrative, legal, audit, or other operational purposes.

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 prepare reports and 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, the project does not employ technology which raises additional 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, 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 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?

ECM does not use web measurement and customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 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.

Agency Responsible Officials

ANGELA COLE

Digitally signed by ANGELA COLE
Date: 2020.09.17 17:18:21 -04'00'

Angela Cole
Information Systems Security Program Manager (ISSPM)
USDA Rural Development

Agency Approval Signature

MICHAEL GARDNER

Digitally signed by MICHAEL GARDNER
Date: 2020.09.18 14:55:33 -04'00'

Michael S. Gardner
Information System Owner
USDA Rural Development