Sensitive Security Information

Privacy Impact Assessment

eServices

Rural Development (RD)

- 16 August, 2016
- Prepared for:

RD

Abstract

eServices consists of the following modules: Account Cross Reference (ACR), Debarment (dev), Electronic File Transfer (EFT), Enterprise Cash Management Services (ECMS), Mortgage Account Information (MAI), NowChecks, Online Identity Proofing (OIDP), Pre-Authorized Debt (PAD) RD Address Verification (Verification), and Rural Development Utilities Program Customer Initiated Payments (RDUPCIP).

- **ACR** is a secure web service that provides masking and/or unmasking of Borrower IDs through a common lookup TDW data store.
- **Debarment** (Development) is a secure enterprise service providing a single point of integration to GSA System for Award Management (SAM) data and Treasury Do Not Pay data during On-Line Transaction Protocol (OLTP) or batch transaction processing involving individual or business entities request for funding or payment.
- **ECMS** is the web view of the ECMS database which holds all the loan level accounting data (FY's appropriation codes, type of assistance codes, cohorts, Treasury Account Symbols (TAS), etc.) all necessary to derive the component TAS and Business Event Type Code (BETC) required by Treasury.
- **EFT** is a repository of customer banking information that is used to disburse government funds electronically to the customer's bank account.
- **MAI** provides online information to Single Family Housing (SFH) Direct borrowers for the accounts held with Rural Housing Service (RHS).
- **PAD** is a program used for automatic payments of loans.
- **NowChecks** is used to print checks for SFH borrower escrow related disbursements, and certain emergency disbursements, on the LoanServ system.
- **OIDP** is intended to enhance the ability of Rural Development (RD) to serve a larger population of users and improve access to USDA RD web applications..
- **Verification** verifies if the address is valid by using the address verification service that provides real-time access to the Microsoft Bing Geocode service.
- **RDUPCIP** is an electronic collection method enabling borrowers with Commercial program loans being serviced in CLSS to make payments through an on-line collection system.

1 Overview

eServices is a collection of web services that support eGov initiatives and systems that supply customer information and includes the following modules: ACR, Debarment, ECMS, EFT, OIDP, PAD, Verification, and RDUPCIP.

- **ACR** is a secure web service that provides masking and/or unmasking of Borrower Identification numbers (IDs) through a common lookup Tabular Data Warehouse (TDW) data store. The data store was generated using a common hash algorithm against the universe of known Borrower IDs. All communication is encrypted through Secure Socket Layer (SSL). ACR supports several request types:
  - A Borrower ID as input,
  - Multiple Borrower IDs as input,
  - A converted number representing a Borrower ID,
  - Multiple converted numbers representing corresponding Borrower IDs, with corresponding response types respectively:
  - A converted number
  - Multiple converted numbers
  - A Borrower ID
  - Multiple Borrower IDs
- **Debarment** (Development) service leverages a Read Only connection to the TDW to query against the GSA SAM "Exclusions Extract" and SAM "Entity Management Extracts" previously referred to as the Central Contract Registry (CCR).
- **ECMS** is the web view of the ECMS database holding all the loan level accounting data necessary to derive the component TAS and BETC required by Treasury.
- **EFT** used in Automated Multi-Family Housing Accounting System (AMAS) under Multi-Family Management puts funds into a borrowers account. National Financial and Accounting Operations Center (NFAOC) Cash Management division maintains Program Loan Accounting System (PLAS) loans and payee information including bank account and routing numbers.
- **MAI** online information to SFH Direct provides a method for the borrower to schedule a mortgage payment to be drafted from their bank account via ACH.
- **PAD** takes pre-authorized funds from a Borrowers Accounts via EFT for automatic payments of loans allowing withdrawal of pre-authorized cash payment amounts from borrower's bank accounts for Multi-Family Housing and Community Program loans reducing the need to handle cash and check unnecessarily.
- **NowChecks** is a Windows-based Commercial-off-the-Shelf (COTS) software package utilized to disburse RD-SFH borrower escrow related disbursements, and certain emergency disbursements, on the LoanServ system. Approximately $250 million in escrow disbursements are processed annually.
- **OIDP** requires a non-USDA employee (customer) to self-register online through the eAuthentication (eAuth) application, create a user profile account and physically present a government issued identification card to a Local registration Authority (LRA) before an eAuthentication (eAuth) level 2 credential is granted.

- **Verification** validates addresses by using the address verification service providing real-time access to the Microsoft Bing Geocode service.
- **RDUPCIP** enables borrowers (businesses) with Commercial program loans to make payments through an on-line collection system. Customers access the site using eAuthentication (eAuth) level 2 identifications.

NOTE

Per the PTA, Verification and RDUPCIP does not require a PIA and will not be included in the remainder of the document. Debarment will not be included since it is still in development. There is no estimated date at this time for Debarment to go into production; awaiting finalization of Computer Matching Agreement.

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?

ACR: The data represents a translation lookup for the set of all known Borrower IDs.

EFT, PAD, MAI: Bank Account Number, Bank Routing Number, Payment Amount

ECMS

Payee Name
Payee Identifier
State Code
Borrower ID
Loan Number
Account Number
Routing Number
Amount
Agency Identifier
Beginning Period
Availability
Ending Period Availability
Availability Type Code
Main Account Code
Sub Account Code
Business Event Type Code
BETC Description
System
Schedule Number

Payment Date
Agency ACH Text
Payment Type Code
Agency Location Code
Agency Account Identifier
Agency Payment Type Code
ISTOP Offset
ACH Transaction Code
Payment ID
Payment Recipient TIN
Indicator
Addendum Information
Treasury Account Symbol
Sub Level Prefix Code
Allocation Transfer Agency
ID
Account Classification
Amount
Is Credit
Assistance Type
Appropriation Code
Transaction Code
Fiscal Year of Obligation
TAS from Legacy
Tax ID
Individual Name
Eligibility 1099
Loan Type
Borrower Name
Create User
Process (Create) Date
Last Update User
Last Update Date

NowChecks: Payee Name, Check number, check amount, check date, and escrow account number

OIDP: The following information will be collected in session but not stored: Name, Date of Birth, Address, and Social Security Number.

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

PII information is collected, received and shared from other USDA systems.

ACR: CLSS, GLS, MFIS, TDW

EFT, PAD: Information is gathered from a loan payment transaction and sent to the user's bank that was supplied by the user.

ECMS: DLATS EDI, AMAS, CLSS, PLAS, GLS, Treasury TAS/BETC master, NFAOC Legacy System TAS cross-reference and Program Classification

MAI: Data is retrieved by borrower account number.

NowChecks: Information is received from LoanServ application.

OIDP: New required information supplied through a HTTPS web page contained within OIDP, question based information is used to validate identity and response information from user interaction questions.

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

ACR, EFT, PAD: The information is collected to provide an electronic service for the customer.

ECMS: As of October 1, 2014, Treasury requires the United States Department of Agriculture (USDA) to provide the Treasury Account Symbol/Business Event Type Code (TAS/BETC) on all collection / disbursement transactions reported to Treasury. ECMS creates disbursement files that are sent to PAM and SPS. The contents of these files are stored in ECMS database tables to:

- Document the disbursement activity and data sent to Treasury
- Allow reports of the data sent to Treasury

MAI: This used to allow borrowers to schedule loan payments on-line.

NowChecks: Prints disbursement checks written for property taxes, hazard insurance, payoff refunds, and other miscellaneous disbursements.

OIDP: Information is collected, not stored, to validate individual's identity.

1.4 How is the information collected?

ACR: Does not collect information

ECMS: Information is collected through a combination of structured system data loads, treasury TAS/BETC periodic data updates (authoritative source loads), NFAOC accounting codes, and user supplied data collected through secure web pages.

EFT, PAD: Checking Account Number, Bank Routing Number, Payment Amount is the information collected to provide an electronic service for the customer.

MAI: An Application Programming Interface (API) pulls account data from LoanServ and verifies that the user is eligible to make an electronic payment. For a borrower to make a payment using MAI/CIP, they must be current in their payments, and the payment can only be scheduled for the same day.

NowChecks: Information is collected in the LoanServ application.

OIDP: Information is collected via HTTPS session.

1.5 How will the information be checked for accuracy?

ACR, EFT, PAD: Manual inspection by authorized USDA employees.

ECMS: The NFAOC COE and CSC Cash Management staff will manually review for accuracy and will be supported by data quality validation during data collections.

MAI and **NowChecks:** Application software contains internal edits to ensure data integrity.

OIDP: Information collected is validated via Lexis Nexis.

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

Legal Authority: 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.). Additionally, this process is also driven by privacy laws, regulations, and government requirements, including the Privacy Act (5 U.S.C. 552a); the E-Govt. Act, Sec. 208 (44 U.S.C. 3501); the FISMA (44 U.S.C. 3541); OMB Memos M-03-22, M-05-08, M-06-15, M-06-16, M-07-16; OMB Circular A-130, Appendix I.

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 with the type of data

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.

ACR: Provides a single point of integration for all RD systems supporting BorrowerID data collections. ACR is a secure web service that provides masking and/or unmasking of Borrower IDs through a common lookup data store.

ECMS: Customer Information Credit Gateway: A deposit program that Treasury uses for the receipt of federal agency Fedwire and ACH credit transactions.

EFT: Authorization of USDA to perform scheduled EFTs. For RD service desk customers, addresses will be collected to create a uniquely identifiable customer record and occasionally to mail information.

MAI: For a borrower to make a payment using MAI, they must be current in their payments, and the payment can only be scheduled for the same day. CSC processors access MAI in the same manner as a public user. CSC processors may schedule payments on certain delinquent loans, and may schedule a payment up to 15 days in advance.

NowChecks: Prints disbursement checks written for property taxes, hazard insurance, payoff refunds, and other miscellaneous disbursements.

PAD: Authorization of USDA to perform scheduled Pre-Authorized Debits. The PAD system takes pre-authorized funds from a Borrowers Accounts via automatic payments of loans.

OIDP: Information is used to confirm customer identification.

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

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

ECMS: The data consumed, processed, and provided by ECMS is analyzed by Subject Matter Experts using ECMS reports in Excel documents. Also, ETL experts use Informatica to load Data Warehouse subject areas for other Business Intelligence functions.

EFT, PAD: Manual inspection by RD government staff is used to analyze the data. No data is produced.

MAI, NowChecks: Application software contains internal edits to ensure data integrity.

OIDP: Information collected is provided to Lexis Nexis and used to provide Local Registration Authorities (LRA) equivalent identity proofing processes. A successful identity proofing outcome will result in an update to the USDA eAuth 2 Assurance Level value to reflect level 2 assurance

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

ACR: N/A

ECMS: The system uses the Department of Treasury TAS/BETC table data as a read only authoritative data set to map RD specific financial codes to the correct Treasury Account Symbol and Business Event Type Code.

EFT, MAI, NowChecks, PAD: N/A

OIDP: The solutions uses Lexis Nexis data to fulfill identity proofing process requirements to reduce public burden of traveling to a government facility to receive LRA based services.

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 Common Call Components are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1-8, 12, 14, 17, and 19-22), Identification and Authentication (IA-1-7) controls are in place to prevent unauthorized access restricting users from accessing the operating system, other applications or other system resources not needed in the performance of their duties and is restricted by eAuth User Identification (User ID). Authority and Purpose (AP) compensating control gives explanation of why PII is allowed on the system. Systems and Communication Protection (SC-1, 2, 4, 5, 7, 8, 10, 12, 13, 17-23, 28, and 39) controls are in place to prevent unauthorized access.

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?

ACR, EFT, PAD: Information is only retained for the length of time to perform a process.

ECMS: The record retention rules for ECMS have not been defined. In this situation, information is retained until otherwise directed by RD CIO.

MAI: Data is retained in the database for 13 months. However, the NITC Midrange backs up data daily to tape.

NowChecks: Data is retained on the SQL database for approximately 3 months. The CTS EU backs up data daily to tape. Tape backups of all data are stored for 15 years.

OIDP: Information is not retained.

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

ACR, EFT, OIDP, PAD: Data is not retained

ECMS, NowChecks: SOR was completed and submitted to NARA in accordance with Section 207(e) of the E-Government Act of 2002 [44 U.S.C. 3601] and

NARA Bulletins 2008-03, *Scheduling Existing Electronic Records*, and 2006-02, *NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002*.

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

ACR, EFT, PAD: Minimal risk associated, since there is no data retention beyond the time it takes to process the information.

OIDP: No, new data is maintained by this service.

ECMS: Risks associated with length of time data is retained for ECMS have been reviewed. The mitigation strategy is to accept the risk.

MAI, NowChecks: At the end of the retention periods defined in Section 3.1, data is properly destroyed.

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?

ACR: CLSS, GLS, MFIS, PFCS, and TDW – requests are made to ACR web service which in turn performs a lookup in Tabular Data Warehouse (TDW) for account information..

ECMS: AMAS, CLSS, DLATS EDI (LoanServ), GLS, MFIS. Centralized Servicing Center (CSC), Cash Branch and Farm Service Agency cash areas. Payment and Collection information is the type of information shared for appropriate processing purposes

EFT/PAD: EFT/PAD puts funds into a borrowers account for Automated Multi-Housing Accounting System (AMAS) under MFIS.

NowChecks: Information is retrieved from LoanServ for disbursements.

MAI: Information is shared within eServices

OIDP: Information is not shared.

4.2 How is the information transmitted or disclosed?

ACR: Provides a single point of integration for all RD systems supporting BorrowerID data collections. ACR is a secure web service that provides masking and/or unmasking of Borrower IDs through a common lookup data store.

ECMS: Information is transmitted using existing communication channels between RD financial systems creating payment or collection transactions to ECMS.

EFT/PAD: An interface between USDA and US Treasury department for transfer of funds from borrowers through the AMAS operating on a Jakarta Apache web server and Tomcat Server container, and connects to a DB2 database.

MAI: Allows for the user communities to access the MAI application via the front end. The first is public with anonymous authentication (aka no authentication is needed at all). When users access this page, they must register and receive a Level 1 eAuth account to proceed in the MAI application

NowChecks: Information is retrieved via SFTP connection from LoanServ.

OIDP: Information is not shared

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: Minimal information is passed through the applications

Mitigation:

The security and control of PII is the responsibility of the System Owner and RD employees.

The NIST 800-53 controls 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).

OIDP: Information is not shared.

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?

ACR, ECMS, EFT, MAI, PAD, and OIDP: N/A

NowChecks: Via LoanServ, SunTrust Bank - clears the checks.

ECMS: US Treasury – routes all agency collections to the correct treasury processing agent.

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.

Yes, ECMS and NowChecks are covered under SORN RD-1.

ACR, ECMS, EFT, MAI, PAD, and OIDP: N/A

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

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.

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

https://www.federalregister.gov/articles/2014/03/12/2014-05351/privacy-act-of-1974-deletion-of-system-of-records-usdaoes-1-correspondence-and-document-management

ECMS, EFT, PAD, MAI, and NowChecks - Yes

ACR, and OIDP: N/A

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

Yes

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

Yes

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

ACR, ECMS, EFT, PAD, MAI, NowChecks and OIDP - Yes, Individuals willingly participate in providing information for the completion of loan and grant requirements.

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.

ACR, EFT, PAD, NowChecks: Yes, 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.

ECMS, MAI: N/A

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?

ACR, EFT, PAD: 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).

ECMS: N/A

MAI: Customers obtain eAuth Level 1 credentials, then log into MAI using their mortgage account number and the last 4 digits of their SSN.

NowChecks: Visit a local servicing office; call Customer Service, access the IVR; access MAI.

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 the Freedom of Information Officer:

Andrea Jenkins
Freedom of Information Officer
Rural Development, USDA
7th Floor, Reporter's Bldg.
Washington, DC 20250
Andrea.Jenkins@wdc.usda.gov
(202) 692-0029

MAI, NowChecks: Call customers call CSC Customer Service or submit written request.

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.

ACR, EFT, PAD: Information is disseminated through annual Point-of-Contact (POC) training and users of PAD have the ability to update their information which is disseminated when they sign their consent form to use the service.

MAI: CSC Customer Service provides that information during the phone conversation; or the IVR recommends they speak to a Customer Service Representative; or the back of the billing statements provide all the contact information.

NowChecks: Information is provided on the billing statement, they can access MAI or RD Home Loans web page.

ECMS: N/A

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.

ACR, EFT, PAD: 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.

MAI: With the information provided on the back of the billing statement, customers can access MAI, and then can access the RD Home Loans web page. Additionally, customers can call the Interactive Voice Response (IVR) or Customer Service.

NowChecks: Information is provided on the billing statement, they can access MAI; they can access the RD Home Loans web page.

ECMS: N/A

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

ACR, ECMS, EFT, OIDP, and PAD: No additional risks are associated with the redress process.

MAI and NowChecks: Customers must provide specific information in order to gain access to any of their loan information, regardless of the method used.

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 are discussed in detail in the System Security Plan (SSP) 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 (UAM) Team relies on a POC supplying the correct UserID and password. UAM tickets are the tool used to track authorized requests by approving 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, Department contractors have access according to the NIST 800-53 controls are discussed in detail in the AC and Configuration Management (CM) controls.

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

USDA RD requires annual Information Security and Awareness Training (ISAT) 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 USDA 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?

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 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.

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 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?

ACR, EFT, PAD: Commercial-off-the-shelf (COTS) applications and Government developed software.

ECMS is a CLP Framework program which is a collection of open source frameworks and technologies.

MAI: public website. First time users to the MAI web site access the http:\\pubmai.sc.egov.usda.gov website using their loan account number and the last 4 digits of their social security number.

NowChecks: An application used to process escrow files and print checks for the disbursements.

OIDP: An application used to identify customers based on their public record and information with the ability to score the responses and make an identity proofing decision.

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"?

eServices does not use 3rd party websites and/or applications.

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

eServices does not use 3rd 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.

eServices does not use 3rd 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?

eServices does not use 3rd 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?

eServices does not use 3rd 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?

eServices does not use 3rd 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?

eServices does not use 3rd 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?

eServices does not use 3rd 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)?

eServices does not use 3rd party websites and/or applications

10.10 Does the system use web measurement and customization technology?

eServices does not use 3rd party websites and/or applications

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?

eServices does not use 3rd party websites and/or applications

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.

eServices does not use 3rd party websites and/or applications

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: 2016.11.15 15:19:18 -06'00'

Mike Sutton
Chief, Enterprise Technology Branch

ROBERT BOZADA Digitally signed by ROBERT BOZADA
Date: 2016.11.16 14:02:32 -06'00'

Janet Havelka
Chief, Mortgage Loan Technology Branch

Approval Signature

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: 2016.11.16 15:39:38 -06'00'

Diego Maldonado
Information Systems Security Program Manager