Privacy Impact Assessment
Affiliates

Technology, Planning, Architecture, & E-Government

- Version: 2.07
- Date: July 8, 2013
- Prepared for: USDA OCIO TPA&E

USDA

United States Department of Agriculture

Privacy Impact Assessment for the

AFFILIATES/AFFILIATES LINK MANAGER

July 8, 2013

Contact Point
Paige Niederer
Natural Resources Conservation Service
970-295-5496

Reviewing Official
Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture
202-720-8493

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

This PIA addresses the Affiliates application, which is a system of the Natural Resources Conservation Service (NRCS).

The Affiliates application (including the integrated Affiliates Link Manager component) 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 Management Act of 2002 (FISMA) and the E-Government Act of 2002 (Public Law. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) Federal Law.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

The designated NRCS system owner for Affiliates/Affiliates Link Manager is George Cleek; the designated project manager is Paige Niederer.

The purpose of the Affiliates system is to provide a way of facilitating access control determinations and ultimately access to NRCS systems and applications by select non-NRCS personnel (also known as "affiliates"). The Link Manager functionality specifically links the Affiliate record to an eAuth ID when/if Level 2 access has been established for a particular person.

The Affiliates application maintains PII information related to 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. This access is necessary to aid NRCS in its core mission of conservation planning.

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 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 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 access to various NRCS applications.

Manual "sharing" occurs when an authorized Affiliates user (i.e., an NRCS employee) searches for and selects the correct Level 2 eAuth account from the read-only eAuth Active Directory. 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.

Affiliates is effectively a single database that maintains actual and prospective non-NRCS employee account subscriber information without subordinate modules or subsystems.

Authority to operate the Affiliates application is provided by the ATO granted in 2010.

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?

Affiliate names, business contact information and business organization information.

Note that Affiliates explicitly does not directly "collect" any PII from any "affiliate."

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 used and maintained in order to facilitate eAuth access control determinations and ultimately access to NRCS systems and applications by select non-NRCS personnel (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 application explicitly does not directly "collect" any PII from any "affiliate," because these non-employees do not have any form of access to the Affiliates application itself.

1.5 How will the information be checked for accuracy?

Information is provided first hand; no provision for accuracy checks.

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

- Federal Register /Vol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)

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

The Affiliates application does not directly "collect" any PII from any "affiliate."

Aside from individual names, Affiliates does not collect information on individuals traditionally considered PII. Instead only business (non-personal) contact information is solicited and recorded. Individual affiliates may choose to provide personal information (home phone numbers and/or addresses), but it is not solicited or desired and is specifically identified as 'other' information in the database as opposed to 'home'.

Privacy risks are mitigated because access to the information will be limited to appropriate NRCS personnel and partners by the use of the USDA-OCIO-eAuthentication application, 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 and Section 8 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 to ensure appropriate access control is given when granting affiliates access to NRCS applications. Affiliates data is linked to each NRCS application that necessitates access by an affiliate.

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

N/A – Data is not 'analyzed'. It is used only comparatively for validation and verification purposes. PII is limited to that which is entered; data is not manipulated or reformatted.

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

N/A – 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 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 3 guidance.

- Access Control (AC)
- 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?

Application-specific information is retained while the application remains in production. Per NARA General Records Schedule 20, this application-specific information has been authorized by the NRCS Records Manager for erasure or deletion when the agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes.

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.

Primary risk is that a data breach could result in the release of information on an affiliate who no longer has any association with NRCS. This is mitigated by limited

access to the data, non-portability of the data and controlled storage of the data on Gov't equipment located only at Gov't 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?

N/A. Affiliates information is not shared with other internal USDA organizations.

4.2 How is the information transmitted or disclosed?

N/A. Affiliates information is not shared with other internal USDA organizations.

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 virtue of NOT sharing information.

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. Affiliates information is not shared with organizations external to NRCS.

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. Affiliates information is not shared with organizations external to NRCS.

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

N/A. Affiliates information is not shared with organizations external to NRCS.

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.

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?

N/A – No PII is directly solicited from any individual to support this application, so no "Notice" is provided to individual affiliates.

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

N/A – Individuals are required to provide business contact associated information (non-PII) as part of the application process. No PII information is directly solicited from any individual to support this application. Individual applicants may voluntarily provide it in lieu of the preferred business contact information, but it is not entered or identified as such.

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

N/A – Since there is only a singular use for the information, initial access authorization and subsequent validation are all that need to be employed.

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.

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. Notice of PII collection does not need to be provided directly to individuals by this application. Only non-PII business contact information is solicited or desired, but respondents can provide personal information as an alternative, but such action is voluntary on their part. Even if provided, it is not recorded or identified as such by the system, only as 'Other' address and phone number info.

Because no PII is solicited from any individual "affiliate" by this application, "Notice" does not need to be provided to any individuals. There is no risk that an individual would be unaware of "collection," because no PII is solicited or directly collected from any individual "affiliate" by this application.

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?

N/A – No procedures are required. The purpose of Affiliates is to provide a way to facilitate access control determination to NRCS systems. Contractors and other "affiliates" are not authorized to access this application.

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

N/A – No procedures are required, because "affiliates" are not authorized to access the Affiliates application. 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?

N/A – No procedures are required, because "affiliates" are not authorized to access the Affiliates application. NRCS affiliates provide their initial data in real time to NRCS employees. See 7.2.

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

N/A – See 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 Affiliates data must be validated.

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 this application is enforced via Role-Based Access Control (RBAC) on a valid "need to know" basis, determined by requirements to perform applicable official duties. 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, this is controlled by Role-Based Access Control (RBAC).

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?

Annual organizational Privacy Awareness Training is mandatory for all NRCS personnel. NRCS requires that every employee and contractor receives information security awareness training before being granted network and account access, per General Manual, Title 270, Part 409 - Logical Access Control and Account Management. Annual Security Awareness and Specialized Training is also required, per FISMA and USDA policy, and is tracked by USDA.

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

In progress, scheduled to be complete by 9/2013.

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

NRCS 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, Revision 3.

NRCS complies with the specific requirements for "auditing measures and technical safeguards" that are provided in OMB M-07-16, including the security requirement that all data on mobile computers/devices carrying agency data must be encrypted using only NIST certified cryptographic modules.

- Encryption that is performed outside of the accreditation boundary of this application is discussed in Section 8.6 below. Given the limited sensitivity and scope of the information retained, this application does not encrypt PII within the database.
- Masking of applicable information is performed outside of the accreditation boundary of this application (e.g., passwords are masked by eAuth). This application does not process the type of very sensitive PII that would require masking (e.g., SSN). Given the limited sensitivity and scope of the information retained, this application does not mask any PII (e.g., "Name" is not masked).
- Controlled access to PII is implemented outside the accreditation boundary of this application (e.g., via multi-factor authentication for remote access). While the PII information retained has limited sensitivity and scope (i.e., the Name of non-employee "affiliates"), this application does control (limit) access to PII. The access of an Affiliate user (i.e., an NRCS employee) is generally limited to the "scope" of their office.
- Timeout for remote access is implemented outside of the accreditation boundary of this application (e.g., by eAuth), so this application does not need to implement timeout for remote access to PII due to inactivity.
- System audit logs are implemented outside of the accreditation boundary of this application. This includes internal audit logs that are used to ensure that administrative functions and activities are being logged and monitored (e.g., modifications, additions, and deletions of privileged accounts per the eAuthentication SLA). Given the limited sensitivity and scope of the information retained, this application does not implement system audit logs

related to PII integrity, nor does this application implement a Security Information and Event Management (SIEM) log management system.

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?

- This application explicitly does not "directly collect" or "share (internally or externally)" any PII from any non-employee affiliate.
- Specific 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 (per NIST SP 800-53 Revision 3 and using FIPS 140-2 compliant algorithms).
    - To mitigate the privacy risk of "data at rest" being lost or stolen, all CCE laptops that access this application are protected with whole disk encryption.
    - To mitigate the privacy risk of "data in transit" being intercepted / stolen, this application uses HTTPS encryption.
    - Given the limited sensitivity and scope of the information retained, encryption is not implemented within the application database.
- All security controls provided by external information systems are reviewed and monitored for compliance annually by NRCS Security as a part of the NRCS continuous monitoring program. Security controls provided by external information systems are identified in SLAs and ISAs, including the following:
    - To mitigate the privacy risk of back-up media (e.g., tapes) being lost or stolen, all back-ups are encrypted per the Service Level Agreement.
    - To mitigate the privacy risk of data being retained longer than required, application-specific data will be erased/deleted using NIST-compliant disposal methods per the Service Level Agreement when the agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes per Section 3.
- Residual privacy risks associated with the sensitivity and the scope of PII that is maintained in this application are mitigated by the technical security controls discussed in Section 2.

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 - 3rd 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 - 3rd 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 - 3rd 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 - 3rd 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 - 3rd 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 - 3rd 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 - 3rd 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 - 3rd party websites / applications are not used.

10.10 Does the system use web measurement and customization technology?

N/A. 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 10.10.

10.12 <u>Privacy Impact Analysis</u>: 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.

Privacy risks are nominal. Affiliates does not provide access to or link to Third Party Applications. In addition, the system does not use web measurement and customization technology.

Responsible Officials

PAIGE NIEDERER

Digitally signed by PAIGE NIEDERER
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=PAIGE NIEDERER, 0.9.2342.19200300.100.1.1=12001000077807
Date: 2013.07.11 14:25:52 -06'00'

Paige Niederer — Date
NRCS
United States Department of Agriculture
This signature certifies that the above PIA responses are provided to the best of my knowledge and understanding.

Approval Signature

7/12/13

Mr. Lian Jin — Date
Acting Chief Information Security Officer
United States Department of Agriculture
This signature certifies that the PTA analysis and PIA determination due diligence has been conducted pursuant to Department guidance and NIST regulations.