Privacy Impact Assessment (PIA)

Farm Service Agency

Document Imaging Systems (Filenet)

KCFRB Imaging (FRB)
Receivable Case Management Application (RCMA)
Receivable Imaging System (RIS)
Tobacco, Finance, IRS (TFI)

Revised: February 2018

Template Version: FSA-PIA-2013-08-19

Document Information

System Owner Contact Information	
Name	Sieg, Angela
Contact Number	816-926-1568
E-mail Address	Angela.Sieg@kcc.usda.gov

Document Revision History		
Date MM/DD/YYYY	Author Name & Organization	What was changed?
04/28/2014	Charlene Niffen - ISO	Initial creation

DOCUMENT REVIEW

Reviewer	Title	Date	Update: Y/N	If systemic, please provide comments
	Information System Owner	N/A	N/A	Yearly review no changes needed

Table of Contents

Purpose of Document

USDA DM 3515-002 states: “Agencies are responsible for initiating the PIA in the early stages of the development of a system and to ensure that the PIA is completed as part of the required System Life Cycle (SLC) reviews…” and “New systems, systems under development, or systems undergoing major modifications are required to complete a PIA.”

This document is being completed in accordance with NIST SP 800-37 Rev 1 which states, “The security plan also contains as supporting appendices or as references to appropriate sources, other risk and security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and continuous monitoring strategy.”

Abstract

Name of the component and system: Document Imaging Systems (Filenet)

Brief description of the system and its function: The Document Imaging System (FileNet) is a Commercial-off-the-Shelf (COTS) client-server application that stores financial information images in the form of PDF and Tiff files. It allows for the input of pertinent Consolidated Financial Management Information Systems (CFMIS) investment documents for storage and retrieval. All data is directly input by the user from electronically stored documents, faxed, and scanned materials. Additionally, FileNet controls the workflows associated with the financial information being imaged. FileNet allows client access from desktop browser to the stored images on a network device managed by the server. Storage of financial records, debts, debtors, and other information to the server uses Netapp Snaplock which is controlled by the server software. The server utilizes a SQL database to manage document indexes and workflow process. The FileNet system resides on the OCIO-CTS network, which is managed by the CTS-CS and CTS SES divisions of CTS.

Why the PIA is being conducted: To support federal law, regulations and policies.

System Information	
Agency:	Farm Service Agency
System Name (Acronym):	Document Imaging Systems (Filenet)
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low

Who owns this system? (Name, agency, contact information)	Angela Sieg FSA, ITSD/ADC/AFAO U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133 816-926-1568 angela.sieg@kcc.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Brian Davies Information Systems Security Program Manager (ISSPM) USDA/FSA 1400 Independence Avenue SW Washington, D.C. 20250 (202) 720-2419 Brian.Davies@wdc.usda.gov
Who completed this document? (Name, agency, contact information)	Charlene Niffen Information System Security Officer USDA/FSA/ISO U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133 816-926-2111 Charlene.Niffen@kcc.usda.gov

Overview

- System Name: Document Imaging Systems (Filenet)
- Agency: FSA

- System Purpose: The Document Imaging System (FileNet) is a Commercial-off-the-Shelf (COTS) client-server application that stores financial information images in the form of PDF and Tiff files. It allows for the input of pertinent Consolidated Financial Management Information Systems (CFMIS) investment documents for storage and retrieval. All data is directly input by the user from electronically stored documents, faxed, and scanned materials. Additionally, FileNet controls the workflows associated with the financial information being imaged. FileNet allows client access from desktop browser to the stored images on a network device managed by the server. Storage of financial records, debts, debtors, and other information to the server uses Netapp Snaplock which is controlled by the server software. The server utilizes a SQL database to manage document indexes and workflow process. The FileNet system resides on the OCIO-CTS network, which is managed by the CTS-CS and CTS SES divisions of CTS.

- General System Description: The Document Imaging System (FileNet) is a Commercial-off-the-Shelf (COTS) client-server application that stores financial information images in the form of PDF and Tiff files. It allows for the input of pertinent Consolidated Financial Management Information Systems (CFMIS) investment documents for storage and retrieval. All data is directly input by the user from electronically stored documents, faxed, and scanned materials. Additionally, FileNet controls the workflows associated with the financial information being imaged. FileNet allows client access from desktop browser to the stored images on a network device managed by the server. Storage of financial records, debts, debtors, and other information to the server uses Netapp Snaplock which is controlled by the server software. The server utilizes a SQL database to manage document indexes and workflow process. The FileNet system resides on the OCIO-CTS network, which is managed by the CTS-CS and CTS SES divisions of CTS.

  KCFRB Imaging (FRB) check images are downloaded and imported in the system. It is used to store and view FRB check images and pertinent information on CCC checks. It is used to pull up images of CCC checks. The KCFRB system is used to research historical archives of treasury checks. No new content is being added to the system. No updating is possible, only retrieval. KCFRB only makes calls to the IBM/FileNet Content Process Engine to retrieve images for display. It has no workflow function.

  Receivable Case Management Application is a FileNet imaging system which allows the input of documents for storage and retrieval. All data is user input from document storage, fax and scanned materials. All data is input by the RMO staff and utilizes IBM/FileNet P8 storage areas. Documents are primarily entered into the system using the Fax capture interface, though adding documents from email and desktop scanners is possible. Fax and email data is entered via DataCap. The workflow of RCMA is dependent on the IBM/FileNet P8 Advanced Case Manager; and accesses the IBM/FileNet P8 Content Process Engine using the IBM Content Navigator web application as part of the process.

Receivable Imaging System is a web based (FSA intranet only) means of accessing specific claims from Receivable Case Management Application. The claims can only be accessed by the claim number. State and county employees utilize this web application based on IBM Content Navigator to search and retrieve imaged documents for producer claims receivables processing. No updating is possible, only retrieval. No fax or print capabilities are available thru this application. RIS only makes calls to the IBM/FileNet Content Process Engine to retrieve images for display. It has no workflow function.

Tobacco, Finance, Internal Revenue Service (IRS) is a subsystem that stores various images. Documents are scanned locally and faxed from county offices. Receivables, Financial & Accounting Info Reporting System (FAIRS) documents are scanned locally and serve as backup information for daily treasury and financing activities. Tobacco documents must be kept held for historic purposes, although the tobacco program is no longer active and no new documents are being imaged. Tobacco, Finance and IRS utilizes the IBM/FileNet Content Process Engine to search and retrieve archive documents using the IBM Content Navigator user interface. IRS additionally uses the IBM P8 Advanced Case Management to manage a business workflow process: 1) Tobacco – This system is no longer active for input and used for storage only of historical documents - This is a read-only application, 2) Finance - The Finance system is used to research historical archives. No new content is being added to the system. No updating is possible, only retrieval. Finance only makes calls to the IBM/FileNet Content Process Engine to retrieve images for display. It has no workflow function. WDC staff can access this application - This is a read-only application and 3) IRS - All data is input by the PMO staff and utilizes all IBM/FileNet P8 storage areas. Documents are primarily entered into the system using the Fax capture interface, though adding documents from email and desktop scanners is possible. This is a read-only application.

- Typical Transaction: N/A
- Information Sharing: N/A
- Module & Component Description: N/A
- Legal Authority to Operate: The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397.

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?

Subsystem	**Name -** Full name, mother's maiden name, maiden	**Date and/or place of birth.**	**Address Information** (street & email address).	**Personal identification number** (social security number, tax identification number, passport number, driver's license number or a unique identification number, etc.)	**Financial data** (Credit card numbers, bank account etc.)	**Health data** (including height, weight, blood pressure, etc.)	**Biometric data** (fingerprints, iris scans, voice signature, facial geometry, DNA, etc.)	**Criminal history**	**Employment history**	**Miscellaneous identification numbers** (agency assigned number, case number, accounts, permits, etc.)	**Photographic image/identifying characteristics.**	**Handwriting or an image of the signature**	**Other -** List	**Misc. or Other Lists**
FRB	X				X							X		
RCMA	X		X	X						X		X	X	Phone #
RIS	X		X	X						X		X	X	Phone #
TFI	X		X	X	X					X		X		Deposit #

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

KCFRB Imaging (FRB) downloads and imports Federal Reserve Bank images into the system.

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

The Document Imaging Systems (FileNet) is a Commercial-off-the-Shelf (COTS) client-server application that stores financial information images in the form of Tiff files. It allows for the input of pertinent Consolidated Financial Management Information Systems (CFMIS) investment documents for storage and retrieval.

1.4 How is the information collected?

All data was directly input by the user from document storage, faxed, and scanned materials.

1.5 How will the information be checked for accuracy?

When data was entered in the applications it was validated for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

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

Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397

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

The privacy risks are moderate. The minimum amount of personally identifiable information is collected to satisfy the purpose of this system. The risks are mitigated using various control mechanisms. See below:

- All users must be uniquely identified and authenticated prior to accessing the application.
- Access to data is restricted.
- IBM Datacap security tables allow role based access to the application.

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.

It allows for the input of pertinent Consolidated Financial Management Information Systems (CFMIS) investment documents for storage and retrieval. All data is directly input by the user from document storage, faxed, and scanned materials. Additionally, FileNet controls the workflows associated with the financial information being imaged.

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

No additional “tools” are used to analyze the data.

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

The system does not use commercial or public data.

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.

Access to the system and data are determined by business need and individual roles. Controls are in place to provide reasonable assurance that data integrity and confidentiality are maintained during processing. Controls in place to ensure the correct handling of information include the following:

- End users are correctly identified and authenticated according USDA and FSA security policies for access managements, authentication and identification controls.
- Audit logging is used to ensure data integrity.
- IBM Datacap security tables allow role based access to the application.

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?

The information is retained indefinitely (permanent records).

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

Yes, in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records.

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

During this period, the stored information may be at risk for viewing by unauthorized parties, data loss or destruction and non-availability. Access to computerized files are protected by access control software, physical access controls and if warranted, password-protected.

SORN USDA/FSA-2 States: Program documents are destroyed within 6 years after end of participation. However, FSA is under a records freeze.

According to Records Management DR3080-001 Disposition of Inactive Records: Records and other documents that are no longer sufficiently active to warrant retention in office space shall be removed as rapidly as possible by: (a) transfer to a Federal Records Center, or (b) transfer to a records retention facility meeting the requirements of 36 CFR Chapter 12, Subchapter B Records Management, Subpart K, 1228.224 through 1228.244, or (c) if authorized, by disposal. (See Appendix B – Records Disposition Procedures.)

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?

N/A

4.2 How is the information transmitted or disclosed?

N/A

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.

N/A

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

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

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

N/A

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

N/A

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

Yes.

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

Yes. FSA Privacy Policy states that "Submitting information is strictly voluntary."

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

Yes, in accordance with FSA Privacy policy and the individual's written consent.

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

The risk is considered moderate. Notification is automatically provided in the system of records notice (Federal Register publication): SORN: USDA/FSA–2 - Farm Records File (Automated) and USDA/FSA-14 - Applicant/Borrower.

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?

As published in SORN USDA/FSA-2 and SORN USDA/FSA-14: "An individual may obtain information about a record in the system which pertains to such individual by submitting a written request to the above listed System Manager. The envelope and letter should be marked ``Privacy Act Request." A request for information should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

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

As published in SORN USDA/FSA-2 and SORN USDA/FSA-14: "Individuals desiring to contest or amend information maintained in the system should direct their request to the above listed System Manager, and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

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

Formal redress is provided via the FSA Privacy Act Operations Handbook.

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

N/A

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

The risk associated with redress is considered low, as the public does not have access to the system or the data. While the public cannot access the system to update or change their personal information, they may update their information using form AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

There is work going on for Customer Self Service which will be public facing. SCIMS is no longer the source of entry since Business Partner was implemented in December 2014.

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?

Access to FSA web applications is gained via an on-line registration process similar to using the FSA-13- A form. For system specific detailed access see SSP.

8.2 Will Department contractors have access to the system?

Department contractors do not have access to the System.

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

Once hired, privacy training and security awareness training is completed prior to gaining access to a workstation. The privacy training addresses user's responsibilities to protect privacy data and how to protect it.

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

Yes, 10/22/2015.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The logging/auditing mechanism is an inherited function. The Application does not generate its own log/audit information. Any logging and auditing of access, transactions or output is left to the OCIO-ITS, and eAuthentication Application.

Other safeguards listed on the PTA:
Encryption, controlled access
authentication process:

Users first logon to the FSA network and are authenticated and authorized with a valid Enterprise Active Directory (EAD) account. Users next access eAuthentication and must have Level 2 authorization status.

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?

The main risk associated with privacy is the exposure to unauthorized access to privacy information. This risk is considered moderate. Mitigating controls are in place to ensure privacy risks are minimal. Mitigated controls are mapped back to SSP in CSAM.

Annual access reviews are done to ensure controls are mitigated.

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?

Major application

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

No.

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, no 3rd party website (hosting) or 3rd party application is being used.

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

Appendix A. Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Document Imaging System (FileNet).

THREATHA MARBRA Digitally signed by THREATHA MARBRA
Date: 2018.04.24 08:49:08 -05'00'

Angela Sieg, Information System Owner Date

AMBER ROSS Digitally signed by AMBER ROSS
Date: 2018.04.24 09:43:29 -05'00'

Amber Ross, Acting Privacy Officer Date

JEFFERY WAGNER Digitally signed by JEFFERY WAGNER
Date: 2018.04.30 08:24:54 -05'00'

Darren Ash, Agency CIO Date