Privacy Impact Assessment
Affiliates (Affiliates)

Policy, E-Government and Fair Information Practices

- Version: 3.1
- Date: February 10, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the Affiliates (Affiliates)

February 10, 2020

Contact Point

Pamela Leith
Natural Resources Conservation Service
970-295-5704

Reviewing Official

James Flickinger
Chief Information Security Officer
United States Department of Agriculture
(816) 926-6010

Abstract

The Affiliates (Affiliates) application is a system of the Natural Resources Conservation Service (NRCS).

The Affiliates application provides a way for authorized NRCS employees to facilitate the process of access control determinations to NRCS systems and applications for select non-NRCS personnel (known as “affiliates”)

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

Affiliates 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.

Affiliates is an application that manages access privileges for non-Federal employees or Affiliates of NRCS. Affiliates are non-employees, typically contractors, who perform services, act on behalf of the government organization, or whose duties on behalf of the government organizations require them to have similar access privileges as government employees. When establishing authorization privileges for affiliates to access government information and to use government systems, it is essential that the identity of the person be known to NRCS, as well as information about the organization they represent and the current status of their relationship with USDA. This information is stored and maintained in the Affiliates Database. The various county-based agencies have a number of affiliates, including contractors, Conservation District employees, State/Local Governments, RC&D employees, volunteers, Lenders, County Committees, Technical Service Providers, and non-profit outreach organizations.

The Affiliates system is only accessible by NRCS employees. While there are many types of non-employees, it must be stressed that none of these "affiliates" has any form of access to the Affiliates application itself.

A typical Affiliates transaction is as follows: An NRCS employee enters the Affiliates information into the Affiliates database. The affiliate's (non-employee's) Level 2 eAuthentication (eAuth) account is linked to the affiliate record. The zRoles application is then used to assign specific roles to the Level 2 account, which allows the affiliate access to various NRCS applications. Single Sign-On (SSO) “eAuth” accounts are used for non-privileged access. The Affiliates application does not update or modify the eAuth Active Directory in any way.

While information in the Affiliates application is not transmitted or shared with any other organizations, automated "sharing" does occur between the Affiliates application and the NRCS zRoles application. The zRoles application does not update or modify the Affiliates database in

any way. NRCS applications or systems contact zRoles to verify the level of authorization granted to affiliates to access their systems.

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?

- Names, business address and contact information, and Affiliate ID of Contractors, Conservation District employees, State/Local Government employees, Resource Conservation & Development Council employees, Volunteers, Lenders, County Committees, Technical Service Providers, and non-profit outreach organization personnel (referred to as Affiliates).

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

- An NRCS employee enters the information about the individual non-employee affiliate, which is populated from information that was provided by the non-employee.

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

- The information is maintained to track pertinent affiliate information to provide to the NRCS zRoles application. The information is shared between the Affiliates application and the NRCS zRoles application for the purpose of assigning specific roles in eAuth to affiliates

1.4 How is the information collected?

- Individual affiliates provide their information to an NRCS employee with the appropriate system access to the Affiliates application. The NRCS employee enters the information. The affiliates do not have access to the Affiliates application.

1.5 How will the information be checked for accuracy?

- Information is provided directly to an NRCS employee by the affiliate

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)

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

- NRCS employees obtain names, business addresses and contact information from affiliates, which is added to the Affiliates database. Individual affiliates may choose to provide personal information, but it is not solicited, and if collected, it would be identified as 'other' information in the database.
- Privacy risks are mitigated because access to the information will be limited to appropriate NRCS personnel and partners by the use of eAuth, which provides user authentication for NRCS. Role Based Access Control (RBAC) provides access enforcement for the Affiliates application. Other access requirements include the need for users to be on the USDA network backbone, using a CCE computer.
- 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 maintain and track pertinent affiliate information and share this information with zRoles to ensure appropriate access control is given to those affiliates when zRoles is contacted by various NRCS applications to grant access.

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

- Data is not 'analyzed'. It is used only comparatively for validation and verification purposes.

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

- Affiliates 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 about an affiliate or about an affiliate who no longer has any association with NRCS. 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?

- Information is shared between the Affiliates application and the NRCS zRoles application for the purpose of assigning specific roles in eAuth.

4.2 How is the information transmitted or disclosed?

- An NRCS employee enters the affiliate's information into the Affiliates database. The affiliate's Level 2 eAuth account is linked to the affiliate record. The zRoles application is then used to assign specific roles to the Level 2 account.

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.

- However, Affiliates is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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.

- Affiliates 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

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

- Yes. Applicants provide information voluntarily to be included in the Affiliates application.

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

- Applicants provide information voluntarily to be included in the Affiliates application. There is a singular use for the information voluntarily provided by the applicant.

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.

- NRCS personnel individually advise affiliates applying for eAuth credentials what information is being collected, the purpose of the collection and how the data will be used.

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.).

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."
- If the data initially given to NRCS changes, affiliates are advised during their initial data submission that it is the NRCS Affiliate's responsibility to notify their NRCS Government Project Manager of changes.

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.

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.

- There are no privacy risks specifically associated with the redress process other than the possibility that the initial data entry made by NRCS on behalf of the affiliate is incorrect. That risk is mitigated by the necessity of eAuth data (entered by the affiliate) corresponding to the Affiliates data for initial and subsequent logins. If eAuth access is granted, but unachievable, then the affiliate's data must be validated.
- 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 Affiliates application 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 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?

- No. The Affiliates system is only accessible by NRCS employees. While there are many types of non-employees, it must be stressed that none of these "affiliates" has any form of role-based access to the Affiliates application itself.

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.

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?

- Privacy risks are mitigated by specific security controls including enforcement of "need to know" and "least privilege" via RBAC as discussed above, as well as the implementation of Department approved encryption measures for data at rest and data in transit.
- 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?

- Affiliates is an NRCS application hosted on devices using common COTS hardware and software configured in accordance with USDA baseline configurations for servers and web portals. This application supports user access control authorization and validation.

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?

- *N/A* - 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.

- *N/A* - 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?

- *N/A* - 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?

- *N/A* - 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?

- *N/A* - 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?

- *N/A* - 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?

- *N/A* - 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)?

- *N/A* - 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?

- *N/A* - See section 10.10.

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.

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

Agency Responsible Officials

JAKE ZEBELL

Digitally signed by JAKE ZEBELL
Date: 2020.04.13 19:56:07 -06'00'

Jake Zebell
Affiliates Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS

Digitally signed by LANITA THOMAS
Date: 2020.04.14 12:41:24 -04'00'

Lanita Thomas
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

AMBER ROSS

Digitally signed by AMBER ROSS
Date: 2020.04.16 14:15:24 -05'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture