USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: USDA Rural Development

System Name: Imaging

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

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

Description of the System:

The Imaging system was instituted because of the Paperwork Reduction Act. In an effort to comply with the ruling it was necessary to institute a set of distributed systems that would not only scan in old documents but also process new documents electronically.

Using scanning software and equipment the Imaging application provides storage of electronic images of loan application documents and other paper requests sent to the Rural Development agency. As a result, this system provides an electronic means to view over 79 million images. Access to documents is provided through client server and intranet based applications.

Who owns this system?

Kathy Anderson
Branch Chief, Enterprise Technology Branch (ITPM)
USDA Rural Development
4300 Goodfellow Blvd. Bldg 104
St. Louis, MO 63120
kathy.anderson@stl.usda.gov
314-457-5012

Who is the security contact for this system?

Eugene Texter
Information System Security Staff
USDA Rural Development
Building 105, FC-44
4300 Goodfellow Boulevard
St. Louis, MO 63120
eugene.texter@stl.usda.gov
314-457-4778

Brenda Dinges
Information System Security Program Manager
USDA Rural Development
Building 105, FC-44
4300 Goodfellow Boulevard
St. Louis, MO 63120
brenda.dinges@stl.usda.gov
314-457-4772

Who completed this document?

Kathy Anderson
Branch Chief, Enterprise Technology Branch (ITPM)
USDA Rural Development
4300 Goodfellow Blvd. Bldg 104
St. Louis, MO 63120
kathy.anderson@stl.usda.gov
314-457-5012

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

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	**Yes**	**No**
Social Security Number	**Yes**	**No**
Telephone Number	**Yes**	**No**
Email address	**Yes**	**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]	**Yes**	**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.)?	**No**	**No**

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

   Imaging provides electronic processing of loan applications and other paper requests coming into the Rural Development (RD) agency. This system provides an electronic means to access past loan documents. This system essentially serves as an electronic file storage center.

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.

   Yes. The data is stored electronically in support of the Paperwork Reduction Act.

5. Sources of the data in the system.

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

   Privacy Act protected information to include (but not limited to): SSN, Taxpayer Identification (ID) Numbers, debt payment information, addresses.

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

   Rural Developments, Rural Housing Service and Rural Utility Service offices provide documents to CSC to be scanned into the Imaging system.

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

   Some documents may originate at other Federal Agencies; however those agencies have no direct input into the Imaging System. No state and local agencies provide data for Imaging System.

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

   There are no third party sources.

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

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

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

All data stored within the Imaging system is a scanned copy of the original source documents and provides electronic storage of the original documents. Each document is scanned, visually reviewed and verified for Quality Assurance.

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

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?

Imaging provides electronic processing of loan applications and other paper requests coming into the Rural Development (RD) agency. This system provides an electronic means to access past loan documents. This system essentially serves as an electronic file storage center.

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.

Yes. The data is stored electronically in support of the Paperwork Reduction Act.

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. The system does not derive new data. Data aggregation results only from scanned data that already exists.

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

N/A

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

No. The "System" does not make determinations but systems users input answers into the system for tracking.

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

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?

Same as the principle purpose (see # 7)

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?

N/A

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. No processes or data is consolidated with Imaging.

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

NIST 800-53A controls for the imaging system are discussed in detail in the System Security Plan.

14. Are processes being consolidated?

☐ Yes
☒ No. If NO, go to question 15

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

See 13, 13.1 (Same as above)

DATA RETENTION

15. Is the data periodically purged from the system?

☐ Yes
☒ No - Data is kept indefinitely via optical storage MSAR. The scanned documents are destroyed after 30 days.

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

Data is kept indefinitely via optical storage MSAR. The scanned documents are destroyed after 30 days.

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

N/A

15.3. Where are these procedures documented?

N/A

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?

The Imaging system contains read-only static imaged documents that do not change.

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

☒ Yes – All data in use is necessary.
☐ 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 -

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

No other agencies share data or have access to the Imaging System.

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

The system owner

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

    Front-end Imaging components are hosted through USDA RD in St. Louis, MO. Concerning FAX and Scan services and inputs, users at different sites all use consistent Imaging processing controls, guidance, and agency driven policies.

    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?

    There are no external connections to the Imaging System

    19.2. Where are those documents located?

    N/A

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

    ☐ Yes
    ☒ No

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

    N/A

DATA ACCESS

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

    The Imaging system will be available to system users, managers, and Imaging Systems Administrators who are granted access to the system based on job function and need-to-know.

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

Access is controlled by userID and password. Access rights are granted to designated individuals only when a written request is approved by their supervisor. The User Access Management Team (UAMT) follow their procedures to provide access to the system. The ISSS personnel approve and process elevated access requests. The procedures are documented.

Desk Procedures document the process for establishing, activating, and modifying IDs. System Owners define this process. System Owners define Groups and account types. System Point of Contact assigns group membership and determines Need-to-know validation. The POC is responsible for verifying user identification; the User Access Management Team (UAMT) relies on a POC supplying the correct userid and password to Logbook to identify themselves. Log Book tickets are the tool used to track authorized requests by approving Point of Contact (POC)

Currently RD reviews reports from HR on a Bi-weekly basis. The organization employs

automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are not used or authorized. ISSS UAM Team does not manage Guest and Anonymous accounts. POCs (empowered by RD IT managers) are responsible for notifying UAMT if access or roles need to be modified and periodically reviewing and certifying established access.

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?

See # 22

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

See # 22

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

☒ Yes–

Imaging log files are created which include transaction history and an event file.
The audit log consists of user id's, application accessed, type of event and success or failure, in addition to the audit log a report is generated daily showing all non-successful events. These logs are e-mailed and reviewed daily by QFlow.
Audit trails are designed and implemented to record appropriate information that can assist in intrusion detection. The audit trails include sufficient information to determine the type of event, when it occurred, the user ID associated with the event, and the command/program used to initiate the event. Access to these logs is restricted to the system administrators

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

☒ Yes – See 23
☐ No

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

☒ Yes – See 23
☐ No

CUSTOMER PROTECTION

26. 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.)?

The System/Application Owner

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

Citizens and employees may contact the Freedom of Information Officer:

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

28. 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)

29. 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

29.1. Explain how this will be mitigated?

30. 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.

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

☐ Yes
☒ No. See Above.

SYSTEM OF RECORD

32. 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

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

Yes. Some data can be retrieved by SSN. In some program areas, the borrowers ID is used to identify the borrower

32.2. 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)

Imaging Operates under SOR USDA/RURAL DEVELOPMENT RD -1 System name: Applicant, Borrower, Grantee, or Tenant File.

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

Changes to the applications are controlled by specific written requests for automation or changes to the Imaging (and other) systems. Upon evaluation, if any such changes could result in modifying the data collection or processing characteristics of the system, the system and data owners will update this Privacy Impact Assessment. The updated PIA would then be used to amend the applicable Privacy Act of 1974 Federal Register publications and postings if need be.

Rural Development's SDLC and CM process requires the ISSS to review system changes for security documentation updates and re-accreditation decisions impact to ensure that the system SORN is revised as needed.

TECHNOLOGY

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

No, the system is not using technologies in ways that the USDA has not previously employed.

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

N/A

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 Imaging System

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.

Kathy Anderson — 6/26/08
System Manager/Owner — Date

Brenda Dinges — 6/30/08
Brenda Dinges - Agency's Chief FOIA Officer — Date

John E. Distler — 6/26/08
John Distler - DCIO — Date