

# Privacy Impact Assessment Farm Service Customer Outreach Management System (FSCOMS)

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: June 1, 2020
- Prepared for: USDA OCIO-Policy,  
E-Government and Fair Information  
Practices (PE&F)





# **Privacy Impact Assessment for the Farm Service Customer Outreach Management System (FSCOMS)**

June 1, 2020

## **Contact Point**

**J. H. Poole  
FPAC-BC  
240-353-9657**

## **Reviewing Official**

**Kurt Benedict  
Information System Owner  
United States Department of Agriculture  
Farm Production and Conservation (FPAC)  
(816) 823-4212**



### Abstract

This PIA is for the Farm Service customer Outreach Management System (FSCOMS). FSCOMS has two applications; the OTIS application does not contain any PII, however the other application (FSAfarm+) does contain PII. This PIA is required since FSAfarm+ uses personal information of farmers and producers.

### Overview

Although it does not store or gather PII, the FSAfarm+ application uses PII to allow county office users to search for a specific farmer or producer. The specific user information is pulled from the SCIMS database (which resides on the FPCMS system); this information includes:

- First Name, Last Name
- Entity (business) information
- Address Information
- Email
- Phone Number
- Demographic Information
- EIN / SSN (via a search screen)

When the county office users log out of FSCOMS, the memory and cache are automatically cleared (no PII is stored in FSCOMS). FSCOMS does not share PII with any other system.

The legal authority to capture limited PII data is established by USDA SORN System of Records Notices (SORN) FSA-2 and FSA-14.

## 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?**

FSCOMS / FSAfarm+ uses this information:

- First Name, Last Name
- Entity (business) information
- Address Information
- Email
- Phone Number
- Demographic Information
- EIN / SSN (via a search screen)

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

FSAfarm+ requests and receives PII from SCIMS, which resides in the FPCMS system.

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

The PII allows County Office users to search for a specific user as well as a second authentication method to validate farmers and producers.

### **1.4 How is the information collected?**

N/A – PII is not collected by FSCOMS.

### **1.5 How will the information be checked for accuracy?**

N/A – PII is not collected by FSCOMS, therefore it cannot be checked for accuracy.

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

CBS, ARCT, EIS, FLOTrack, SDMS, NATS: Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397

IPIA: Improper Payments Information Act of 2002

PPID, EREP, WKRS: records are retained in accordance with National Archives and Records Administrations General Records Schedule 14. The General Records Schedule 14 covers certain records pertaining to informational services performed by Government agencies in their day-to-day affairs and in their relations with the public, including records created in Freedom of Information Act and Privacy Act (FOIA) programs. These records for PPID consist of the producer’s name and tax ID/SSN.

TMS, VVAS, WEB 52: OMP/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107. USDA/FSA-7: 5 U.S.C. 301

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

- All users must be uniquely identified and authenticated prior to accessing the application.
- Access to data is restricted
- No PII is stored in the FSCOMS system
- When the user logs out of FSCOMS, the memory and cache are automatically cleared

## 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.**

There are 2 uses of PII in the FSAfarm+ application:

- The PII allows County Office users to search for a specific user (farmer or producer)
- If a farmer or producer has an eAuth account, the SSN can be used as a second authentication method to validate the farmer / producer

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

N/A – no tools are used to analyze PII data in FSCOMS

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

N/A – no commercially or publicly available data is used by FSCOMS

**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.**

This application is in compliance with the Federal Information Security Management Act of 2002 (FISMA), USDA Office of the Chief Information Officer (OCIO) Directives, and U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4 guidance.

- Access Control (AC)
- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Security Awareness and Training Policy and Procedures (AT)
- Identification and Authentication (IA)
- Media Protection (MP)
- Physical Access (PE)
- Personnel Security (PS)
- System and Communication Protection (SC)
- System and Information Integrity (SI)

## 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 stored in FSCOMS, therefore PII is not retained by the system. When a user logs out of FSCOMS, the memory and cache are automatically cleared.

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

N/A – data not retained.

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

N/A – data not retained.

## 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?**

FSCOMS does not share PII data with any other system (internal or external).

**4.2 How is the information transmitted or disclosed?**

N/A – data not shared or disclosed.

**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 – data not shared or disclosed.

## 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?**

FSCOMS does not share PII data with any other system (internal or external).

**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 – data not shared or disclosed.

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

N/A – data not shared or disclosed.

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

N/A – data not shared or disclosed.

## 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 Does this system require a SORN and if so, please provide SORN name and URL.**

No.

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

PII is not collected by FSCOMS, therefore this notice would be provided by the system that collects the PII.

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

PII is not collected by FSCOMS, therefore this opportunity / right to decline would be provided by the system that collects the PII.

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

PII is not collected by FSCOMS, therefore this right to consent would be provided by the system that collects the PII.

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

PII is not collected by FSCOMS, therefore this notice would be provided by the system that collects the PII.

## 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?**

PII is not collected or stored by FSCOMS, therefore individuals would gain access through the system that collects the PII.

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

PII is not collected or stored by FSCOMS, therefore PII corrections / updates would occur in the system that collects the PII.

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

PII is not collected or stored by FSCOMS, therefore notification of PII procedures to correct or update their PII would occur in the system that collects the PII.

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

As PII is not collected or stored by FSCOMS, the user can correct or update their PII in the system that collects the PII.

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

No privacy risks have been identified to redress of incorrect information within FSCOMS.

## 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 Control is through eAuthentication.

**8.2 Will Department contractors have access to the system?**

Contractor access is limited to contractors supporting the FSCOMS system / FSAfarm+ application.

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

All USDA employees and contractors, as well as personnel at county offices receive annual PII security training.

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

Yes

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

FSA complies with the "Federal Information Security Management Act of 2002" (FISMA). Assessment and Accreditation, as well as annual key control self-assessments, and continuous monitoring procedures are implemented for this application per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53. Additionally, FSA complies with the specific security requirements for "auditing measures and technical safeguards" provided in OMB M-07-16. Finally, the system provides technical safeguards to prevent misuse of data including:

- Confidentiality: Encryption is implemented to secure data at rest and in transit for this application (e.g., by PIPS 140-2 compliant HTTPS and end-user HMD disk encryption).
- Integrity: Masking is not implemented by this application (e.g., passwords are masked by eAuth).
- Access Control: The system implements least privileges and need to know to control access to PII (e.g., by RBAC).
- Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: Logging is implemented for this application (e.g. by logging infrastructure).
- Attack Mitigation: The system implements security mechanisms such as input validation.

The FSCOMS IT hosting environment and related components capture audit logs at the system level to support incident investigations.

**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?**

- FSCOMS applications do not collect any PII from any individual, but they do utilize PII obtained from other sources.
- FSCOMS does not retain any PII
- FSCOMS does not share any PII
- When FSCOMS users disconnect from the system, the memory and cache are automatically cleared

Minimal risks have been identified for the PII data within FSCOMS. Mitigation occurs through separation of duties and access control policies which ensure that system operators, system administrators, and associated personnel have limited, if any, access to PII.

### 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?**

The application that contains PII is FSAfarm+, a Major Application residing inside the FSCOMS system boundary.

#### **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.

#### **10.2 What is the specific purpose of the agency’s use of 3<sup>rd</sup> party websites and/or applications?**

FSA will not use third party websites for FSCOMS deployment in a production environment.

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

N/A – see 10.2.

**10.4 How will the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications be used?**

N/A – see 10.2.

**10.5 How will the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications be maintained and secured?**

N/A – see 10.2.

**10.6 Is the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications purged periodically?**

N/A – see 10.2.

**10.7 Who will have access to PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications?**

N/A – see 10.2.

**10.8 With whom will the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications be shared - either internally or externally?**

N/A – see 10.2.

**10.9 Will the activities involving the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications require either the creation or modification of a system of records notice (SORN)?**

N/A – see 10.2.

**10.10 Does the system use web measurement and customization technology?**

The system does not use web measurement and customization technology

**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 – see 10.2.

**10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications, discuss the privacy risks identified and how they were mitigated.**

Privacy risks are minimal. There is the unlikely event that data which falls within the PII definition may be erroneously released. The security/privacy training administrator/operator would dispose of such rarely encountered PII immediately.

Additionally, as PII is not stored in FSCOMS, a Disaster Recovery related error is not possible.



## Agency Responsible Officials

---

Kurt Benedict  
FSCOMS Information System Owner  
United States Department of Agriculture

## Agency Approval Signature

---

Brian Davies  
Information Systems Security Program Manager  
United States Department of Agriculture

## Agency Privacy Approval Signature

---

Amber Ross  
FPAC Privacy Officer  
United States Department of Agriculture