Privacy Impact Assessment (PIA)

Farm Service Agency

Customer Name/Address Systems (CN/AS)

Customer Name/Address (CN/A)

Revised: November 09, 2012

Template Version: FSA-PIA-2011-08-19-A

Document Information

System Owner Contact Information	
Name	Matthew Tellado
Contact Number	(816) 926-6951
E-mail Address	Matthew.Tellado@kcc.usda.gov

Document Revision History		
Date	Author	What was changed?
MM/DD/YYYY	Name & Organization	
11/09/2012	Joe Apple - ESC	New Template and C&A

Table of Contents

Purpose of Document 1

Abstract 1

Overview (System Description) 2

Section 1.0 Characterization of the Information 3

Section 2.0 Uses of the Information 5

Section 3.0 Retention 6

Section 4.0 Internal Sharing and Disclosure 7

Section 5.0 External Sharing and Disclosure 8

Section 6.0 Notice 9

Section 7.0 Access, Redress and Correction 10

Section 8.0 Technical Access and Security 12

Section 9.0 Technology 13

Section 10.0 Third Party Websites/Applications 14

Appendix A. Privacy Impact Assessment Authorization Memorandum 16

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: Customer Name/Address (CN/A)
Brief description of the system and its function: Customer Name/Address (CN/A) maintains the name and address and other information for customers doing business or requesting information located in each County.
Why the PIA is being conducted: To support federal law, regulations and policies.

System Information	
Agency:	Farm Service Agency
System Name (Acronym):	Customer Name/Address (CN/A)
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)	Matthew Tellado ITSD/ADC/PARMO/FRG 6501 Beacon Drive Kansas City MO 64133 (816) 926-6951 Matthew.Tellado@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)	Joe Apple ESC 6500 S MacArthur Blvd Oklahoma City, Ok 73169 405-627-6648 Joe.Apple@esc.gov

Overview

- System Name: Customer Name/Address (CN/A)
- Agency: FSA
- System Purpose: To maintain the name and address and other information for each farm producer and farm owner with a farming interest.
- General System Description: Customer Name/Address (CN/A) maintains the name and address and other information for customers doing business or requesting information located in each County.
- Typical Transaction: Input and maintenance of customer name and address information by FSA staff and the updating of the mainframe data by Service Center Offices (SCO) through the AS400/S/36 by local IBM S/36 emulation software.
- Information Sharing: None.
- Module & Component Description: None.
- Legal Authority to Operate: The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397 and Farm Records–USDA/FSA-2.

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?

Customer: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation. Name & Address (MF) includes Farm Service Agency employees, farm owners, farm operators, and Technical Service Providers. Additionally business customers can be identified by business entity type (i.e. general partnership, Limited Liability Company, corporation, etc.)

Employee: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation.

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

Farm Service Agency (FSA), Natural Resource Conservation Service (NRCS) and Rural Development (RD). Ongoing data is entered by authorized USDA Service Center employees.

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

Data is collected and used to perform administrative and programmatic business by the USDA.

1.4 How is the information collected?

Data is collected from customers and employees and entered into the system by FSA and county office employees.

1.5 How will the information be checked for accuracy?

All data collected from customers, employees and USDA sources are required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

The Customer Information is validated by the Application business rules at the time the information is entered into the application. It is also reviewed by the Producer for accuracy.

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

As published in SORN USDA/FSA-2: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, year of records in question, and any other pertinent information to help identify the file.

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.

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.

CN/A data is used to maintain name and address and other information to support administrative and programmatic business by the USDA.

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

The system does not analyze stored data. The system's primary function is to store and maintain customers and employee data.

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.

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.

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?

Information is not purged from the system. Information is kept indefinitely.

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

The retention period has been approved by the Records Manager and the National Archives and Records Administration (NARA).

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

The retention period is based on a combination business need (i.e., how long do we need this information for our business process) and long term usefulness. When records have reached their retention period, they are immediately retired or destroyed in accordance with the USDA Record Retention policies and procedures.

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.

FSA2 SORN 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.

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, customers consent to the purpose and use of their data at the time they provide the information for entry into the system.

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): USDA/FSA-2 – Farm Records File (Automated).

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: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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: Contesting record procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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 nor the data in the system. While the public cannot access the system to update or change their personal information, they may update their information using from AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

In FY 2014, FSA plans to implement a public facing SCIMS complimentary system which will allow the public to register, complete a profile and update their profile. This complimentary system will then synchronize the data with SCIMS. During synchronization, any profile data to include, name, address, telephone number, and email address updated by the public will be updated in SCIMS within 24 hours.

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 must be requested through FSA-13A security forms with justification and approval. Security Identification and Authentication is performed by the OS/400 and SSP operating systems and the mainframe ACF2. In addition, on the S36 application, users are restricted to the data on the local AS/400 (service center).
On the mainframe further authorization must be enabled to access the DB2 database objects.

8.2 Will Department contractors have access to the system?

Department contractors do not have access to CN/A.

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

Upon hire, privacy training is completed prior to gaining access to a workstation. In addition, annual security awareness and privacy refresher training is required to be completed. (Reference IRM 438). This type of access is also documented in the requirements document.

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

Yes, 08/31/2010.

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

Standard Security Training and Awareness Program.

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. Quarterly 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?
Minor 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 Customer Name/Address (CN/A).

jennifer.thomas.1
@usda.gov
Digitally signed by
jennifer.thomas.1@usda.gov
DN: cn=jennifer.thomas.1@usda.gov
Date: 2013.06.03 09:44:01 -05'00'

Information System Owner (Acting) Date

John W. Underwood
Digitally signed by
john.underwood@usda.gov
DN: cn=john.underwood@usda.gov
Date: 2013.06.17 15:24:40 -05'00'

John Underwood, Privacy Officer Date

for

JUN 19 2013

Jim Gwinn, Agency CIO Date

Privacy Impact Assessment (PIA)

Farm Service Agency

Customer Name/Address Systems (CN/AS)

Other Name/Address (O/NA)

Revised: November 09, 2012

Template Version: FSA-PIA-2011-08-19-A

Document Information

System Owner Contact Information	
Name	Matthew Tellado
Contact Number	(816) 926-6951
E-mail Address	Matthew.Tellado@kcc.usda.gov

Document Revision History		
Date MM/DD/YYYY	Author Name & Organization	What was changed?
11/09/2012	Joe Apple - ESC	New Template and C&A

Table of Contents

Purpose of Document 1

Abstract 1

Overview (System Description) 2

Section 1.0 Characterization of the Information 3

Section 2.0 Uses of the Information 5

Section 3.0 Retention 6

Section 4.0 Internal Sharing and Disclosure 7

Section 5.0 External Sharing and Disclosure 8

Section 6.0 Notice 9

Section 7.0 Access, Redress and Correction 10

Section 8.0 Technical Access and Security 12

Section 9.0 Technology 13

Section 10.0 Third Party Websites/Applications 14

Appendix A. Privacy Impact Assessment Authorization Memorandum 16

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: Other Name/Address (O/NA)
Brief description of the system and its function: The Other Name and Address (O/NA) system is used to enter and maintain the name and address and other information for each farm producer and farm owner with a farming interest.
Why the PIA is being conducted: To support federal law, regulations and policies.

System Information	
Agency:	Farm Service Agency
System Name (Acronym):	Other Name/Address (O/NA)
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)	Matthew Tellado ITSD/ADC/PARMO/FRG 6501 Beacon Drive Kansas City MO 64133 (816) 926-6951 Matthew.Tellado@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)	Joe Apple ESC 6500 S MacArthur Blvd Oklahoma City, Ok 73169 405-627-6648 Joe.Apple@esc.gov

Overview

- System Name: Other Name/Address (O/NA)
- Agency: FSA
- System Purpose: To maintain the facility Name and address and other information for each farm producer and farm owner with a farming interest.
- General System Description: The Other Name and Address (O/NA) system is used to enter and maintain the name and address and other information for each farm producer and farm owner with a farming interest.
- Typical Transaction: Input and maintenance of facility name and address information by FSA staff and the updating of the mainframe data by Service Center Offices (SCO) through the AS400/S/36 by local IBM S/36 emulation software.
- Information Sharing: None.
- Module & Component Description: None.
- Legal Authority to Operate: The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397 and Farm Records–USDA/FSA-2.

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?

Customer: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation. Name & Address (MF) includes Farm Service Agency employees, farm owners, farm operators, and Technical Service Providers. Additionally business customers can be identified by business entity type (i.e. general partnership, Limited Liability Company, corporation, etc.)

Employee: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation.

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

Farm Service Agency (FSA), Natural Resource Conservation Service (NRCS) and Rural Development (RD). Ongoing data is entered by authorized USDA Service Center employees.

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

Data is collected and used to perform administrative and programmatic business by the USDA.

1.4 How is the information collected?

Data is collected from customers and employees and entered into the system by FSA and county office employees.

1.5 How will the information be checked for accuracy?

All data collected from customers, employees and USDA sources are required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

The Customer Information is validated by the Application business rules at the time the information is entered into the application. It is also reviewed by the Producer for accuracy.

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

As published in SORN USDA/FSA-2: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, year of records in question, and any other pertinent information to help identify the file.

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.

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.

O/NA data is used to maintain name and address and other information to support administrative and programmatic business by the USDA.

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

The system does not analyze stored data. The system's primary function is to store and maintain customers and employee data.

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.

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.

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?

Information is not purged from the system. Information is kept indefinitely.

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

The retention period has been approved by the Records Manager and the National Archives and Records Administration (NARA).

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

The retention period is based on a combination business need (i.e., how long do we need this information for our business process) and long term usefulness. When records have reached their retention period, they are immediately retired or destroyed in accordance with the USDA Record Retention policies and procedures.

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.

FSA2 SORN 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.

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, customers consent to the purpose and use of their data at the time they provide the information for entry into the system.

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): USDA/FSA-2 – Farm Records File (Automated).

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: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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: Contesting record procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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 nor the data in the system. While the public cannot access the system to update or change their personal information, they may update their information using from AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

In FY 2014, FSA plans to implement a public facing SCIMS complimentary system which will allow the public to register, complete a profile and update their profile. This complimentary system will then synchronize the data with SCIMS. During synchronization, any profile data to include, name, address, telephone number, and email address updated by the public will be updated in SCIMS within 24 hours.

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 must be requested through FSA-13A security forms with justification and approval. Security Identification and Authentication is performed by the OS/400 and SSP operating systems and the mainframe ACF2. In addition, on the S36 application, users are restricted to the data on the local AS/400 (service center).
On the mainframe further authorization must be enabled to access the DB2 database objects.

8.2 Will Department contractors have access to the system?

Department contractors do not have access to ON/A.

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

Upon hire, privacy training is completed prior to gaining access to a workstation. In addition, annual security awareness and privacy refresher training is required to be completed. (Reference IRM 438). This type of access is also documented in the requirements document.

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

Yes, 08/31/2010.

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

Standard Security Training and Awareness Program

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. Quarterly 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?
Minor 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 Other Name/Address (O/NA).

jennifer.thomas.1@
usda.gov

Digitally signed by jennifer.thomas.1@usda.gov
DN: cn=jennifer.thomas.1@usda.gov
Date: 2013.06.03 09:46:25 -05'00'

Information System Owner (Acting) Date

John W. Underwood

Digitally signed by john.underwood@usda.gov
DN: cn=john.underwood@usda.gov
Date: 2013.06.17 15:21:30 -05'00'

John Underwood, Privacy Officer Date

for

JUN 19 2013

Jim Gwinn, Agency CIO Date

Privacy Impact Assessment (PIA)

Farm Service Agency

Customer Name/Address Systems (CN/AS)

Service Center Information Management System (SCIMS)

Revised: November 09, 2012

Template Version: FSA-PIA-2011-08-19-A

Document Information

System Owner Contact Information	
Name	Matthew Tellado
Contact Number	(816) 926-6951
E-mail Address	Matthew.Tellado@kcc.usda.gov

Document Revision History		
Date MM/DD/YYYY	Author Name & Organization	What was changed?
11/09/2012	Joe Apple - ESC	New Template and C&A

Table of Contents

Purpose of Document 1

Abstract 1

Overview (System Description) 2

Section 1.0 Characterization of the Information 3

Section 2.0 Uses of the Information 5

Section 3.0 Retention 6

Section 4.0 Internal Sharing and Disclosure 7

Section 5.0 External Sharing and Disclosure 8

Section 6.0 Notice 9

Section 7.0 Access, Redress and Correction 10

Section 8.0 Technical Access and Security 12

Section 9.0 Technology 13

Section 10.0 Third Party Websites/Applications 14

Appendix A. Privacy Impact Assessment Authorization Memorandum 16

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: Service Center Information Management System (SCIMS)

Brief description of the system and its function: SCIMS provides for the collection and maintenance of customer data for the Farm Service Agency (FSA), the lead agency for SCIMS.

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

System Information	
Agency:	Farm Service Agency
System Name (Acronym):	Service Center Information Management System (SCIMS)
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)	Matthew Tellado ITSD/ADC/PARMO/FRG 6501 Beacon Drive Kansas City MO 64133 (816) 926-6951 Matthew.Tellado@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)	Joe Apple ESC 6500 S MacArthur Blvd Oklahoma City, Ok 73169 405-627-6648 Joe.Apple@esc.gov

Overview

- System Name: Service Center Information Management System (SCIMS)
- Agency: FSA
- System Purpose: Users and applications may query customer data using the Web application or an XML Web Service.
- General System Description: SCIMS provides for the collection and maintenance of customer data for the Farm Service Agency (FSA), the lead agency for SCIMS.
- Typical Transaction: Collection and maintenance of customer data and data queries.
- Information Sharing: Natural Resources Conservation Service (NRCS), Rural Development (RD), Risk Management Agency (RMA) and Master Reference Tables (MRT).
- Module & Component Description: None.
- Legal Authority to Operate: The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397 and Farm Records–USDA/FSA-2.

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?

Customer: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation. Name & Address (MF) includes Farm Service Agency employees, farm owners, farm operators, and Technical Service Providers. Additionally business customers can be identified by business entity type (i.e. general partnership, Limited Liability Company, corporation, etc.)

Employee: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation.

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

Farm Service Agency (FSA), Natural Resource Conservation Service (NRCS), Rural Development (RD) and Master Reference Tables (MRT). Ongoing data is entered by authorized USDA Service Center employees.

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

Data is collected and used to perform administrative and programmatic business by the USDA.

1.4 How is the information collected?

Data is collected from customers and employees and entered into the system by FSA and county office employees. County and state office information is pulled weekly from Master Reference Tables (MRT).

1.5 How will the information be checked for accuracy?

All data collected from customers, employees and USDA sources are required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

The Customer Information is validated by the Application business rules at the time the information is entered into the application. It is also reviewed by the Producer for accuracy.

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

As published in SORN USDA/FSA-2: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, year of records in question, and any other pertinent information to help identify the file.

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.

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.

SCIMS data is used to perform administrative and programmatic business in USDA Service Centers. SCIMS provides a centralized and standardized data store used by FSA systems to query customer and employee information.

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

The system does not analyze stored data. SCIMS data may be queried through other CN/AS systems using Web applications or XML Web services.

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.

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.

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?

Information is not purged from the system. Information is kept indefinitely.

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

The retention period has been approved by the Records Manager and the National Archives and Records Administration (NARA).

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

The retention period is based on a combination business need (i.e., how long do we need this information for our business process) and long term usefulness. When records have reached their retention period, they are immediately retired or destroyed in accordance with the USDA Record Retention policies and procedures.

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.

FSA2 SORN 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?

SCIMS data is shared with the Natural Resources Conservation Service (NRCS), Rural Development (RD) and the Risk Management Agency (RMA). All SCIMS data used by the NRCS, RD and RMA is used in support of administrative and programmatic business needs.

4.2 How is the information transmitted or disclosed?

Access to the data is through established security rules via eAuthentication, EAS, and Database Security. The NRCS has access to a copy of the SCIMS2 database via replication. The Risk Management Agency (RMA) receives a copy of the SCIMS database weekly via FTP. County and state office information is pulled weekly from Master Reference Tables (MRT) using SSIS.

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.

Acceptable use requirements and further disclosure restrictions are identified in the applicable Memorandum of Understandings (MOUs) and Interconnection Security Agreements (ISAs).

Farm Service Agency (FSA) performs a Privacy Impact Assessment (PIA) in accordance with OMB Memorandum 03-22 (http://www.whitehouse.gov/omb/memoranda_m03-22). The PIA is performed and updated as necessary:

- When a significant change creates new or different privacy risks.
- And every three years as part of the information system Certification and Accreditation (C&A) process.

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.

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, customers consent to the purpose and use of their data at the time they provide the information for entry into the system.

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): USDA/FSA-2 – Farm Records File (Automated).

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: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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: Contesting record procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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 nor the data in the system. While the public cannot access the system to update or change their personal information, they may update their information using from AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

In FY 2014, FSA plans to implement a public facing SCIMS complimentary system which will allow the public to register, complete a profile and update their profile. This complimentary system will then synchronize the data with SCIMS. During synchronization, any profile data to include, name, address, telephone number, and email address updated by the public will be updated in SCIMS within 24 hours.

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 must be requested through FSA-13A security forms with justification and approval. Only authorized users who have been certified by their respective agency's SCIMS Security Officer may access the system.

8.2 Will Department contractors have access to the system?

Yes, department contractors 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?

Upon hire, privacy training is completed prior to gaining access to a workstation. In addition, annual security awareness and privacy refresher training is required to be completed. (Reference IRM 438). This type of access is also documented in the requirements document.

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

Yes, 08/31/2010.

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

Standard Security Training and Awareness Program.

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.

Quarterly 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?
Minor 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 Service Center Information Management System (SCIMS).

jennifer.thomas.1@usda.gov
Digitally signed by jennifer.thomas.1@usda.gov
DN: cn=jennifer.thomas.1@usda.gov
Date: 2013.06.03 09:48:37 -05'00'

Information System Owner (Acting) Date

John W. Underwood
Digitally signed by john.underwood@usda.gov
DN: cn=john.underwood@usda.gov
Date: 2013.06.17 15:22:45 -05'00'

John Underwood, Privacy Officer Date

for JUN 19 2013

Jim Gwinn, Agency CIO Date

Privacy Impact Assessment (PIA)

Farm Service Agency

Customer Name/Address Systems (CN/AS)

SCOAP Mailings (SCOAP Mailings)

Revised: November 09, 2012

Template Version: FSA-PIA-2011-08-19-A

Document Information

System Owner Contact Information	
Name	Matthew Tellado
Contact Number	(816) 926-6951
E-mail Address	Matthew.Tellado@kcc.usda.gov

Document Revision History		
Date MM/DD/YYYY	Author Name & Organization	What was changed?
11/09/2012	Joe Apple - ESC	New Template and C&A

Table of Contents

Purpose of Document 1

Abstract 1

Overview (System Description) 2

Section 1.0 Characterization of the Information 3

Section 2.0 Uses of the Information 5

Section 3.0 Retention 6

Section 4.0 Internal Sharing and Disclosure 7

Section 5.0 External Sharing and Disclosure 8

Section 6.0 Notice 9

Section 7.0 Access, Redress and Correction 10

Section 8.0 Technical Access and Security 12

Section 9.0 Technology 13

Section 10.0 Third Party Websites/Applications 14

Appendix A. Privacy Impact Assessment Authorization Memorandum 16

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: SCOAP Mailings (SCOAP Mailings)
Brief description of the system and its function: The SCOAP Mailings system performs the business functions of mailings for application needs requiring the sending of addressed messages to some FSA constituency.
Why the PIA is being conducted: To support federal law, regulations and policies.

System Information	
Agency:	Farm Service Agency
System Name (Acronym):	SCOAP Mailings (SCOAP Mailings)
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)	Matthew Tellado ITSD/ADC/PARMO/FRG 6501 Beacon Drive Kansas City MO 64133 (816) 926-6951 Matthew.Tellado@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)	Joe Apple ESC 6500 S MacArthur Blvd Oklahoma City, Ok 73169 405-627-6648 Joe.Apple@esc.gov

Overview

- System Name: SCOAP Mailings (SCOAP Mailings)
- Agency: FSA
- System Purpose: Through the SCOAP Mailings interface a county officer has access to mailing lists based on other farm programs, producer types, crop types, etc. Processing provides for address retrieval, sorting, printing, preparation of bulk mailing reports, and recording of management information.
- General System Description: The SCOAP Mailings system performs the business functions of mailings for application needs requiring the sending of addressed messages to some FSA constituency.
- Typical Transaction: SCOAP Mailings allow for address retrieval, sorting, printing, preparation of bulk mailing reports and the recording of management information.
- Information Sharing: None.
- Module & Component Description: None.
- Legal Authority to Operate: The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397 and Farm Records–USDA/FSA-2.

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?

Customer (Producer): Name, Address, Mailing Preferences, Producer ID/Tax ID, Producer Type, Crop Types, Dates of previous mailings and how many pieces of mail previously sent.

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

Legacy S/36 Name and Address file maintained by SCIMS for the applicable Service Center Offices (SCO's).

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

Data is collected and used to perform the administrative and programmatic business function of mailing (e.g., address retrieval, sorting, printing, preparation of bulk mailing reports, and recording of management information) in USDA Service Center Offices (SCO).

1.4 How is the information collected?

Data is collected from customers and entered into the system by FSA and county office employees.

1.5 How will the information be checked for accuracy?

All data collected from customers, employees and USDA sources are required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

The Customer Information is validated by the Application business rules at the time the information is entered into the application. It is also reviewed by the Producer for accuracy.

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

As published in SORN USDA/FSA-2: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, year of records in question, and any other pertinent information to help identify the file.

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.

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.

Data is collected and used to perform the administrative and programmatic business function of mailing (e.g., address retrieval, sorting, printing, preparation of bulk mailing reports, and recording of management information) in USDA Service Center Offices (SCO).

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

Through the SCOAP Mailings interface a county officer has access to mailing lists based on other farm programs, producer types, crop types, etc. Processing provides for address retrieval, sorting, printing, preparation of bulk mailing reports, and recording of management information.

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.

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.

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?

Information is not purged from the system. Information is kept indefinitely.

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

The retention period has been approved by the Records Manager and the National Archives and Records Administration (NARA).

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

The retention period is based on a combination business need (i.e., how long do we need this information for our business process) and long term usefulness. When records have reached their retention period, they are immediately retired or destroyed in accordance with the USDA Record Retention policies and procedures.

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.

FSA2 SORN 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.

Acceptable use requirements and further disclosure restrictions are identified in the applicable Memorandum of Understandings (MOUs) and Interconnection Security Agreements (ISAs).

Farm Service Agency (FSA) performs a Privacy Impact Assessment (PIA) in accordance with OMB Memorandum 03-22 (http://www.whitehouse.gov/omb/memoranda_m03-22). The PIA is performed and updated as necessary:

- When a significant change creates new or different privacy risks.
- And every three years as part of the information system Certification and Accreditation (C&A) process.

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.

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, customers consent to the purpose and use of their data at the time they provide the information for entry into the system.

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): USDA/FSA-2 – Farm Records File (Automated).

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: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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: Contesting record procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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 nor the data in the system. While the public cannot access the system to update or change their personal information, they may update their information using from AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

In FY 2014, FSA plans to implement a public facing SCIMS complimentary system which will allow the public to register, complete a profile and update their profile. This complimentary system will then synchronize the data with SCIMS. During synchronization, any profile data to include, name, address, telephone number, and email address updated by the public will be updated in SCIMS within 24 hours.

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 must be requested through FSA-13A security forms with justification and approval.

8.2 Will Department contractors have access to the system?

Yes, department contractors 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?

Upon hire, privacy training is completed prior to gaining access to a workstation. In addition, annual security awareness and privacy refresher training is required to be completed. (Reference IRM 438). This type of access is also documented in the requirements document.

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

Yes, 08/31/2010.

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

Standard Security Training and Awareness Program.

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.

Quarterly 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?
Minor 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 SCOAP Mailings (SCOAP Mailings).

jennifer.thomas.1@usda.gov Digitally signed by jennifer.thomas.1@usda.gov DN: cn=jennifer.thomas.1@usda.gov Date: 2013.06.03 09:46:48 -05'00'

Information System Owner (Acting) Date

John W. Underwood Digitally signed by john.underwood@usda.gov DN: cn=john.underwood@usda.gov Date: 2013.06.17 15:23:51 -05'00'

John Underwood, Privacy Officer Date

JUN 19 2013

Jim Gwinn, Agency CIO Date

Privacy Impact Assessment (PIA)

Farm Service Agency

Customer Name/Address Systems (CN/AS)

SCIMS XML Search Page (SXML)

Revised: November 09, 2012

Template Version: FSA-PIA-2011-08-19-A

Document Information

System Owner Contact Information	
Name	Matthew Tellado
Contact Number	(816) 926-6951
E-mail Address	Matthew.Tellado@kcc.usda.gov

Document Revision History

Date MM/DD/YYYY	Author Name & Organization	What was changed?
11/09/2012	Joe Apple - ESC	New Template and C&A

Table of Contents

Purpose of Document 1

Abstract 1

Overview (System Description) 2

Section 1.0 Characterization of the Information 3

Section 2.0 Uses of the Information 5

Section 3.0 Retention 6

Section 4.0 Internal Sharing and Disclosure 7

Section 5.0 External Sharing and Disclosure 8

Section 6.0 Notice 9

Section 7.0 Access, Redress and Correction 10

Section 8.0 Technical Access and Security 12

Section 9.0 Technology 13

Section 10.0 Third Party Websites/Applications 14

Appendix A. Privacy Impact Assessment Authorization Memorandum 16

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: SCIMS XML Search Page (SXML) and SCIMS Web Service (component of SXML)
Brief description of the system and its function: The SCIMS XML Search page is used by many FSA applications to allow a user to search for a specific customer in SCIMS via a web based interface. SCIMS Web Service (component of SXML) is used by many applications in FSA to retrieve specific information about FSA customers.
Why the PIA is being conducted: To support federal law, regulations and policies.

System Information	
Agency:	Farm Service Agency
System Name (Acronym):	SCIMS XML Search Page (SXML)
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)	Matthew Tellado ITSD/ADC/PARMO/FRG 6501 Beacon Drive Kansas City MO 64133 (816) 926-6951 Matthew.Tellado@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)	Joe Apple ESC 6500 S MacArthur Blvd Oklahoma City, Ok 73169 405-627-6648 Joe.Apple@esc.gov

Overview

- System Name: SCIMS XML Search Page (SXML)
- Agency: FSA
- System Purpose: The applications can set what information they require about the customer during the call to the Search Page. When the user clicks on a specific customer, the information for this customer is returned to the calling application utilizing the SCIMS Web Service.
- General System Description: The SCIMS XML Search page is used by many FSA applications to allow a user to search for a specific customer in SCIMS via a web based interface. SCIMS Web Service (component of SXML) is used by many applications in FSA to retrieve specific information about FSA customers.
- Typical Transaction: User and Application searches for relevant customer data.
- Information Sharing:
  - FSA.
  - NRCS.
  - RD.
  - RMA.
- Module & Component Description:
  - SCIMS Web Service.
- Legal Authority to Operate: The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397 and Farm Records–USDA/FSA-2.

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?

Customer: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation. Name & Address (MF) includes Farm Service Agency employees, farm owners, farm operators, and Technical Service Providers. Additionally business customers can be identified by business entity type (i.e. general partnership, Limited Liability Company, corporation, etc.)

Employee: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation.

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

Farm Service Agency (FSA), Natural Resource Conservation Service (NRCS), Rural Development (RD) and Master Reference Tables (MRT). Ongoing data is entered by authorized USDA Service Center employees.

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

Data is collected and used to perform administrative and programmatic business by the USDA providing a centralized and standardized method of developing program decisions.

1.4 How is the information collected?

Data is collected from customers and employees and entered into the system by FSA and county office employees. County and state office information is pulled weekly from Master Reference Tables (MRT).

1.5 How will the information be checked for accuracy?

All data collected from customers, employees and USDA sources are required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

The Customer Information is validated by the Application business rules at the time the information is entered into the application. It is also reviewed by the Producer for accuracy.

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

As published in SORN USDA/FSA-2: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, year of records in question, and any other pertinent information to help identify the file.

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.

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.

SCIMS data retrieved by SXML is used to perform administrative and programmatic business in USDA Service Centers. SCIMS provides a centralized and standardized data store used by FSA systems to query customer and employee information.

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

The system does not analyze stored data. SCIMS data may be queried but no analysis of the data is performed.

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.

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.

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?

Information is not purged from the system. Information is kept indefinitely.

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

The retention period has been approved by the Records Manager and the National Archives and Records Administration (NARA).

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

The retention period is based on a combination business need (i.e., how long do we need this information for our business process) and long term usefulness. When records have reached their retention period, they are immediately retired or destroyed in accordance with the USDA Record Retention policies and procedures.

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.

FSA2 SORN 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?

SCIMS data is shared with the Natural Resources Conservation Service (NRCS), Rural Development (RD) and the Risk Management Agency (RMA). All SCIMS data used by the NRCS, RD and RMA is used in support of administrative and programmatic business needs.

4.2 How is the information transmitted or disclosed?

Access to the data is through established security rules via eAuthentication, EAS, and Database Security. The NRCS has access to a copy of the SCIMS2 database via replication. The Risk Management Agency (RMA) receives a copy of the SCIMS database weekly via FTP. County and state office information is pulled weekly from Master Reference Tables (MRT) using SSIS.

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.

Acceptable use requirements and further disclosure restrictions are identified in the applicable Memorandum of Understandings (MOUs) and Interconnection Security Agreements (ISAs).

Farm Service Agency (FSA) performs a Privacy Impact Assessment (PIA) in accordance with OMB Memorandum 03-22 (http://www.whitehouse.gov/omb/memoranda_m03-22). The PIA is performed and updated as necessary:

- When a significant change creates new or different privacy risks.
- And every three years as part of the information system Certification and Accreditation (C&A) process.

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.

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, customers consent to the purpose and use of their data at the time they provide the information for entry into the system.

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): USDA/FSA-2 – Farm Records File (Automated).

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: Record access procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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: Contesting record procedures: 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 pertaining to an individual should contain: name, address, ZIP code, name of system of record, 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 nor the data in the system. While the public cannot access the system to update or change their personal information, they may update their information using from AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

In FY 2014, FSA plans to implement a public facing SCIMS complimentary system which will allow the public to register, complete a profile and update their profile. This complimentary system will then synchronize the data with SCIMS. During synchronization, any profile data to include, name, address, telephone number, and email address updated by the public will be updated in SCIMS within 24 hours.

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 must be requested through FSA-13A security forms with justification and approval. Only authorized users who have been certified by their respective agency's SCIMS Security Officer may access the system.

8.2 Will Department contractors have access to the system?

Yes, department contractors 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?

Upon hire, privacy training is completed prior to gaining access to a workstation. In addition, annual security awareness and privacy refresher training is required to be completed. (Reference IRM 438). This type of access is also documented in the requirements document.

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

Yes, 08/31/2010.

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

Standard Security Training and Awareness Program.

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.

Quarterly 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?
Minor 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 SCIMS XML Search Page (SXML).

jennifer.thomas.1@
usda.gov

Digitally signed by
jennifer.thomas.1@usda.gov
DN: cn=jennifer.thomas.1@usda.gov
Date: 2013.06.03 09:45:00 -05'00'

Information System Owner (Acting) Date

John W. Underwood

Digitally signed by john.underwood@usda.gov
DN: cn=john.underwood@usda.gov
Date: 2013.06.17 15:25:57 -05'00'

John Underwood, Privacy Officer Date

for

JUN 19 2013

Jim Gwinn, Agency CIO Date