Privacy Impact Assessment CLP Shared Services 6 of 7 - eServices

- Version: 4.0
- Date: April 25, 2023
- Prepared for: USDA Rural Development (RD)

United States Department of Agriculture

Privacy Impact Assessment for the

CLP Shared Services 6 of 7 - eServices

April 25, 2023

Contact Point

RDPrivacy@usda.gov
Rural Development, Cyber Security Division
United States Department of Agriculture

Abstract

eServices is an area boundary that includes a collection of web services that support eGovernment initiatives and systems. Each of these services provide Rural Development with functionality to mask PII, verify accounts, process payments, transfer funds, and maintain federal reporting requirements with U.S. Treasury.

This PIA is required, under the E-Government Act of 2002, because the following eServices modules process PII: Account Cross Reference (ACR), Enterprise Cash Management System (ECMS), Electronic Funds Transfer (EFT), Mortgage Account Information (MAI), and Now Checks.

Overview

eServices is an area boundary that includes a collection of web services that support eGovernment initiatives and systems. Each of these services provide Rural Development with functionality to mask PII, verify accounts, process payments, transfer funds, and maintain federal reporting requirements with U.S. Treasury. The following applications process PII:

Account Cross Reference (ACR) is a secure web service that provides masking and/or unmasking of Borrower Identification numbers (IDs) 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. ACR collects PII, including but not limited to social security numbers (SSNs) from members of the program participants, and creates a spoofed number using a system algorithm.

Enterprise Cash Management System (ECMS) currently holds Disbursement, Cash Tracking and Collection Reconciliation information. ECMS processes PII, specifically full names, address information, SSN/Tax Identification Number (TIN), miscellaneous identification numbers, and borrower's banking account number(s) program participants, from LoanServ.

Electronic Funds Transfer (EFT) maintains a repository of bank account and routing information for parties who may receive disbursements for GLS, AMAS and PLAS. The information is used to support the electronic funds transfer of a disbursement when an EFT account is available for a payee in each of the systems. The application is used by internal Field Office users of each of the respective Loan areas. EFT collects PII, including but not limited to the borrower's full name, address information, SSN, personal identification number, financial data, and miscellaneous identification numbers from program participants.

Mortgage Account Information (MAI) provides online information to Single Family Housing Direct borrowers regarding the accounts they hold with Rural Housing Service (RHS). MAI allows borrowers to make direct payments to RHS. MAI collects and maintains PII, specifically the borrower's full name, last 4 digits of SSN, financial data, and miscellaneous identification numbers from program participants.

Now Checks is a Windows-based commercial-off-the-Shelf (COTS) package used to print checks for RD-SFH borrower escrow related disbursements, and certain emergency disbursements, on the LoanServ system. Approximately $250 million in escrow disbursements are processed annually. The Now Checks daily check file is imported as a text file to Bank of America's CashPro Online web page. Now Checks collects and maintains PII of RD borrowers for the purposes of processes checks.

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?

eServices' modules process PII to service and disburse payments related to RD customers' loans and grants. Specifically, each application processes various types of PII from program participants:

- **ACR** processes social security numbers (SSNs) from RD program participants to create a spoofed number using a system algorithm;
- **ECMS** processes full names, address information, SSN/TIN, agency assigned numbers, and financial data;
- **EFT** processes borrower's full name, address information, SSN, financial data, and agency assigned numbers;
- **MAI** processes full names, financial data, agency assigned numbers; and
- **Now Checks** processes the borrowers' full name, agency assigned numbers, and financial information.

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

- **ACR** receives its data from other USDA source systems, specifically CLSS, Guaranteed Loan System (GLS), Guaranteed Underwriting System (GUS2), Multi- Family Integrated System (MFIS), and the Program Fund Control System (PFCS).
- **ECMS** receives the data from other USDA source systems, specifically AMAS, CLSS, LoanServ, GLS, MFIS, and PLAS.
- **EFT** receives data from other USDA source systems, specifically AMAS, GLS, and PLAS.
- **MAI** receives data from LoanServ.
- **Now Checks** receives data from LoanServ.

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

- **ACR** – masks SSNs to be used in other applications
- **ECMS** – to document the disbursement activity and the data is sent to Treasury
- **EFT** – is a repository of customer banking information and serves as an interface between USDA and US Treasury department to ensure timely transfer of funds from borrowers.
- **MAI** – to enable borrowers to schedule loan payments on-line

- **Now Checks –** to process disbursement checks for taxes, hazard insurance, payoff refunds, and other disbursements.

1.4 How is the information collected?

- **ACR** – does not collect information; applications make calls to mask data.
- **ECMS** - collects information through a combination of structured system data loads, Treasury TAS/BETC periodic data updates, Servicing Office accounting codes, and user supplied data provided through secure web pages.
- **EFT –** receives disbursement payments calls from MAS, GLS, and PLAS.
- **MAI –** makes API calls to LoanServ to validate account.
- **Now Checks –** LoanServ provides the information to be printed on checks.

1.5 How will the information be checked for accuracy?

Information is checked for accuracy at the initial point of collection.

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

- Privacy Act of 1974, as Amended (5 U.S.C. § 552a)
- OMB Circular A-130, Managing Information as a Strategic Resource, July 2016
- Freedom of Information Act, as amended (5 U.S.C. § 552)
- Federal Information Security Modernization Act of 2014 (also known as FISMA), (44 U.S.C. §3551), December 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 U.S.C. §1681f
- Consumer Credit Protection Act, 15 U.S.C. §1601, et. seq.
- Equal Credit Opportunity Act, 15 U.S.C. §1691, et. seq.
- The Fair Debt Collection Practices Act, 15 U.S.C. §162, et. seq.
- 7 CFR Part 3550, Direct Single Family Housing Loans and Grants
- 7 CFR Part 3555, Guaranteed Rural Housing Program
- 7 CFR Part 3560, Direct Multi-Family Housing Loans and Grants

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

MODERATE RISK. eServices privacy risks centers around unauthorized disclosure use of PII and the potential adverse consequences would have on the RD customer in the event of a breach. Only authorized RD staff can access the eServices applications using E-Authentication. ACR, ECMS, EFT, Now Checks use E-Authentication, Level 2. MAI use E-Authentication, Level 1. These measures mitigate the risks to privacy data in eServices.

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 –** masks SSNs to be used in other applications
- **ECMS** – information is used report required financial transaction to U.S. Treasury
- **EFT –** information is used to send an electronic funds transfer for RD service desk customers
- **MAI** – PII information is used to validate accounts
- **Now Checks** – information is used to process disbursement checks

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

Tools are not used with eServices.

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

N/A

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

The controls in place to detect unauthorized access to eServices information or transactions include audit/security logs. There are logs for eAuthentication.

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 data is not scheduled and therefore held permanently.

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

No.

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

HIGH RISK: The risk associated with maintaining data permanently is high.

MITIGATION: RD is in the process of scheduling system records. Until eServices records are scheduled, the data is safeguarded in accordance with NIST 800-53 security controls.

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** processes social security numbers (SSNs) from RD program participants to create a spoofed number using a system algorithm for GLS, RDForce, MFIS, and PFCS.
- **ECMS** processes full names, address information, SSN/TIN, agency assigned numbers, and financial data from AMAS, GLS, LoanServ, MFIS, PLAS. The data is sent to Treasury to document disbursement activity.
- **EFT** processes borrower's full name, address information, SSN, financial data, and agency assigned numbers from AMAS, GLS, and PLAS to provide an Electronic Funds Transfer and Pre- Authorized Debit service for RD program participants.
- **MAI** processes full names, financial data, agency assigned numbers from LoanServ to enable borrowers to schedule loan payments on-line.
- **Now Checks** processes the borrowers' full name, agency assigned numbers, and financial information from LoanServ to process disbursement checks for taxes, hazard insurance, payoff refunds, and other disbursements.

4.2 How is the information transmitted or disclosed?

eServices is an area boundary that includes a collection of web service that use Hypertext Transfer Protocol Secure (HTTPS). The information that is shared internally is within the USDA network using technical protections in place to protect the data with security and privacy protections. USDA security requirements are implemented to protect the data in eServices and as it flows internally.

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.

MODERATE RISK. The privacy risk is associated with the unauthorized access and potential compromise of PII data.

MITIGATION: This privacy risk is mitigated with internal security and privacy controls outline in the System Security Plan. Access is limited to authorized personnel using E-Authentication. Audit logs are maintained to monitor activity.

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?

Now Checks: The Now Checks daily check file is imported as a text file to Bank of America's CashPro Online web page and includes the borrower/payee's full name, amount, check number and date. This exchange allows Bank of America to provide disbursement services for the escrow account balances maintained by USDA for real estate taxes, insurance premiums, and loan closings for the Single-Family Housing Loan Program borrowers. RD has a relationship with Proctor Insurance to send Automated Clearing House (ACH) to various State Farm insurers for pay-outs.

ECMS: ECMS sends the borrower's full name, bank account number, routing number, amount, account types, Treasury Account Symbol, and Business Event Type Code to U.S. Department of Treasury's Treasury Web Application Infrastructure's (TWAI) Pay.Gov. The purpose of the exchange is to route 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, SORN 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?

Data files are sent between Bank of America and NowCheck via Single File Transfer Protocol (SFTP).

The interconnection between TWAI and ECMS is through a Virtual Private Network (VPN) using AES-256 encryption or Hypertext Transfer Protocol Secure (HTTPS) (256 bit Transport Layer Security) to registered Internet Protocol (IP) addresses.

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

MODERATE RISK. The risk is related to the unauthorized disclosure of statement and tax report information, borrower information, and federal public funds accounting information.

MITIGATION: The risk is mitigated by the security protections, specifically firewalls, DNSSec, encryption of data in transit, and audit logs. Only authorized RD staff have direct access to eServices. RD has continuous monitoring processes to comply with FISMA requirements.

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.

No, eServices is not the initial point of collection.

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

No, eServices is not the initial point of collection.

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

No, eServices is not the initial point of collection.

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, eServices is not the initial point of collection.

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.

No, eServices is not the initial point of collection.

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?

No, eServices is not the initial point of collection.

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

eServices is not the initial point of collection.

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

eServices is not the initial point of collection.

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

eServices is not the initial point of collection.

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

LOW RISK: eServices is not impacted by risks associated with redress. Risk is associated with the applications collecting information initially.

MITIGATION: Any redress information with RD financial services is protected by security and privacy protections as outlined in the System Security Plan.

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?

RD employees and RD contractors are required to obtain appropriate Level access via e-Authentication. 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, see 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.

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

Yes, eServices has an Authorization to operate (ATO), which is valid until 3/12/2023.

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 access management requirements and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53. eServices applications follow USDA security and privacy requirements.

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?

MODERATE RISK: The risk is related to the unauthorized disclosure of statement and tax report information, borrower information, and federal public funds accounting information.

MITIGATION: The risk is mitigated by the security protections, specifically firewalls, DNSSec, encryption of data in transit, and audit logs. Only authorized RD staff have direct access to eServices. RD has continuous monitoring processes to comply with FISMA requirements.

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 to streamline financial services to customers and Federal reporting and accounting obligations.

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.

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 memoranda.

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

N/A.

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

N/A.

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

N/A.

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?

N/A.

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

N/A.

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

N/A.

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?

N/A.

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)?

N/A.

10.10 Does the system use web measurement and customization technology?

N/A

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

10.12 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.

N/A

Approval Signature

Signed copy kept on record