Privacy Impact Assessment

Document Imaging Systems (FileNet)

- **Producer Claims Imaging**
- **Department of Justice Imaging**
- **Automated Clearing House (ACH) Return Imaging**
- **Document Wizard Web Retrieval Imaging**

Revision: Final

Farm Service Agency

ADC/AFAO
6501 Beacon Drive
Kansas City, MO 64133-4676

Date: 09/03/2008

Document Information

Owner Details	
Name	Threatha Worsham, (Acting) Chief AFAO/FMG
Contact Number	816-926-6398
E-mail Address	threatha.worsham@kcc.usda.gov

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
Draft Version 1	06/06/2008	S. Timbrook, EDS R. Grant-Smith, EDS	Original document with revisions.
Final	06/24/2008	Threatha Worsham, (Acting) Chief AFAO/FMG	Reviewed and Signed document
Final V.1	08/19/2008	S. Timbrook, ECS	Changed the description of the DOJ component per D. Cowan.
Final	08/25/2008	R. Grant-Smith, ECS	Marked document as final and forwarded to Karen A. Malkin, Esq., for review and signature.
Final	09/02/2008	S. Timbrook, ECS	Changed Steve Sanders to Sue Bussells within document
Final	09/03/2008	S. Timbrook, ECS	Marked Final and change date to reflect current date 09/03/2008. Changed assessment date to reflect 06-06-08 Sec 2.7, Removed Acting from Dennis Taitano's Title, Corrected Karen Malkin's Title through out the document to reflect "Esq. Chief Privacy Officer and Assistant to the Administrator" , Replaced Karen Malkin, Esq. with Brain Davies ISSPM on signatures page.
	06/30/2009	S. Timbrook, ECS	Changed in block 3.1.6 Customer Protection section to reflect John Underwood, resent for final signature.
	02/24/2009	S. Timbrook, ECS	Section review and changed per request from R. Ciampa. Section 3.1.3 #2, 3.1.5 #2.1, 3.1.6. #3.1

Table of Contents

1 PURPOSE OF DOCUMENT 1

2 APPLICABILITY 2

2.1 Applicability of System 2

2.2 System Overview 2

2.3 System Categorization 3

2.4 Responsible Organization 3

2.5 Information Contacts 3

2.6 Assignment of Security Responsibility 4

2.7 Who Completed this Assessment? 5

3 USDA PRIVACY IMPACT ASSESSMENT 6

3.1 Does the System Contain Information About Individuals in an Identifiable Form? 6
3.1.1 Data Collection 8
3.1.2 Data Use 9
3.1.3 Data Retention 10
3.1.4 Data Sharing 11
3.1.5 Data Access 12
3.1.6 Customer Protection 13
3.1.7 System Of Record 14
3.1.8 Technology 14

4 PRIVACY IMPACT ASSESSMENT AUTHORIZATION MEMORANDUM 18

1 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. Systems include data from applications housed on mainframes, personal computers, and applications developed for the Web and agency databases. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in USDA.

Both the system owners and system developers must work together to complete the PIA. System owners must address what data are used, how the data are used, and who will use the data. System owners also need to address the privacy implications that result from the use of new technologies (e.g., caller identification). The system developers must address whether the implementation of the owner's requirements presents any threats to privacy."

The Privacy Impact Assessment (PIA) document contains information on how the **Document Imaging Systems (FileNet)** affect the privacy of its users and the information stored within. This assessment is in accordance with NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems.*

2 Applicability

2.1 Applicability of System

The information in this document is applicable to the Document Imaging Systems (FileNet).

2.2 System Overview

The Document Imaging Systems (FileNet) consists of nine applications/components of which only two that are ***active*** as of the date of this document. These are as follows:

1. Producer Claims Imaging (PCB) – is a FileNet imaging system allows the input of documents for storage and retrieval. All data is user input from document storage, fax and scanned materials.
2. Department of Justice Imaging (DOJ) - is a FileNet imaging system that allows the tracking of DOJ payments & record payments. This is strictly a workflow component of FileNet application.

The third and fourth component; Automated Clearing House (ACH) Return and Document Wizard Web Retrieval are currently in the ***testing phase*** as of the writing of this document.

3. Automated Clearing House (ACH) Return – is a FileNet imaging system that takes data downloaded from a mainframe feed and converts each ACH Return and Notice of Change into a document. The application groups all items by state and county codes, and faxes the documents to each county. Once information is obtained for each ACH Return, the counties will fax the information back to the imaging system.
4. Document Wizard Web Retrieval – is a web based (FSA intranet only) means of accessing specific claims from Producer Claims Imaging. The claims can only be accessed by the claim number.

Components five through eight are noted for documentation purposes and will be ***reviewed at a later date***.

5. 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. POG uses it to pull up images of CCC checks.
6. FDS Monthly and Accounts Payable – Accounts payable reports are scanned using a single dedicated PC and scanner.
7. Tobacco, Finance, IRS (PPRS, Fairs, Tobacco data is Inactive) – PPRS documents are scanned locally and faxed from county offices. 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.
8. GSM Registration/EOE and Claims Data – Inactive; FSA/WDS are not using this of the time of writing of this document.

The ninth and final is CNC (St. Louis) this component has never been used and will be ***removed*** from the workstations.

2.3 System Categorization

By following the guidance set forth in NIST SP 800-60 and FIPS PUB 199 taking into account the information types and other factors for this system, the Security Categorization for this system has been determined to be **Moderate**. Therefore, Risk Assessments and Security Testing and Evaluation (ST&E) will be performed following the Moderate baseline set forth in NIST SP 800-53 Annex 2.

2.4 Responsible Organization

United States Department of Agriculture (USDA)
Farm Service Agency (FSA)
1400 Independence Avenue SW
Washington, D.C. 20250

This system is maintained by:

Farm Service Agency-Kansas City Complex
Farm Credit Application Office
6501 Beacon Drive
Kansas City, MO 64133

This system's hardware is located at:

Farm Service Agency-Kansas City Complex
Farm Credit Application Office
6501 Beacon Drive
Kansas City, MO 64133

2.5 Information Contacts

Name	Title	Address	Phone Number	E-mail Address
Certifying Officer: Sue Bussells	FSA Chief Information Officer (Acting) Director, Information Technology Services Division (ITSD) (Acting) FSA/DAM/ITSD	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington D.C. 20250	(202)720-5320	sue.bussells@wdc.usda.gov
Business Owner (DAA): Dennis Taitano	Director, FSA Office of Budget and Finance.	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington D.C. 20250	202-720-3674	dennis.taitano@wdc.usda.gov

Name	Title	Address	Phone Number	E-mail Address
Business Program Manager: Monty Tranbarger	Director, Kansas City Financial Office (KCFO)	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-3250	monty.tranbarger@kcc.usda.gov
Program Manager: Threatha Worsham	(Acting) Chief, Administrative and Financial Application Office AFAO/FMG	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-6398	threatha.worsham@kcc.usda.gov
System Managers: Threatha Worsham	Group Chief, Financial Management Group (FMG)	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-6398	threatha.worsham@kcc.usda.gov

2.6 Assignment of Security Responsibility

Name	Title	Address	Phone Number	E-mail Address
Karen Malkin , Esq.	Chief Privacy Act Officer and Assistant to the Administrator USDA/FSA/OA/OBPI/SPS	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-690-2203	karen.malkin@wdc.usda.gov
Thomas B. Hofeller,	Freedom of Information Act (FOIA) Coordinator Associate Administrator for Operations and Management USDA/FSA/OA	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-690-0153	tom.hofeller@wdc.usda.gov
Brian Davies	Information System Security Program Manager (ISSPM) FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-720-2419	brian.davies@wdc.usda.gov
Mindy Gehrt	Disaster Recovery Coordinator Information Security Office (ISO) FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-3522	mindy.gehrt@kcc.usda.gov

Name	Title	Address	Phone Number	E-mail Address
Georgia "Shelly" Nuessle	Certification & Accreditation Coordinator Information Security Office (ISO) USDA - FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-3018	georgia.nuessle@kcc.usda.gov

2.7 Who Completed this Assessment?

June 6, 2008

Debbie Cowan
FileNet Administrator
U.S. Department of Agriculture
Farm Service Agency
6501 Beacon Drive
Kansas City, MO 64133
816-926-7415
debbie.cowan@kcc.usda.gov

3 USDA Privacy Impact Assessment

3.1 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 individuals:	Yes		No
	Citizens	Employees	
Name	☒	☐	☐
Social Security Number	☒	☐	☐
Telephone Number	☒	☐	☐
Email address	☒	☐	☐
Street address	☒	☐	☐
Financial data	☒	☐	☐
Health data	☐	☐	☒
Biometric data	☒	☐	☐
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]	☒	☐	☐
Are social security numbers embedded in any field?	☒	☐	☐
Is any portion of a social security numbers used?	☐	☐	☒
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	☐	☐	☒

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

[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.

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.

3.1.1 Data Collection

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

   There is no actual data being used by the system; only the images of documents relating to debt and ACH/NOC collections are stored and accessible.

2. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

   ☒ Yes
   ☐ No

3. Sources of the data in the system.

   3.1. What data is being collected from the customer?

   No data is being collected by the customer.

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

   The Farm Service Agency (FSA) is providing data for use in the system.

   3.3. What state and local agencies are providing data for use in the system?

   No state or local agencies are providing data for use in the system.

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

   No data is collected from third party sources.

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

   ☐ Yes
   ☒ No. If NO, go to section 3.1.2, question 1.

   4.1. How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?

   N/A

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

   N/A

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

N/A

3.1.2 Data Use

1 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?

There is no data being collected; only the images of documents relating to debt, ACH/NOC collections.

2 Will the data be used for any other purpose?

☐ Yes
☒ No. If NO, go to question 3 (below).

2.1 What are the other purposes?

N/A

3 Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

☒ Yes
☐ No

4 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 5 (below).

4.1 Will the new data be placed in the individual's record (customer or employee)?

☐ Yes
☐ No

4.2 Can the system make determinations about customers or employees that would not be possible without the new data?

☐ Yes
☐ No

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

N/A

5 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?

There is no data being collected; only the images of documents relating to debt, ACH/NOC collections.

6 Will the data be used for any other uses (routine or otherwise)?

☐ Yes
☒ No. If NO, go to question 7 (below).

6.1 What are the other uses?

N/A

7 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 8 (below).

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

N/A

8 Are processes being consolidated?

☐ Yes
☒ No. If NO, go to section 3.1.3, question 1.

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

N/A

3.1.3 Data Retention

1 Is the data periodically purged from the system?

☐ Yes
☒ No. If NO, go to question 2 (below).

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

N/A

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

N/A

1.3 Where are these procedures documented?

N/A

2 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?

Images of documents and only as accurate as the documents being photographed.

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

☒ Yes Images are retained for an indefinite period of time.
☐ No

3.1.4 Data Sharing

1 *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 2 (below)

1.1 How will the data be used by the other agency?

N/A

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

N/A

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

☐ Yes
☒ No. If NO, go to question 3 (below)

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

N/A

3 Is the system operated in more than one site?

☐ Yes
☒ No. If NO, go to section 3.1.5, question 1.

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

N/A

3.1.5 Data Access

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

In conjunction with their assigned job functions, end users, managers, and system administrators will have access to document images in the system.

2 How will user access to the data be determined?

Managers will determine user accessibility to the system.

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

☒ Yes
☐ No

3 How will user access to the data be restricted?

Users will have access based on UserID and password within the FSA network and FileNet system. Password controls apply rules to ensure that they are not compromised easily. Passwords must adhere to certain guidelines such as: minimum character length, special characters must be used, passwords must be changed periodically, and passwords may not be re-used for a period of time.

The users within Document Wizard Web Retrieval (still in testing) will go through eAuth and again with FileNet security controls.

All users must be authenticated in some form in order to access the CFMIS/Debt System Document Imaging (FileNet) for those components residing on the workstations. Users must first log on to their workstation and be authenticated by the FSA network. After authenticated the users may access the component and once again be authenticated within FileNet.

3.1 Are procedures in place to detect or deter browsing or unauthorized user access?

☒ Yes
☐ No

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

☒ Yes
☐ No

3.1.6 Customer Protection

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

The FileNet system manager is initially responsible for protecting the privacy rights of USDA/FSA customers. As access is primarily controlled by the system manager, initial responsibility lies with this officer.

2 How can customers and employees contact the office or person responsible for protecting their privacy rights?

Customers can contact the USDA/FSA Privacy Officer at the following address:

Name	Address	Phone Number	E-mail Address
John W. Underwood FSA Privacy Act Officer / FSA PII Officer	USDA - Farm Service Agency Beacon Facility - Mail Stop 8388 9240 Troost Avenue Kansas City, Missouri 64131-3055	Phone: 816-926-6992 Cell: 816-564-8938 Fax: 816-448-5833	mailto:john.underwood@kcc.usda.gov

3 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, go to question 4 (below).
☐ No

3.1 If NO, please enter the POAM number with the estimated completion date:

N/A

4 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 customer of due process rights (fundamental rules of fairness)?

☐ Yes
☒ No. If NO, go to question 5 (below)

4.1 Explain how this will be mitigated?

N/A

5 How will the system and its use ensure equitable treatment of customers?

The system cannot differentiate between debtors.

6 Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?

☐ Yes
☒ No. If NO, go to section 3.1.7, question 1.

6.1 *Explain*

N/A

3.1.7 System Of Record

1 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 section 3.1.8, question 1.

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

Images can be retrieved via Federal Tax ID.

1.2 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/FSA-13 Claims Data Base

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

NO

3.1.8 Technology

1 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.

1.1 How does the use of this technology affect customer 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

USDA Privacy Impact Assessment for Document Imaging Systems (FileNet)

4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Document Imaging System (FileNet)

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.

Threatha Worsham 8/20/08

Threatha Worsham
FileNet System Manager

Date

Sue Bussells
Agency CIO

Date

Karen Mallin, ESQ
Chief Privacy Officer

Date

Sensitive But Unclassified/Sensitive Security Information

USDA Privacy Impact Assessment for Document Imaging Systems (FileNet)

4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Document Imaging System (FileNet)

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.

Threatha Worsham FileNet System Manager	Date
Sue Bussells Agency CIO (Acting)	9/2/08 Date
Karen A. Malkin, Esq. Chief Privacy Act Officer	Date

4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Document Imaging System (FileNet)

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.

Threatha Worsham FileNet System Manager	Date
Sue Bussells Agency CIO (Acting)	Date
Brian Davies Information System Security Program Manager (ISSPM)	Date