Privacy Impact Assessment (PIA)

Automated Mail Processing (AMP)

Rural Development (RD)

- May 30, 2017
- Prepared for: RD

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	07/08/2016	ISSS/SN	Transitioned to FY16 template
1.1	05/30/2017	ISSS/TW	Updated with Solimar addition

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.

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. *Any of the above PII data resides outside the AMP accreditation boundary and is not stored in AMP.*

Mail Run Data File (MRDF): Name and address.

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

AMAS, CLSS, GLS, LoanServ, MFIS, and FSA [which includes Program Loan Accounting System (PLAS)].

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: Information is not collected by AMP, it is transitory and not stored in A

MRDF: Mainframe mail processing software creates file.

1.5 How will the information be checked for accuracy?

N/A

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

Legal Authority: 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.).

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, no risk were identified. Since the information is transitory, the information is not collected and stored in AMP, however its source systems are located in a secure network environment with limited access to users with proper system user identification (UserID) and password. 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?

N/A

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 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 NITC. Access to the AMP software at NITC is controlled by ACF2, which is administered by the Information Systems Security Staff (ISSS).

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 mailrun/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.

Archived jobs will remain accessible through InSite's Archive Warehouse object for 60 days; thereafter, after which time the Importer removes them altogether from the system.

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

N/A

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

MRDF is of minimal risk since it is manually 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 Mainframe via MRDF file for processing.

4.2 How is the information transmitted or disclosed?

N/A – information is transitory and not collected..

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:

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

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?

N/A – information is transitory and not collected and/or shared.

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.

N/A – information is transitory and not collected and/or shared.

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

N/A – information is transitory and not collected and/or shared.

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

N/A – information is transitory and not collected and/or shared.

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 transitory and not stored; additionally, AMAS, CLSS, GLS, LoanServ, MFIS are covered by SORN RD-1; FSA [which includes Program Loan Accounting System (PLAS) is covered by SORN USDA FSA-14.

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

N/A – information is not collected by AMP

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

N/A – information is not collected by AMP

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

N/A - information is not collected by AMP

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.

N/A - information is not collected by AMP

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?

N/A - information is not collected by AMP

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

N/A - information is not collected by AMP

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

N/A - information is not collected by AMP

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

N/A - information is not collected by AMP

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

N/A - information is not collected by AMP

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 NITC. Access to the AMP software at NITC is controlled by ACF2, which is administered by the Information Systems Security Staff (ISSS).

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.

8.2 Will Department contractors have access to the system?

Yes

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

USDA RD requires annual Information Security and Awareness training for all employees and contractors. RD is responsible for ensuring all new employees and contractors have taken the Department Security Awareness Training developed by Office of Chief Information Officer-Cyber Security. Training must be completed with a passing score prior to access to a USDA RD system. All RD employees/contractors are required to complete Computer Security Awareness Training 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?

No risk incurred. However, to further secure the system and data the following security controls are in place and fully documented in the SSP: AC and IA controls defining access; AU controls defining auditable events; PE controls discussing the physical security of the system;nd SI controls to ensure data integrity.

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?

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.

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

Yes. Pitney Bowes manages each integrity breach with the highest priority and uses the information gathered to not only fix the problem, but also to develop new capabilities to protect against future occurrences. One of those capabilities is their Strict Integrity tools.

These tools set report and protect the critical software settings that implement our integrity features. These tools and settings were developed over a period of two years and incorporate the knowledge and experience of their development, applications, and field systems engineers. While every inserting system is customized to some degree, these settings reflect the "best practices" that they have developed from installing and responding to their customers worldwide. All errors of this type are also reviewed for exposure to their install base and appropriate upgrades are made, if necessary.

The Strict Integrity tools have been deployed beginning April of 2011 on many Pitney Bowes customer's machines. It is a standard for all new factory builds. On machines running this version of software and settings, their data to date indicates that over 700 million mail pieces have been produced without a single report of an integrity error.

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"?

AMP 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?

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?

No

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 <u>Privacy Impact Analysis</u>: 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

Responsible Officials

JANET HAVELKA Digitally signed by JANET HAVELKA Date: 2017.08.08 09:08:37 -05'00'

Janet Havelka
Chief, Mortgage Loan Technology Branch

Approval Signature

signed for

EUGENE TEXTER Digitally signed by EUGENE TEXTER Date: 2017.08.08 09:04:19 -05'00'

Diego Maldonado
Information Systems Security Program Manager