USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: Rural Development

System Name: Automated Mail Processing

System Type: ☒ **Major Application**
□ **General Support System**
□ **Non-major Application**

System Categorization (per FIPS 199): □ **High**
☒ **Moderate**
□ **Low**

Description of the System:

Application/System Environment

The software applications described in the following paragraphs are utilized by the AMP system to generate the mail outputs.

The Xerox Elixir DesignProTool software application used to create forms is maintained at the Rural Development Deputy Chief Information Officer (DCIO) Staff in St. Louis, Missouri, on a Common Computing Environment (CCE) compliant PC. The underlying operating system (OS) is Windows XP Professional. A password is required to login to the ITS controlled computer.

All Pitney Bowes Group1 software is used for the US Postal Service Coding Accuracy Support System (CASS) compliance; e.g., FINALIST, MailStream Plus, and StreamWeaver.

Pitney Bowes Application/System Environment: The Automated Mail Processing (AMP) system's Pitney Bowes mail insertion and reporting system processes Name and Address information to match loan servicing and customer notification correspondence. The system uses a mainframe addressing file called the Mail Run Data File (MRDF) to match pre-printed correspondence to system addressed envelopes.

1. For each Print Job, a corresponding MRDF is created and downloaded to a share on the PB Fileserver.
2. The InSite Importer (InSite01) polls the PB Fileserver for newly downloaded MRDF's. When it detects a new MRDF, it validates that it's not a duplicate job and that its record format/structure is correct. If no issues are detected, the Importer will "import" the file into the production environment. If issues are detected, the Importer will highlight the respective MRDF with a red background for further (offline) analysis by lead USDA personnel.

3. Once an MRDF is successfully imported, it is assigned a state of "Ready" and becomes available to the production inserting equipment for processing (i.e., the Inserters and Manual Handling Workstations). Once processing starts on the mailrun, its state changes to "Processing".
4. After 1st-pass processing has been completed on the mailrun, the job is ready for reconciliation and reprint submission. The process of reconciling the job can be performed at either the Inserter or an InSite Workstation, whereas the process of creating the Reprint File can be performed at an InSite Workstation by a Key Operator or higher-level user or at the Inserter.
5. Whenever a Reprint File is created, the mailrun's state changes to "Rework". Both the Reprint File and Output File reside on a shared folder on the PB Fileserver.
6. The mailrun remains in the "Rework" state until all mailpieces have been successfully rendered (i.e., either machine inserted or manually handled). Note that the reprinted mailpieces are assigned their original barcode and processed against their original MRDF, thus a new MRDF does not get created for reprint jobs. This process is often referred to as "closed-loop" processing, as the mailrun remains active until all mailpieces have been successfully rendered against it.
7. Once the job has been deemed complete, by the designated USDA administrator, the job will be manually closed.
8. The mailrun/job will remain on InSite's Production Display for 24 hours thereafter, at which time the Importer will automatically archive the job and remove it from the Production Display.
9. Archived jobs will remain accessible through InSite's Archive Warehouse object for two-months thereafter, after which time the Importer removes them altogether from the system.

This process is controlled and managed by two Pitney Bowes Applications: DFWorks and Direct Connect.

DF works is a proprietary Java application with resident user and account management. It provides a front end to the Direct Connect application an provides performance reporting metrics.

The Direct Connect application control the function of the inserters, hosts the MRDF during operations, tracks mail efficiency, and provides DFWorks report data.

Xerox 4635 high-speed printers with EPS controller Application/System Environment: The EPS controller receives print jobs from the NITC mainframe and prints local reports as well as loan processing and customer notification correspondence. It uses the

Document Services Platform (DocuSP) application to manage and process the printing process.

DocuSP (Document Services Platform) is a raster image processing (RIP) and print management controller for production-class printers in the Xerox DocuPrint and DocuTech families.

DocuSP provides queue management, job processing, and printer control capabilities.

For Production Printing, DocuSP provides the critical features required for the transactional printing market. Xerox LCDS (Line Conditioned Data Stream) is handled as a native PDL, including DJDE's and Metacode support. Job Streaming mode allows printing of long jobs without the usual queue size constraints or delays in receiving an entire job before printing. And since you need a printer that can handle more than just your transactional printing, DocuSP with LCDS can also print PostScript, PDF, PCL5e and TIFF jobs. Currently, DocuSP LCDS is available in the DocuPrint 180 EPS.

DocuSP is scalable. Based on the Sun Ultra Sparc workstation, DocuSP can drive printers from the 65 PPM DocuTech 65 up to the DocuPrint 900 Plus, a 900 PPM production printing and publishing system.

None of the components of the AMP system are located in a harsh environment. The AMP software runs on the NITC mainframe which is not under the direct control of Rural Development.

Who owns this system? (Name, agency, contact information)

Name	Peggy Stroud
Title	Director, Enterprise Systems Design and Development Division
Address	USDA Rural Development 4300 Goodfellow Blvd, FC-42 St. Louis, MO 63120
Email address	Peggy.Stroud@stl.usda.gov
Phone Number	(314) 457-5080

Who is the security contact for this system? (Name, agency, contact information)

Designated Approval Authority	Eugene Texter
Title	Information Security Staff Team Lead
Address	USDA Rural Development 4300 Goodfellow Blvd, FC-44 St. Louis, MO 63120
Email address	eugene.texter@stl.usda.gov
Phone Number	(314) 457-4778

Who completed this document? (Name, agency, contact information)

Name	Janet Havelka
Title	Chief, Mortgage Loan Technologies Branch
Address	USDA Rural Development 4300 Goodfellow Blvd, FC-424 St. Louis, MO 63120
Email address	Janet.Havelka@stl.usda.gov
Phone Number	(314) 457-4980

Name	Greg Lovett
Title	Chief, Support Services Branch
Address	USDA Rural Development 4300 Goodfellow Blvd St. Louis, MO 63120
Email address	Greg Lovett@st.usda,gov
Phone Number	(314) 457-4332

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	Yes	Yes
Social Security Number	Yes	No
Telephone Number	No	No
Email address	No	No
Street address	Yes	No
Financial data (i.e. account numbers, tax ids, etc)	Yes	No
Health data	No	No
Biometric data	No	No
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code[1]	No	No
Are social security numbers embedded in any field?	Yes	No
Is any portion of a social security numbers used?	Yes	No
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	Yes	No

If all of the answers in Questions 1 and 2 are NO, STOP

You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

DATA COLLECTION

3. Generally describe the data to be used in the system.

Data is received from the Systems of Record (SOR) containing the following categories:

Customer Information: Borrower and co-borrower names and addresses; social security numbers; account numbers; client names and addresses; and business financial data and debt payment information.

Lender Information: Lender Identification Numbers, lender names, addresses, and business financial data.

Producer Information: Producer name, address, and business financial data.

4. Is the collection of the data both relevant and necessary to the purpose for which the system is designed? In other words, the data is absolutely needed and has significant and bearing on the system's purpose.

☒ Yes
☐ No. If NO, go to question 5

4.1. Explain.

The SOR data is used for generating proper distribution of mail correspondence and financial management and loan servicing reports. This data is transitory and is not stored in this system.

5. Sources of the data in the system.

5.1. What data is being collected from citizens and/or employees?

Not applicable. The output data printed and/or mailed by the AMP System is obtained from the SOR received from the agency or program area.

5.2. What USDA agencies are providing data for use in the system?

Rural Development
Farm Service Agency (FSA)
Natural Resources Conservation Service (NRCS)
Grain Inspection, Packers and Stockyards Administration (GIPSA)

5.3. What government agencies (state, county, city, local, etc.) are providing data for use in the system?

Not Applicable.

5.4. From what other third party sources is data being collected?

Not Applicable.

6. Will data be collected from sources outside your agency? For example, citizens and employees, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

□ Yes
☒ No. If NO, go to question 7

This data is not collected by AMP. It is transitory.

6.1. How will the data collected from citizens and employees be verified for accuracy, relevance, timeliness, and completeness?

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?

DATA USE

7. Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?

This data is not collected by AMP. It is transitory and is not stored in this system. The data is used for the generating proper distribution of mail correspondence and financial management and loan servicing reports.

8. Will the data be used for any other purpose?

□ Yes
☒ No. If NO, go to question 9

8.1. What are the other purposes?

9. Is the use of the data both relevant and necessary to the purpose for which the system is being used? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose.

☒ Yes
□ No. If NO, go to question 10

9.1. Explain.

This data is not collected by AMP. It is transitory and is not stored in this system. The data is used for the generating proper distribution of mail correspondence and financial management and loan servicing reports.

10. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

□ Yes
☒ No. If NO, go to question 11

10.1. Will the new data be placed in the individual's record (citizen or employee)?

□ Yes
□ No

10.2. Can the system make determinations about citizens or employees that would not be possible without the new data?

□ Yes
□ No

10.3. How will the new data be verified for relevance and accuracy?

11. Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?

This data is not collected by AMP. It is transitory. The data is used for the generating proper distribution of mail correspondence and financial management and loan servicing reports.

12. Will the data be used for any other purpose (other than indicated in question 11)?

□ Yes
☒ No. If NO, go to question 13

12.1. What are the other purposes?

13. Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

□ Yes
☒ No. If NO, go to question 14

This data is not consolidated by AMP. It is transitory.

13.1. What controls are in place to protect the data and prevent unauthorized access?

14. Are processes being consolidated?

□ Yes
☒ No. If NO, go to question 15

Processes are not consolidated by AMP. It is transitory.

14.1. What controls are in place to protect the data and prevent unauthorized access?

DATA RETENTION

15. Is the data periodically purged from the system?

☒ Yes
□ No. If NO, go to question 16

15.1. How long is the data retained whether it is on paper, electronically, in the system or in a backup?

Mail Data Run Files (MRDF) are retained for 60 days and then manually deleted per Operations and Scheduling Branch standard operating procedures.

15.2. What are the procedures for purging the data at the end of the retention period?

Operators manually delete obsolete or aged MRDF file using the Connect:Direct software.

15.3. Where are these procedures documented?

Procedures are on file with the Mission Support Division, Operation and Schedule Branch.

16. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

MRDF files as required for forensics of the mail insertion process.

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

☒ Yes
□ No

DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

□ Yes
☒ No. If NO, go to question 19

18.1. How will the data be used by the other agency?

18.2. Who is responsible for assuring the other agency properly uses of the data?

19. Is the data transmitted to another agency or an independent site?

□ Yes
☒ No. If NO, go to question 20

19.1. Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

19.2. Where are those documents located?

20. Is the system operated in more than one site?

□ Yes
☒ No. If NO, go to question 21

20.1. How will consistent use of the system and data be maintained in all sites?

DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

Schedulers, programmers, system operators, system administrators, and contractors have access to read only SOR data. Access is granted on a need-to-know basis.

22. How will user access to the data be determined?

AMP system access is controlled by User ID and password. Access rights are granted to designated individuals only when a written request is approved by their supervisor, the site system manager, and the ISSPM.

A behavioral set of rules has been established for this system and is enforced by an intricate network of user ID's and passwords, along with limited access to restricted areas. The rules of behavior have clearly defined the responsibilities and expected behavior of all individuals with access to the system. The rules are clear about the consequences of behavior not consistent with the rules. They are in writing and form a basis for computer security awareness activities and training.

Managers and high-level technical staff are responsible for ensuring individuals comply with published rules of behavior.

22.1. Are criteria, procedures, controls, and responsibilities regarding user access documented?

☒ Yes
□ No. If NO, go to question 23

22.2. Where are criteria, procedures, controls, and responsibilities regarding user access documented?

Information Systems Security Staff Intranet web site.

23. How will user access to the data be restricted?

Privileges granted are based on job functions and area of authority.

23.1. Are procedures in place to detect or deter browsing?

☒ Yes
□ No

23.2. Are procedures in place to detect or deter unauthorized user access?

☒ Yes
□ No

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

☒ Yes
□ No

CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the citizens and employees affected by the interface (i.e. office, person, departmental position, etc.)?

AMP Subsystems – Pitney Bowes inserters, Xerox high-speed printers – Janet Havelka and Greg Lovett

AGLO Domain – Chris Kendrick

WAN and LAN – Gary Davis

SOR – ITPM for applicable systems

Rural Development ISPM

26. How can citizens and employees contact the office or person responsible for protecting their privacy rights?

Dorothy Hinden
Freedom of Information Officer
Rural Development, USDA
7th Floor, Reporter's Bldg.
Washington, DC 20250
Dorothy.Hinden@wdc.usda.gov
(202)692-0031

27. A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

☒ Yes - If YES, where is the breach notification policy located?

- U.S. Department of Agriculture Incident Notification Plan September 2007

- DM3505-001 USDA Computer Incident Response Procedures Manual.

- Computer Incident Response Standard Operating Procedures (CIRT)

☐ No - If NO, please enter the POAM number with the estimated completion date:

28. Consider the following:

- Consolidation and linkage of files and systems
- Derivation of data
- Accelerated information processing and decision making
- Use of new technologies

Is there a potential to deprive a citizens and employees of fundamental rules of fairness (those protections found in the Bill of Rights)?

☐ Yes
☒ No. If NO, go to question 29

28.1. Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of citizens and employees?

DM 3515-002, section e states:

To fulfill the commitment of the USDA to protect customer and employee data, several issues must be addressed with respect to privacy:
1 The use of information must be controlled; and
2 Information may be used only for a necessary and lawful purpose.

Where Public Affairs systems of records are involved:
1 Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them;
2 Information collected for a particular purpose should not be used for another purpose without the subject's consent unless such other uses are specifically authorized or mandated by law; and
3 Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

Also, P.L. 95-454, the Civil Service Reform Act of 1978 which is enforced by The U.S. Equal Employment Opportunity Commission (EEOC) ensures the equitable treatment of the employees.

30. Is there any possibility of treating citizens and employees differently and unfairly based upon their individual or group characteristics?

□ Yes
☒ No. If NO, go to question 31

30.1. Explain

SYSTEM OF RECORD

31. Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

☒ Yes
□ No. If NO, go to question 32

31.1. How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

MRDF file contains non-sensitive data fields, such name and address.

31.2. Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov)

USDA RD-1

31.3. If the system is being modified, will the SOR require amendment or revision?

No.

TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

□ Yes
☒ No. If NO, the questionnaire is complete.

32.1. How does the use of this technology affect citizens and employees privacy?

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO
THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE/CYBER SECURITY

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Automated Mail Processing
(System Name)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

Janet Havelka — 3/7/2008
System Manager/Owner — Date
OR Project Representative
OR Program/Office Head.

Brenda Dinges — 3/7/08
Agency's Chief FOIA officer — Date
OR Senior Official for Privacy
OR Designated privacy person

3/17/08
Agency OCIO — Date