Privacy Impact Assessment
CLP Shared Services 1 of 7 - AMP

Policy, E-Government and Fair Information Practices

- Version: 1.3
- Date: May 7, 2020
- Prepared for: Rural Development (RD)

United States Department
of Agriculture

Privacy Impact Assessment for the

CLP Shared Services 1 of 7 – AMP

05/07/2020

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

Automated Mail Processing (AMP): Rural Development Operations and Management (RD-O&M) provides financial enterprise print and mail-handling services to the entire RD mission area, the St. Louis Farm Service Agency (FSA), Grain Inspection, Packers and Stockyards Administration (GIPSA). RD, FSA, and GIPSA depend on these enterprise print and mail-handling services to produce and distribute financial and management reports, as well as loan servicing and customer notification correspondence for all program areas. This PIA was conducted based on information obtained through the system's Privacy Threshold Analysis (PTA) and mandated by M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* Overview.

Overview

AMP is an enterprise print and mail-handling service that produces and distributes financial and management reports, as well as loan servicing and customer notification correspondence as outlined in the above paragraph. The volume of printed material exceeds 36.6 million pages per year and supports an average of 475,000 pieces of metered mail per month.

AMP consists of three components: Mail Preparation, Printing, and Mail Insertion.

Mail Preparation – Has three components, including Elixir software, Group 1 software and RDLETR. Elixir software builds form templates for customer correspondence and is maintained on premise at the Deputy Chief Information Officer (DCIO), with a password being required to log on to the Customer Experience Center (CEC) controlled computer. Group 1 software is hosted on a mainframe platform, which is administered and operated by the USDA's Digital Information Service Center (DISC). Access to the mainframe portion of AMP is controlled. The software packages from Group 1 software provide for address data entry, correction, deliverability, standardization, zip code correction and additions; certify the accuracy of mail and maximize postal discounts for all classes of mail; create presort mailings, separate mail and determine which letters will be mailed and which letters will be rejected among other functions. Additionally, this software creates the Mail Run Data File (MRDF) which is used by Mail Insertion. RDLETR program is written by RD DCIO staff and coordinates the Group 1 software to process data from financial systems of record and produces a Print Stream (information received from and converted to hard copy loan servicing documents and IRS tax forms) and corresponding MRDF (used for mail insertion, processing, and control purposes only). Merged letters are processed in an automated mail job, which prepares the batch of mail for printing.

Printing – Consists of a server, printers and workstation that provides the platform for the Queue Manager. The server receives print jobs from the DISC mainframe. The Queue Manager workstation is connected to the network and receives and displays the print jobs received by the server and controls the printers and job stream control. The printers print the jobs produced by the Mail Preparation system.

Mail Insertion – Contains hardware components located on premise at an RD secure location, and includes Inserters, an InSite Importer and Pitney Bowes servers. The Inserters automatically insert customer correspondence into envelopes, print the address on the envelopes, and then meter them for processing by the USPS. InSite Importer handles the import of the MRDF (from mail preparation) and the printed output (from printing) to produce inserted mail pieces ready to send to USPS for delivery. Mail insertion and reporting function uses the MRDF to match pre-printed correspondence to system addressed envelopes. The Pitney Bowes servers provide operational services, performed by the DirectConnect application, and a platform for DFWorks application. Server #1 acts as the gateway to the USDA network and receives the MRDF, and connects to the Pitney Bowes internal private network, located on premise at an RD secure location. Server #1 hosts the FTP service that is controlled by a USDA managed password. Server #2 hosts the DFWorks application and provides an interface to the DirectConnect application. The services on Server #2 are not accessible remotely from outside of the USDA network. The MRDF file is retained by the DirectConnect server for 60 days, after which it is automatically deleted.

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?

Print Stream: Borrower and co-borrower names and addresses, social security numbers (last four positions), account numbers, client names and addresses, business financial data and debt payment information; lender identification numbers, lender names, addresses, and business financial data; and producer name, address, and business financial data.

Mail Run Data File (MRDF): Borrower and co-borrower name(s) and address(es).

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

AMAS, CLSS, GLS, LoanServ, MFIS, and PLAS (owned by FSA).

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

Print Stream: Information is received and converted from the System of Record (SOR) to hard copy loan servicing documentation and IRS tax forms.

MRDF: Mail insertion, processing, and control purposes only.

1.4 How is the information collected?

Print Stream: RDLETR program is written by RD DCIO staff and coordinates the Group 1 software, hosted on the mainframe, to process data from financial systems of record and produces a Print Stream.

MRDF: Mainframe mail processing software creates Mail Run Data File.

1.5 How will the information be checked for accuracy?

Accuracy checks are incorporated into the operation of the system at various checkpoints.

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

- 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.

Given the amount/type of PII collected, low privacy risk was identified. AMP processes PII information from Systems of Record (SOR) located in a secure network environment within USDA. Any PII information is automatically deleted within 60 days of the creation of the print job. The information printed is PII so therefore the privacy controls must be applied. See the System Security Plan (SSP) security controls DM 1 & 2.

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.

Print Stream: Information is used in financial and management reports, as well as loan servicing and customer notification correspondence.

MRDF: Mail insertion, processing, and control purposes only.

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

Software hosted on a mainframe platform, administered and operated by DISC, creates the MRDF. RDLETR program produces the Print Stream.

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

N/A. No commercial or publicly available data is used.

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 AMP are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1-8, 11, 12, 14, 17, 18, 19, 20 and 22), Identification and Authentication (IA-1-8) controls are in place to prevent unauthorized access. Compensating controls of AP-02, Purpose Specification control is to give an explanation of why PII is allowed on your system and MP-1 Media Protection Policy and Procedures for how to properly mark the printed documentation. Systems and Communication Protection

(SC 4, 5, 7, 8, 10, 12) controls are in place to erase memory in printers, remove media, internal traffic enhance protection, and protect the PII by keeping patches up to date

The equipment is in a secure environment (PE-2 and PE-3) where access is only granted to Mission Support Division (MSD) employees, Pitney Bowes Customer Service Engineers and a small group of other authorized personnel. Access to space is granted with a LincPass (or USDA-RD issued site badge).

The mainframe is managed and controlled by DISC. Access to the AMP software at DISC is controlled by ACF2, which is administered by the Technology Office IT Helpdesk.

Access to AMP functions is controlled by individual password-protected accounts for each system. Login can only be performed by physical access to consoles within the AMP equipment room.

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?

Once the job has been deemed complete, by the designated USDA administrator, the job will be manually closed.

The mail run/job will remain on InSite's Production Display for 24 hours (DM-01); thereafter, at which time the Importer will automatically archive the job and remove it from the production display.

MRDF file is retained in DirectConnect server for 60 days, after which it is automatically deleted.

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

AMP will comply with the requirements of 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.

Low risk, as the MRDF file is automatically deleted after 60 days.

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?

AMAS, CLSS, GLS, LoanServ, MFIS – Loan information is submitted to AMP through the use of software on the Mainframe to create a Print Stream and the MRDF file is used for mail insertion, processing and control purposes.

4.2 How is the information transmitted or disclosed?

Loan information is submitted to AMP through the use of software on the mainframe to create a Print Stream and the MRDF file is used for mail insertion, processing and control purposes.

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:

Privacy risk to AMP is low, as the mainframe is administered and operated by DISC on premises at the Enterprise Data Center (EDC), a USDA facility. Access to mainframe is controlled. In addition, DISC provides protection to the data in transit and at rest

Mitigation:

The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality.

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?

Information is not shared from AMP to external organizations.

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.

Information is not shared from AMP to external organizations.

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

Information is not shared from AMP to external organizations.

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

Information is not shared from AMP to external organizations.

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. Information is not collected by AMP from any individuals. The Systems of Record, AMAS, CLSS, GLS, LoanServ, MFIS, are covered by SORN RD-1; Program Loan Accounting System (PLAS), which is owned by FSA, is covered by SORN USDA FSA-14.

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

Information is not collected by AMP from any individuals.

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

Information is not collected by AMP from any individuals.

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

Information is not collected by AMP from any individuals.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Information is not collected by AMP from any individuals. Notice to any individuals would be provided by the Systems of Record (SOR).

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?

Information is not collected by AMP from any individuals. Each System of Record would be responsible for providing access to individuals.

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

Information is not collected by AMP from any individuals. Each System of Record would be responsible for correcting inaccurate or erroneous information.

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

Information is not collected by AMP from any individuals. Each System of Record would be responsible for providing notification to individuals of the procedure for correcting their information.

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

Information is not collected by AMP from any individuals.

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

Information is not collected by AMP from any individuals.

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?

Operations Support Branch (OSB) determines which employees have access to the AMP system described in the following security controls PS-02, PS-03, PS-07 within the National Financial and Accounting Operations Center (NFAOC) organization.
The mainframe is managed and controlled by DISC. Access to the AMP software at DISC is controlled by ACF2.
Access to AMP functions is controlled by individual password-protected accounts for each system. Login can only be performed by physical access to consoles within the AMP equipment room, which is located on premise at a secure RD location.

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?

USDA RD requires annual Information Security and Awareness training for all employees and contractors. Training must be completed with a passing score prior to access to a USDA RD system.

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

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

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?

Privacy risk to AMP is low, as the mainframe is administered and operated by DISC on premises at the Enterprise Data Center (EDC), a USDA facility. Access to mainframe is controlled. DISC provides protection to the data in transit and at rest. Access to AMP functions by RD is controlled by individual password-protected accounts for each system. Login can only be performed by physical access to consoles within the AMP equipment room, which is located on premise at a secure RD location. The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality.

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?

Rural Development Operations and Management (RD-O&M) provides financial enterprise print and mail-handling services to the entire RD mission area, the St. Louis Farm Service Agency (FSA), Grain Inspection, Packers and Stockyards Administration (GIPSA), and other on-demand Federal agencies that are crucial to effective and efficient program delivery. RD, FSA, and GIPSA depend on these enterprise print and mail-handling services to produce and distribute financial and management reports, as well as loan servicing and customer notification correspondence for all program areas.

AMP is an enterprise print and mail-handling service that produces and distributes financial and management reports, as well as loan servicing and customer notification correspondence as outlined in the above paragraph. The volume of printed material exceeds 36.6 million pages per year and supports an average of 475,000 pieces of metered mail per month.

AMP consists of three systems: Mail Preparation, Printing, and Mail Insertion.

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

Yes, the AMP project uses software to process data from financial systems of record and produce a Print Stream to hard copy loan servicing documentation and IRS tax forms. Additionally, AMP uses software via the mainframe to create the MRDF, used for mail insertion, processing and control purposes. AMP also uses a Queue Manager to receive and display print jobs received from the server and uses the FreeFlow application to manage and process the printing process. FreeFlow is a raster image processing (RIP) and print management controller.

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, AMP 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.

Not Applicable, AMP 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?

Not Applicable, AMP 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?

Not Applicable, AMP 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?

Not Applicable, AMP 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?

Not Applicable, AMP 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?

Not Applicable, AMP 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)?

Not Applicable, AMP does not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

No, AMP does not use web measurement and customization technology.

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

No, AMP does not use web measurement and customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable, AMP does not use 3rd party websites and/or applications.

Agency Responsible Officials

ANGELA COLE

Digitally signed by ANGELA COLE
Date: 2020.05.07 12:39:13 -04'00'

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

Date

Agency Approval Signature

MICHAEL GARDNER

Digitally signed by MICHAEL GARDNER
Date: 2020.05.07 15:26:28 -04'00'

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

Date