

Privacy Impact Assessment eServices

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: December 31, 2019
- Prepared for: USDA OCIO-Policy,
E-Government and Fair Information
Practices (PE&F)





Privacy Impact Assessment for the eServices

February 4, 2020

Contact Point

Angela Cole

Rural Development Business Center, ISSPM

(202)-401-0757

Reviewing Official

Michael S. Gardner

System Owner (SO)

United States Department of Agriculture

(202) 692-0212

Abstract

eServices are a collection of web services that support eGov initiatives and systems that supply customer information. eServices consist of the following components: Account Cross Reference (ACR), Debarment, Electronic File Transfer (EFT), Enterprise Cash Management Services (ECMS), Enterprise Notification Service (ENS), Mortgage Account Information (MAI), Now Checks, Pre-Authorized Debt (PAD), RD Address Verification (Verification), and Rural Development Utilities Program Customer Initiated Payments (RDUPCIP). This PIA is required because there is PII data in eServices with the components and the PTA determined that a PIA is required.

Overview

eServices are a collection of web services that support eGov initiatives and systems that supply customer information and includes the following modules: ACR, Debarment, ECMS, EFT, ENS, MAI, NowChecks, PAD, RD Address 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, multiple borrower IDs, a converted number representing a borrower ID, and multiple converted numbers representing corresponding borrower IDs.

Debarment 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 Transactional Processing (OLTP) or batch transaction processing for individual or business entities requesting funding or payment.

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) 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.

Now Checks 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.

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.

RD Address Verification takes an address and verifies if the address is valid by using the address verification service that provides real-time access to the Microsoft Bing Geocode service.

RDUPCIP provides secure internet connectivity to RD customers for making an online loan payment and processes their requests through Pay.gov. The RDUPCIP flow begins with a Public request to make a loan payment. Customers access the site using E-Authentication, Level 2. RDUPCIP integrates with E-Authentication for authentication services and interfaces to RD business services provided by the loan payment authorization and loan payment processing. Pay.gov receives batch payment requests from RDUPCIP and provides a batch response. The Batch response is provided to the commercial financial system for account balancing processes. Physical server equipment and current operating system configurations is provided by the NITC platform.

Debarment, EFT, ECMS, PAD and RDUPCIP use E-Authentication, Level 2. ACR and MAI use E-Authentication, Level 1 and Now Checks and RD Address Verification do not require authentication.

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 general public
- Address Information
- Personal identification number
- Miscellaneous identification numbers
- SSN

Debarment:

- The general public
- Name
- Date and/or place of birth
- Address Information
- Personal identification number
- SSN



EFT:

- The general public
- Name
- Address Information
- Personal identification number
- Financial data
- Miscellaneous identification numbers
- SSN

ECMS:

- USDA employees
- Name
- Address Information
- Miscellaneous identification numbers

ENS:

- USDA employees
- Name
- Address Information

MAI:

- The general public
- Name
- Financial data
- Miscellaneous identification numbers

Now Checks:

- USDA employees
- The general public
- Name
- Address Information
- Miscellaneous identification numbers

PAD:

- USDA Partner
- Name
- Personal identification number
- Financial data
- Miscellaneous identification numbers
- SSN

RD Address Verification:

- Address information

RDUPCIP:

- The general public
- Name
- Address Information
- Financial data
- Miscellaneous identification numbers
- SSN

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

ACR: CLSS, GLS, GUS, MFIS, PFCS and TDW

Debarment: ECMS and TDW

ECMS: AMAS, CLSS, DLATS EDI, GLS, MFIS, PLAS, and TDW

ENS: ECMS and ECF

EFT/PAD: AMAS, GLS, and PLAS

MAI: ECMS and LoanServ

Now Checks: LoanServ

RDUPCIP: Pay.gov batch processes and need to verify other sources of information for this?

RD Address Verification: Bing Geocode Service is used

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

ACR does not collect information.

EFT and PAD collect information to provide an electronic service for the customer.

Debarment tracks ECMS disbarments and business processes to Treasury Do Not Pay and GSA SAM during On-line Transactional Processing (OLTP) or batch transaction processing for individual or business entities requesting funding or payment.

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 the data is sent to Treasury. 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 provides this required financial reporting to Treasury.



ENS accepts a complete message body or values for template place holder fields, then connects to the SMTP server and sends email messages on behalf of consumer applications.

MAI enables borrowers to schedule loan payments on-line.

Now Checks prints disbursement checks written for property taxes, hazard insurance, payoff refunds, and other disbursements.

RD Address Verification uses Bing, but this information is not collected, disseminated or maintained, but rather accessed and used to verify an address. RD Address Verification is not applicable for information collection.

RDUPCIP provides secure internet connectivity to RD customers for making an online loan payment and processes their requests through Pay.gov. The RDUPCIP flow begins with a Public request to make a loan payment.

1.4 How is the information collected?

ACR does not collect information.

Debarment uses the System for Award Management (SAM) site to connect to the Treasury Do Not Pay for individuals on the debarment list. The login has a portal, which uses individual user credentials to determine, if they can proceed to make a payment. SAM pulls data containing the debarment information, which is integrated with eServices.

ECMS collects information through a combination of structured system data loads, Treasury TAS/BETC periodic data updates, NFAOC accounting codes, and user supplied data provided through secure web pages.

EFT and PAD collect checking account number, bank routing number, payment amount to provide an electronic service to the RD customer.

ENS accepts a complete message body or values for template place holder fields, then connects to the SMTP server and sends email messages on behalf of consumer applications.

MAI has 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.

RD Address Verification does not collect information, it uses Bing to verify addresses of RD customers.

RDUPCIP facilitates online loan payments for RD customers.

1.5 How will the information be checked for accuracy?

The data is verified by authorized RD staff with regular review and verification as part of the normal workflow for eServices components. Authorized RD Staff routinely review the information to ensure its accuracy as part of the normal workflow for eServices applications.

RD customers can contact authorized RD staff for eServices components to make necessary corrections to RD customer data that is not accurate. Data integrity controls protect the data from accidental or malicious alteration or destruction and provide assurance that the data is valid.

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

Information in eServices falls under the following:

- *Privacy Act of 1974, as Amended (5 USC 552a);*
- *Computer Security Act of 1987, Public Law 100-235, ss 3 (1) and (2), codified at 15 U.S.C. 272, 278 g-3, 278 g-4 and 278 h which establishes minimum security practices for Federal computer systems;*
- *OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, which establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems;*
- *Freedom of Information Act, as Amended (5 USC 552), which provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy.*
- *Federal Information Security Modernization Act of 2014*
- *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).*
- *Farm Bill 2018 (P.L. 115-334)*
- *Fair Credit Reporting Act, 15 USC 1681 a(f)*
- *Consumer Credit Protection Act, 15 USC 1601*
- *Equal Credit Opportunity Act, 15 USC 1691*
- *The Fair Debt Collection Practices Act, Pub. L 111-203, title X, 124, Stat. 2092 (2010)*
- *7 CFR, section 3560, subsections 55 and 154*
- *RD Records Management Policy*
- *NARA Records Retention*

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

The privacy risk is the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the RD customer.

The eServices system owners define access roles to ensure separation of duties, account management and authorized access to data and information in eServices, which is hosted on the NITC platform, with the exception of Now Checks, which is hosted in the CEC environment. Only authorized RD staff can access the eServices applications using E-Authentication and some eServices applications require E-Authentication for RD customers. Debarment, EFT, ECMS, PAD and RDUPCIP use E-Authentication, Level 2. ACR and MAI use E-Authentication, Level 1 and Now Checks and RD Address Verification do not require authentication. These measures mitigate the risks to privacy data in eServices. Since eServices components are hosted on the NITC platform and Now Checks by CEC, both NITC and CEC comply with all security and privacy protections required by USDA as a federal agency.

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 borrower ID data collections. ACR is a secure web service that provides masking and/or unmasking of borrower IDs through a common lookup data store.

Debarment 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 Online Transactional Processing (OLTP) or batch transaction processing for individual or business entities requesting funding or payment.

ECMS uses the Customer Information Credit Gateway, which is a deposit program that Treasury uses to receive Fedwire and ACH credit transactions.

EFT is used to send an electronic funds transfer for RD service desk customers. For EFT, addresses are collected to create a uniquely identifiable customer record and sometimes to mail information. EFT is an interface between USDA and US Treasury department to ensure timely transfer of funds from borrowers through the Automated Multi-Housing Accounting System (AMAS).

ENS accepts a complete message body or values for template place holder fields, then connects to the SMTP server and sends email messages on behalf of consumer applications. This relay server uses the localhost's email server for automatic distribution of email messages. ENS is an email proxy service that provides ability for client applications to establish and manage email subscribers and email templates.

MAI is used by RD borrower to make a payment. For a RD borrow to use 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 the RD customer. CSC processors may schedule payments on specific delinquent loans, and may schedule a payment up to 15 days in advance.

Now Checks prints disbursement checks written for property taxes, hazard insurance, payoff refunds, and other disbursements.

RD Address Verification takes an address and verifies if the address is valid by using the address verification service that provides real-time access to the Microsoft Bing Geocode service.

The PAD system takes pre-authorized funds from a borrower’s account for the automatic payments of loans. Multi-Family Housing (MFH) and PLAS borrowers that mail paper checks to RD for the installment payments may register for PAD transactions. When a borrower registers for PAD, their payment is made via EFT from their bank account or designated management agent’s bank account through an Automated Clearing House (ACH) to Rural Development. Authorized RD staff in Multi-Family Housing (MFH) Servicing Offices and Finance Offices, Cash Management Branch use EFT.

RDUPCIP provides secure internet connectivity to RD customers for making an online loan payment and processes their requests through Pay.gov. The RDUPCIP flow begins with a Public request to make a loan payment. Customers access the site using E-Authentication, Level 2.

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

Authorized RD staff manually review eServices information to ensure that RD loan and grant information is accurate and meets the RD and USDA requirements.

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

Unclear as to whether Debarment and ECMS use data from SSA Master Death Index and Treasury, respectively? This data might not fall under commercial or publicly available data?

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The controls in place to detect unauthorized access to eServices information include NITC audit logs/security logs and CEC audit logs. There are logs for E-Authentication, which is how the authorized RD staff identify and authenticate to access eServices components.

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?

eServices information is retained in accordance with NARA, RD Records Management policy and financial compliance regulations.

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

Yes, eServices follow data retention as provided by the RD Records Management, which is in accordance with NARA.

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

eServices data retention has the potential risk of unauthorized access, unauthorized disclosure or illegal use of the customer PII data.

eServices data is protected by NITC and CEC, which follow USDA federal agency requirements for data protection. NITC is accredited by FedRAMP. All eServices components, except Now Checks are hosted on the NITC platform. Now Checks is hosted in the Client Experience Center (CEC) End User Computing environment. eServices follow the RD Records Management data retention requirements to manage risk associated with data retention.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The following eServices applications share data with the following internal RD applications:

ACR shares information with CLSS, GLS, GUS, MFIS, PFCS and TDW from requests made to the ACR web service, which performs a lookup in Tabular Data Warehouse (TDW) for account information.

Debarment shares information with TDW and ECMS, which tracks disbarments and processes with Treasury and GSA.



ECMS shared information with AMAS, CLSS, DLATS EDI (LoanServ), GLS, MFIS, PLAS, and TDW. Customer Servicing Center (CSC), Cash Branch and Farm Service Agency cash areas share payment and collection information for financial processing.

EFT and PAD place funds into a borrower's account for Automated Multi-Housing Accounting System (AMAS) under MFIS and GLS.

ENS shares information with ECMS and ECF.

MAI information is available to CSC personnel working in the areas that process Customer Initiated Payments and pulls account data from LoanServ.

NowCheck information is retrieved from LoanServ for disbursements.

4.2 How is the information transmitted or disclosed?

The information within the eServices applications is transmitted using HTTPS. The information that is shared internally is within the USDA network using DISC's technical protections in place to protect the data with security and privacy protections.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The privacy risk is the unauthorized access and potential compromise of PII data in eServices.

This privacy risk is mitigated by NITC platform and CEC for Now Checks, which host eServices and provides security and privacy data protection and complies with USDA requirements on protecting information. Also, authorized RD staff and authorized RD customers access eServices using E-Authentication, so there are audit logs on this activity. Debarment, EFT, ECMS, PAD and RDUPCIP use E-Authentication, Level 2. ACR and MAI use E-Authentication, Level 1 and Now Checks and RD Address Verification do not require authentication.

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?

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

Debarment: System for Award Management (SAM) site connects into Treasury (Do Not Pay) to retrieve information on persons listed on debarment list.

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, USDA/Rural Development 1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs covers the routine use of this information with the external trusted sources described in section 5.1.

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

Information is shared via online file transfer using SFTP, HTTPS and SSH. Intrusion Detection is provided by the host network at each location. Containment control is achieved by enforcing host network segmentation to isolate major portions of the host network from a security breach. Interconnection Security Agreements (ISA) and Memorandum of Understanding (MOU) agreements are in place for all connections.

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

The risk to external information sharing would be the unauthorized disclosure of statement and tax report information, borrower information and accounting information. This is mitigated by the security protections, such as firewalls, DNSSec, encryption of data in transit, and DISC audit logs. Only authorized RD staff have direct access to eServices and RD has continuous monitoring from DISC in compliance with FISMA and as required by RD and USDA. eServices data is stored in a secure environment on the DISC platform.

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.

Yes, it follows Rural Development 1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants and Other Participants in RD Programs, <https://www.govinfo.gov/content/pkg/FR-2016-04-28/pdf/2016-09938.pdf>

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

Yes, notice was provided to the individual prior to the collection of information through the use of Form RD 410-9, Statement Required by the Privacy Act, which is provided before a RD customer utilizes the Debarment, EFT, ECMS, PAD, RDUPCIP, ACR, MAI and Now Checks application. RD Address Verification does not require authentication or notice, since it does not collect information from an individual.

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

Individuals have the opportunity and/or right to decline to provide information, but if they decline, then they will not be able to apply for the eServices financial service. With the RD Form 410-9, Statement Required by the Privacy Act, individuals agree to provide the information, so RD customers are aware of the collection of personal information.

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

No, in order to apply for an eServices financial service, the RD customer consents to the collection of personal information as required for eServices financial service. The RD customer provides their consent as part of the eServices financial services with RD Form 410-9, Statement Required by the Privacy Act

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.

RD customers consent to providing information for the completion of eServices financial services. RD customers are notified with the privacy form, RD Form 410-9, when they apply for eServices financial services and consent to the use of their data before this information is provided.

Risks associated with individuals being unaware of the collection are mitigated because RD individual customers must consent to the use of their data and this notification is included in the privacy form that is completed as part of the process for applying for eServices financial services with RD.

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?

RD customers have access to their eServices information from the review and workflow processing by RD staff. The RD staff member will keep the RD customer informed as to the status of their eServices financial service.

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

If a RD customer notices inaccurate information with their eServices financial service, then they will contact the RD staff for correction of any erroneous information. The RD staff member will facilitate the correction of any inaccurate information for the RD customer.

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

Notification is part of the application process for eServices financial services, so the RD customer can contact the appropriate RD staff member to correct any inaccurate information. Also, RD staff involved in processing the eServices applications do manual review and will contact the RD customer for any information corrections with their financial service.

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

Individuals have access, redress, and amendment rights under the Privacy Act and the Fair Credit Reporting Act.

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

Privacy risks associated with redress available to individuals are compromise of PII data involved in the redress activity.

This is mitigated by RD staff acting as responsible data stewards of the RD customer's information and from the network security protections in place for the eServices applications from NITC and CEC, which host eServices applications and from USDA. Any redress information with eServices financial services is protected in accordance with RD policy, which follows USDA security and privacy protections as provided by OMB and USDA policy.

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?

Desk Procedures document the User Access Management (UAM) Team process for establishing, activating, and modifying individual users for eServices. The group and account types are defined by the System Owners for the eServices components. The System Point of Contact (POC) assigns group membership and determines individual RD user access. The UAM Team creates, modifies and deletes user requests approved by the System Point of Contact.

RD employees and RD contractors access eServices after being provisioned in E-Authentication by a User Access Management (UAM) ticket, created by the System POC and completed by the UAM Team (UAMT).

Steps to provision RD employees and RD contractors follow desk procedures as set by the system owners for eServices components.

8.2 Will Department contractors have access to the system?

Yes, RD contractors are required to undergo the same access and authentication procedures that RD federal employees follow, as discussed in section 8.1.

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

Yes, all RD employees and contractors are required to complete annual information security and awareness training, which includes privacy training for eServices.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, eServices has an ATO, which is in CSAM.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

eServices complies with the Federal Information Security Modernization Act of 2014 (FISMA) by documenting the Authorization and Accreditation, annual control self-assessments, and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 4. eServices components, except Now Checks, are hosted on the NITC platform at USDA, which is FedRAMP certified and follows USDA security and privacy requirements. Now Checks is hosted on the CEC environment, which follows USDA security and privacy requirements.

Access to eServices is controlled through E-Authentication for authorized RD staff and with applicable eServices applications (Debarment, EFT, ECMS, PAD, RDUPCIP, ACR and MAI), for RD customers, and access to sensitive information is controlled through NITC Profiles/Groups on a need-to-know basis with audit logs of user activity for eServices. Section 5 of this PIA describes security protections in place for eServices data.

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?

Since eServices is used by authorized RD staff and RD customers using E-Authentication and there are group access management controls, the privacy risks are minimal. Potential compromise of privacy data is mitigated by NITC and CEC audit event monitoring and USDA network security protections in place to protect RD data for eServices components. Additionally, eServices applications are accessed using E-Authentication by RD staff and RD customers through the USDA network.

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?

eServices are a collection of web services that support eGov initiatives and systems that supply customer information and includes the following modules: ACR, Debarment, ECMS, EFT, ENS, MAI, NowChecks, PAD, RD Address 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, multiple borrower IDs, a converted number representing a borrower ID, and multiple converted numbers representing corresponding borrower IDs.

Debarment 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 Transactional Processing (OLTP) or batch transaction processing for individual or business entities requesting funding or payment.



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) 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.

Now Checks 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.

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.

RD Address Verification takes an address and verifies if the address is valid by using the address verification service that provides real-time access to the Microsoft Bing Geocode service.

RDUPCIP provides secure internet connectivity to RD customers for making an online loan payment and processes their requests through Pay.gov. The RDUPCIP flow begins with a Public request to make a loan payment. Customers access the site using E-Authentication, Level 2. RDUPCIP integrates with E-Authentication for authentication services and interfaces to RD business services provided by the loan payment authorization and loan payment processing. Pay.gov receives batch payment requests from RDUPCIP and provides a batch response. The Batch response is provided to the commercial financial system for account balancing processes. Physical server equipment and current operating system configurations is provided by the NITC platform.

Debarment, EFT, ECMS, PAD and RDUPCIP use E-Authentication, Level 2. ACR and MAI use E-Authentication, Level 1 and Now Checks and RD Address Verification do not require authentication.

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

No, the project utilizes Agency approved technologies for eServices components and these technology choices do not raise privacy concerns.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

Yes, the system owner and the ISSPM have reviewed the OMB memorandums.

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

Not applicable, eServices do 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.

Not applicable, eServices do 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?

Not applicable, eServices do 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?

Not applicable, eServices do 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?

Not applicable, eServices do 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?

Not applicable, eServices do 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?

Not applicable, eServices do 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)?

Not applicable, eServices do not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

Not applicable, eServices do 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?

Not applicable, eServices do 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.

Not applicable, eServices do not use 3rd party websites and/or applications.



Responsible Officials

Angela Cole
Information Systems Security Program Manager (ISSPM)
Rural Development
United States Department of Agriculture

Approval Signature

Michael S. Gardner
System Owner
Rural Development
United States Department of Agriculture