Privacy Impact Assessment (PIA)

Farm Service Agency

Farm Service Security Services System (FSSSS)

Revised: August 2019

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

Document Information

System Owner Contact Information	
Name	Kurt Benedict
Contact Number	816-823-4212
E-mail Address	Kurt.Benedict@usda.gov

Document Revision History		
Date MM/DD/YYYY	**Author Name & Organization**	**What was changed?**
08/15/2019	Darren Smith – FPAC-BC A&A	FY19 Update

Document Review				
Reviewer	Title	Date	Update: Y/N	If systemic, please provide comments

Table of Contents

Purpose of Document

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

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

Abstract

Name of the component and system: Farm Service Security Services System (FSSSS)

Brief description of the system and its function: The Farm Service Security Services System (FSSSS) is an online security request application and approval system that allows users to submit security requests on line and track the status.

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

System Information

System Information	
Agency:	Farm Service Agency
System Name (Acronym):	Farm Service Security Services System (FSSSS)
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)	Kurt Benedict U.S. Department of Agriculture Farm Service Agency 6501 Beacon Kansas City, MO 64133 816-823-5661 Kurt.Benedict@usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Brian Davies Information Systems Security Program Manager (ISSPM) USDA/ FPAC-ISD-IAB-CS 1400 Independence Avenue SW Washington, D.C. 20250 (202) 720-2419 Brian.Davies@usda.gov
Who completed this document? (Name, agency, contact information)	Julian Green IT Specialist – FPAC-BC U.S. Department of Agriculture 1400 Independence Avenue SW Washington, DC 20250 202-260-9193 Julian.Green@usda.gov

Overview

- **System Name:** Farm Service Security Services System (FSSSS)
- **System Description:** The Farm Service Security Services System (FSSSS) is an online security request application and approval system that allows users to submit security requests on line and track the status.

Applications	Overview
Extensible Authorization System (EAS)	The Extensible Authorization System (EAS) was created to augment the eAuthentication system by providing a fine-grained Role-Based Access Control system. EAS allows administrators to use a web browser to manage security access rights, assigning and removing roles/groups/attributes to users on-line in real time. EAS Web Service is a major web service, which was initiated as a result to support the FFAS mission. The purpose of this system is providing storage and retrieval of authorization data pertaining to users' roles, groups, offices, and any specially defined attributes to business applications which apply logical access controls to the users according to business rules enacted by the application.

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?

Applications	Information is collected, used, disseminated or maintained in the system.
EAS	Name & mailing address

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

Applications	Sources of information in the system.
EAS	Employees

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

Applications	Why information being collected, used, disseminated or maintained.
EAS	Facilitate Role-Based Access Control system.

1.4 How is the information collected?

Applications	How information collected.
EAS	Provides a fine-grained Role-Based Access Control system.

1.5 How will the information be checked for accuracy?

Applications	How information is checked for accuracy.
EAS	Data collected from the customer is 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.

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

Applications	Legal authority to collect information.
EAS	Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397.

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

Applications	Privacy risks and how mitigated.
EAS	The controls that have been implemented, inherited, compensated, tested, satisfied and continuously monitored.

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.

Applications	Uses of information.
EAS	Facilitates providing role-based access to applications.

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

Applications	Tools used to analyze data and what type of data produced.
EAS	No additional “tools” (other than the application and database itself) are used to analyze the data.

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

Applications	Why and how commercial or publicly available data is used.
EAS	The system does not use commercial or public data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Applications	Controls in place to ensure information is handled in accordance with the above described uses.
EAS	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 1) security policies for access managements, authentication and identification controls, 2) 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?

Applications	Time information is retained?
EAS	The information is retained indefinitely (permanent records).

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

Applications	Retention period approved by component records officer and National Archives and Records Administration (NARA)?
EAS	Yes, in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records.

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

Applications	Risks associated with the length of time data is retained and how those risks are mitigated.
EAS	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. SORN USDA/FSA-2 States: Program documents are destroyed within 6 years after end of participation. However, FSA is under a records freeze. According to Records Management DR3080-001 Disposition of Inactive Records: Records and other documents that are no longer sufficiently active to warrant retention in office space shall be removed as rapidly as possible by: (a) transfer to a Federal Records Center, or (b) transfer to a records retention facility meeting the requirements of 36 CFR Chapter 12, Subchapter B Records Management, Subpart K, 1228.224 through 1228.244, or (c) if authorized, by disposal. (See Appendix B – Records Disposition Procedures.)

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Applications	Internal organization(s) in which information is shared, what information is shared and for what purpose?
EAS	N/A

4.2 How is the information transmitted or disclosed?

Applications	Information transmittal / disclosure.
EAS	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.

Applications	Privacy risks associated with the sharing and how they were mitigated.
EAS	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?

Applications	External organization(s) is the information shared, what information is shared, and for what purpose?
EAS	No application information is being shared outside of the USDA environment.

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.

Applications	External PII sharing compatibility and SORN coverage, or legal mechanisms by which system is allowed to share PII.
EAS	N/A

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

Applications	Externally shared information and security measures.
EAS	N/A

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

Applications	External sharing privacy risks and mitigation.
EAS	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?

Applications	Individual notice prior to collection of PII information.
EAS	Yes

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

Applications	Individual's right to decline to provide PII information?
EAS	Yes. FSA Privacy Policy states that "Submitting information is strictly voluntary."

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

Applications	Individual's right to consent to uses of PII and how exercised.
EAS	Yes, in accordance with FSA Privacy policy and the individual's written consent.

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

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

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

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

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

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

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

Applications	How individuals notified of correction procedures.
EAS	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?

Applications	Alternatives available to individual if no redress.
EAS	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.

Applications	Privacy risks associated with redress and risk mitigation.
EAS	The risk associated with redress is considered low, as the public does not have access to the system or the data. While the public cannot access the system to update or change their personal information, they may update their information using from AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided. There is work going on for Customer Self Service which will be public facing. SCIMS is no longer the source of entry since Business Partner was implemented in December 2014.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Applications	Access procedures and documentation.
EAS	FSA-13-A is used to request user access to USDA and FSA information technology systems including specifying authorization for accessing the system. (Refer to Notice IRM-440) In addition, access to FSA web applications is gained via an on-line registration process similar to using the FSA-13- A form. For system specific detailed access see SSP.

8.2 Will Department contractors have access to the system?

Applications	Contractor access.
EAS	Department contractors do not have access to the System.

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

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

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

Applications	Certification & Accreditation.
EAS	Yes, 10/13/17

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

Applications	Auditing measures and technical safeguards.
EAS	Specific logging of transaction events (including who entered and when the transaction was completed along with type of financial transaction (such as loan activity, program payments, approvals, determinations, general or subsidiary ledger entries, etc.)); and application parameter/table changes (such as loan rates, penalties, etc.) occurs as part of the nightly process.

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?

Applications	Privacy risks identified and risk mitigation.
EAS	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?

Applications	Project / System type.
EAS	Major Application

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

Applications	Technology privacy risks.
EAS	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"?

Applications	SO and/or ISSPM review of Web guidance.
EAS	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?

Applications	Purpose of 3rd-party websites and/or applications?
EAS	N/A

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Applications	PII availability through 3rd-party websites and/or applications.
EAS	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?

Applications	Use of PII available through 3rd party websites and/or applications.
EAS	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?

Applications	Maintenance and security of PII available through 3rd party websites and/or applications.
EAS	N/A

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Applications	Periodic purging of PII available through 3rd party websites and/or applications.
EAS	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?

Applications	Access to PII available through 3rd party websites and/or applications.
EAS	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?

Applications	Internal / external sharing of PII available through 3rd party websites and/or applications.
EAS	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)?

Applications	SORN requirements for sharing of PII available through 3rd party websites and/or applications.
EAS	N/A

10.10 Does the system use web measurement and customization technology?

Applications	Web measurement and customization technology.
EAS	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?

Applications	User rights for web measurement and customization technology.
EAS	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.

Applications	3rd party websites and/or applications privacy risks and mitigation.
EAS	N/A

Appendix A. Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Farm Service Security Services System (FSSSS).

KURT BENEDICT Digitally signed by KURT BENEDICT
Date: 2019.08.22 07:08:00 -05'00'

Kurt Benedict
Information System Owner

Date

DARREN ASH Digitally signed by DARREN ASH
Date: 2019.08.27 05:09:34 -04'00'

Darren Ash
Agency CIO

Date

JEFFERY WAGNER Digitally signed by JEFFERY WAGNER
Date: 2019.08.23 13:30:24 -04'00'

Jeffery G. Wagner, Jr.
Chief Information Security Officer, FPAC-BC

Date