Privacy Impact Assessment
FSA Compliance Review
(FSA Compliance Rev)

Technology, Planning, Architecture, & E-Government

- Version: 3.0
- Date Prepared: 06/05/2019
- Prepared for: USDA FPAC CISO

United States Department of Agriculture

Privacy Impact Assessment for the FSA Compliance Review (FSA Compliance Rev)

06/05/2019

Contact Point
Ken Kinard
Project Manager, FPAC-BC
(970)295-5708

Reviewing Official
Jeffery G. Wagner, Jr.
Chief Information Security Officer – FPAC-BC
United States Department of Agriculture
(202) 619-8553

Abstract

The FSA Compliance Review (FSA Compliance Rev) application is a system of the Natural Resources Conservation Service (NRCS).

FSA Compliance Review (FSA Compliance Rev) is an historical application used to sample a subset of tract systems from around the country to ensure compliance reviews are conducted of farms receiving commodity payments and are implementing and/or maintaining conservation practices. Status reviews are conducted on highly erodible (HEL) and wetlands (WET) designated farm tracts.

A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101).

Overview

FSA Compliance Rev is a system of the Natural Resources Conservation Service (NRCS). NRCS provides private landowners with advice, guidance and technical services to carry out conservation practices. The NRCS is an agency within the USDA that has provided over 75 years of leadership in a partnership effort to help America's private land owners and managers. NRCS works with its partners to conserve their soil, water, and other natural resources by providing financial and technical assistance based on sound science and technology suited to a customer's specific needs.

Compliance reviews are conducted to ensure that farms receiving commodity payments are implementing and/or maintaining conservation practices. Compliance reviews are conducted on a yearly basis with a national sample of farm tracts provided to the States. The national sample of farm tracts is derived from records kept by the Farm Service Agency in a Kansas City mainframe. The sample size is approximately 1 percent of the farm tracts that receive a farm payment in the past year and contain cropland. The tracts are provided to the States on January 1 and they can conduct the compliance review at any time during the year. The compliance review determinations must be available to NHQ by December 1. The States have the obligation to add additional farm tracts to the sample set according to the 1985 Food Security Act Manual. The compliance review determination is selected from a list of 12 Highly Erodible Land Conservation (HELC) and 3 Wetland Conservation (WC) determinations. Other information collected by the tracking system are the time spent conducting the review, the number of acres in the tract, and the category identifying why the tract was reviewed.

The Food Security Act of 1985 (otherwise known as the 1985 Farm Bill), as amended, requires producers participating in most programs administered by the Farm Service Agency (FSA) and the NRCS to abide by certain conditions on any land owned or

farmed that is highly erodible or that is considered a wetland. Producers participating in these programs and any person or entity considered to be an "affiliated person" of the producer, are subject to these conditions. Compliance reviews are conducted to ensure that farms receiving commodity payments are implementing and/or maintaining conservation practices. Since the 1985 Farm Bill, eligibility for most commodity, disaster, and conservation programs has been linked to conservation compliance. The 2014 Farm Bill states that the Secretary shall use existing processes and procedures for certifying compliance and does not exempt any producer or land from the conservation compliance provisions.

Legal Authority: This system is regulated by privacy laws, regulations and government requirements, including the Privacy Act (5 U.S.C. §552a); the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101); the Paperwork Reduction Act of 1995 (44 U.S.C. §3501); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559); OMB Memos M-03-22, M-10-22, M-10-23, M-16-24, and M-17-12; and OMB Circular A-130, Appendix I.

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?

- FSA Compliance Rev uses and maintains minimal PII information obtained via the Service Center Information Management System (SCIMS) database. FSA Compliance Rev uses the SCIMS ID to obtain the "Tract Producer" Name and Address.

- FSA Compliance Rev receives PII from the SCIMS database copy (see Section 1.2). The PII that is used and maintained by FSA Compliance Rev includes the name and typical contact information for affected individuals (e.g. program participants, producers), including name, address, and SCIMS ID.

- As reflected on the FSA PIA for Customer Name/Address System (CN/AS)

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

- The *Service Center Information Management System* (SCIMS), maintained by FSA, Service Center Information Management System (SCIMS), CSAM ID # 1672, is the database of customer information that is shared by the three Service Center Agencies, FSA, NRCS, and Rural Development. SCIMS is a repository

for USDA business entity and conservation compliance information. This link allows the most current customer information to be printed on forms and letters. It also allows NRCS managers to generate reports on the race, sex, national origin, and disability of program applicants and participants.

- NRCS has access to a copy of the SCIMS database via replication and access to the data from SCIMS for NRCS users is via NPAD and through eAuthentication (eAuth). NRCS users do not have direct access to SCIMS. The landowners and general public applicants may provide information to SCIMS, which is the source of the PII. All information is obtained through a database copy. FSA Compliance Rev does not modify or update any information in SCIMS.

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

- FSA Compliance Rev is used to facilitate Farm Bill Compliance requirements related to conservation planning, tracking and reimbursement measures. The PII is used to allow the FSA Compliance user to verify that the SCIMS record for the tract exists in FSA. The address is displayed, but only the name and SCIMS ID are retained in FSA Compliance.

1.4 How is the information collected?

- FSA Compliance Rev collects landowner information, including the names, addresses and SCIMS IDs from the SCIMS database copy. NRCS users do not have a direct access to SCIMS. All information is obtained through a database copy.

- Two files are provided by FSA. These files are loaded into a temporary database, and the tract selection process is run to:
    - Identify tracts owned by government employees. These tracts are removed from the database and sent as a separate dataset to the NHQ Program Manager for compliance reviews. States are given a complete set of employee-owned tracts in the state each year.

    - Create a random sample set of about 20,000 tracts spread over all states from the remaining records.

- Various State and Local Government agencies provide data for use within FSA Compliance Review.

1.5 How will the information be checked for accuracy?

- The majority of FSA Compliance Rev data collected is validated and verified by the field office employees and their respective quality assurance contacts above them at the area and state office levels.

- The accuracy of PII obtained from SCIMS is not within the scope of FSA Compliance Rev. FSA Compliance Review does not have the ability to update any information in SCIMS, nor does it have the ability to update the information in any other application databases not maintained by NRCS.

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

These regulations are applicable:

- Privacy Act (5 U.S.C. §552a);
- E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101);
- Paperwork Reduction Act of 1995 (44 U.S.C. §3501)
- Food Security Act of 1985
- 7 CFR Part 12—Highly Erodible Land Conservation and Wetland Conservation

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

- FSA Compliance Rev uses and maintains PII information obtained via SCIMS ID (i.e., "Tract Producer" name and address for farmers receiving commodity payments).

- Privacy risks are mitigated as access to the information will be limited because users are authenticated via the USDA eAuth system and authorized via USDA's role-based authorization for end-user access to the application.

- Please see Section 2.4 and Section 8.6 for a further discussion of security controls that are in place to mitigate privacy risks.

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.

- To facilitate FSA Compliance Review requirements related to conservation planning, delivery, tracking and reimbursement measures.

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

- The tool that is used to analyze Farm Service Agency (FSA) data and perform compliance reviews involves a sampling methodology. These reviews are conducted on a yearly basis, based on a national sample of farm tracts that is provided to the States. The national sample of farm tracts is derived from records kept by the FSA in SCIMS.

- The States produce data related to a compliance review determination. The States can conduct the compliance review at any time during the year, and compliance review determination must be available to NHQ by December 1.

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

- FSA Compliance Rev does not use commercial or publicly available 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.

- This application is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.

- If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

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?

- All information contained will be retained in compliance with NARA Guidelines, which vary on average in years from less than one year to more

than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017.

- Per the NRCS-1 System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs".

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

- Yes

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 primary privacy risk is that a data breach could result in the release of information on program participants and producers. This is mitigated by limited access to the data, nonportability of the data and controlled storage of the data located in controlled facilities.

- Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed above.

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?

- FSA Compliance Rev obtains information related to landowners from SCIMS. FSA Compliance Rev does not share or transmit any information to SCIMS, nor does it update any information in SCIMS.

- High level summary of FSA Compliance Rev reports is made publicly available. The summary reports do not contain PII.

4.2 How is the information transmitted or disclosed?

- NRCS has access to a copy of the SCIMS database via replication. Access to the data is through established security rules via eAuth.

- PII (name and address) information is obtained from SCIMS database for use by the FSA Compliance Rev application, however no PII Information is transmitted or disclosed by internal users.

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.

- Privacy risks are mitigated by ensuring that access to the data is through established security rules via eAuth. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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- PII is not shared or disclosed with organizations that are external to the USDA.

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- PII is not shared or disclosed with organizations that are external to the USDA.
- However, FSA Compliance Rev is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

- FSA Comp Rev is subject to the following FSA SORNs: USDA/FSA-2 – Farm Records File (Automated) and USDA/FSA-14 – Applicant/Borrower.

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

- N/A- PII is not shared or disclosed with organizations that are external to the USDA.

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

- Privacy risks are mitigated by virtue of NOT sharing information external to the USDA. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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.

- FSA Compliance Rev is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

- Yes. NRCS Privacy Policy published on USDA website.
- Yes, FSA Privacy Policy, which states that "Submitting information is strictly voluntary."

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

- The information in FSA Comp Rev is based on the rules of the source database. Any PII information is obtained from the SCIMS system, which is maintained by FSA.

- Individuals have a right to consent in accordance with the FSA Privacy Policy and the individual's written consent.

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

- The information in FSA Comp Rev is based on the rules of the source database. Any PII information is obtained from the SCIMS system, which is maintained by FSA.

- Individuals have a right to consent in accordance with the FSA Privacy Policy and the individual's written consent.

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.

- Any PII information that is obtained from the SCIMS system, is maintained by FSA.

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/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

- Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

- As published in SORN USDA/NRCS-1: "Any individual may obtain information as to the procedures for contesting a record in the system which pertains to him/her

by submitting a written request to the district conservationist or his/her designated representative or to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013."

- Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to correct their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

- The SORN USDA/NRCS-1 is published on the USDA.gov website.

- Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to correct their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

- *N/A*- See section 7.3.

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

- The risk associated with redress is considered low, as the public does not have access to the system or the data. Any PII information obtained from the SCIMS system would be subject to the applicable procedures governing their SCIMS information as maintained by the FSA.

- Residual privacy risks associated with the redress process for individuals are mitigated since individuals can use the relevant procedures discussed above to update their original public records.

Section 8.0 Technical Access and Security

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

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

- Access to the FSA Compliance Rev system is determined via the USDA eAuth system (level II) and authorized via USDA's Role Based Access Control (RBAC) model for end-user access to the application.

- The application/system has documented Access Control Procedures, in compliance with FISMA and USDA directives. See Section 2.4.

8.2 Will Department contractors have access to the system?

- Yes. Department contractors with a need to know will have access to this application as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements.

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

- NRCS requires that every employee and contractor receives information security awareness training before being granted network and account access, which contains the requisite privacy training, and Annual Security Awareness and Specialized Training, as required by FISMA (NIST SP 800-53 rev 4) and USDA policies (USDA OCIO DR 3545-001 – Information Security Awareness and Training Policy and USDA OCIO DR 3505-003 - Access Control Policy).

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

- Yes. FSA Compliance Rev's authorization to operate (ATO) dated on 07/12/2016.

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

- NRCS complies with the "Federal Information Security Modernization Act of 2014" (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, Rev. 4. Additionally, 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 FIPS 140-2 compliant HTTPS and end-user hard disk encryption).

- Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).

- Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC). Administrative and management operational controls in place to ensure proper access termination.

- 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.

Notice: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

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?

- FSA Compliance Rev does not directly collect any PII from any affected landowner (i.e., member of the public), but FSA Compliance Rev does utilize PII within the system which is obtained from SCIMS, which is maintained by FSA (see Section 1.0 above). Data extracts containing PII are not regularly obtained from the system, therefore, privacy risk from this area is limited and addressed through IT Data Extract processes controls. Any PII information is obtained from the SCIMS database, copied from the SCIMS system, which is maintained by FSA.

- Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5, and by the security controls discussed in Section 2.4 above. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5, respectively.

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?

- FSA Compliance Rev is a web-based application housed within the OCIO-NITC Data Center in Kansas City, MO.

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

- No, the project utilizes Agency approved technologies, and these technology choices do not raise privacy concerns.

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 3rd party websites and/or applications?

- Not applicable, third party websites/applications are not used.

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

- Not applicable, third party websites/applications are not used.

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

- Not applicable, third party websites/applications are not used.

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?

- Not applicable, third party websites/applications are not used.

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

- Not applicable, third party websites/applications are not used.

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

- Not applicable, third party websites/applications are not used.

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?

- Not applicable, third party websites/applications are not used.

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)?

- Not applicable, third party websites/applications are not used.

10.10 Does the system use web measurement and customization technology?

- No, 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?

- Not applicable, the system does not use web measurement and customization technology.

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.

- FSA Compliance Rev does not provide access or link to Third Party websites or applications. In addition, the system does not use web measurement or customization technology.

Responsible Officials

LATHARD KINARD

Digitally signed by LATHARD KINARD
Date: 2019.06.06 14:12:29 -06'00'

Ken Kinard
Project Manager. FPAC-BC
United States Department of Agriculture

Approval Signatures

JEFFERY WAGNER

Digitally signed by JEFFERY WAGNER
Date: 2019.06.07 14:14:51 -05'00'

Jeffery G. Wagner, Jr.
Chief Information Security Officer – FPAC-BC
United States Department of Agriculture