

Privacy Impact Assessment eLearning Center (eLearn)

Natural Resources Conservation Service Information Security

- Version: 1.2
- Date: August 2, 2013
- Prepared for: USDA NRCS





Privacy Impact Assessment for the eLearning Center

February 11, 2012

Contact Point
Paige Niederer
NRCS
(970) 295-5496

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



Abstract

The NRCS eLearning Center (eLearn) application's main objective is to provide NRCS employees, Customers and Partners, and the General Public with easy access to USDA/NRCS training and educational resources. eLearn contains training modules that were published prior to the availability of AgLearn, as well as records of individual personnel training progress and completion. This PIA is required since eLearn contains the names, home addresses, and telephone numbers of users.

Overview

eLearn is a legacy system that entered production prior to the deployment of the USDA's AgLearn training system. eLearn provides web accessible training materials and activities to US government personnel, State and local government partners, and members of the general public. Users authenticate to eLearn using their USDA eAuthentication Level 1 or Level 2 credentials, depending upon individual training requirements. eLearn presents training materials within a graphical user interface, or via downloadable content. The application maintains records of users planned and completed training, and offers the option to print certificates of completion and accrued continuing education unit reports. eLearn does not share any information with other USDA or external systems. The legal authority to capture limited PII data is established by USDA System of Records Notice (SORN) "NRCS-1".

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?

eLearn maintains individual training records for USDA employees and associates. The following elements are imported from the USDA eAuthentication Application during account establishment and account management activities: user names, phone number and email address. While the data is initially imported from eAuth (based upon whatever eAuth originally collected from the user), the data can also be changed by the user in eLearn (e.g., maintained via the User Profile screen). The data is home or work or cell: whatever the user typed in.

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

The PII is sourced directly from the user by collection from the USDA eAuthentication application. The connection between eLearn and eAuth is specified in the eAuth ISA. Note that the user can also maintain their information in eLearn,



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

The information is used to for training completion certificates, , training reports, and/or other material which may be provided to the users.

1.4 How is the information collected?

The PII is entered directly by the user when they first establish an account within eLearn. When using the USDA eAuthentication Application to authenticate, eLearn will capture the eAuth user account data (name, address, telephone) upon first login.

1.5 How will the information be checked for accuracy?

eLearn users are responsible for validating the accuracy of PII within eLearn. If the PII is imported from eAuth, the user will be prompted to verify that the information is correct when first logging in via eAuth.

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

An Interconnection Security Agreement is in place between NRCS and eAuth (EAS I&AMS) that addresses security responsibilities of all parties sharing data with eAuth.

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

Minimal privacy risks have been identified. Individual names, and training course information related to each user, would have minimal impact on the users themselves or the USDA.

For the eLearn application, there is a risk that an un-authenticated user will gain access to the application. Mitigation: Common mitigation is provided by the USDA-OCIO-eAuthentication application, which provides user Authentication for NRCS.

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.

No PII data exists in any documents—it is not in any of the training materials. The only PII uses are to maintain an updated user profile. There are no other authorized or planned uses for the PII collected.

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

eLearn data is not subject to any routine analysis by the USDA. PII contained within eLearn will not be used for any purpose other than for identifying users who have completed training courses.

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

No PII is used in the publicly available training material provided by eLearn. or sensitive information is included within eLearn.

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) as reflected in CSAM, USDA Office of the Chief Information Officer (OCIO) Directives, and U.S. National Institute of Standards and Technology (NIST) guidance, including applicable controls provided in these NIST Special Publication 800-53 control families.

- Access Control (AC)
- Security Awareness and Training (AT)
- Identification and Authentication (IA)
- Media Protection (MP)
- Physical and Environmental Protection(PE)
- Personnel Security (PS)
- Risk Assessment (RA)
- 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, 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.

The primary privacy risk is that a data breach could result in the release of information on members of the public. This is mitigated by limited access to the data, non-portability 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?

eLearn does not share (outbound) PII data with any other system or organization within USDA.

4.2 How is the information transmitted or disclosed?

eLearn does not have the capability to directly share PII with other systems.

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.



Minimal risks have been identified related to internal sharing of PII data.

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?

eLearn does not share PII data with any other system or organization external to 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. However, if sharing were to occur, this is covered by the NRCS SORN "NRCS-1." See 5.1.

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

N/A. See 5.1

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

There are minimal risks identified with external sharing since such sharing is at the discretion of the individual users. The electronic data retrieval system is secured by the USDA Common Computing Environment user authentication process and USDA eAuthentication login and password protection. Offices are locked during non-business hours.

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?



Notification of the collection of PII occurs when a user completes their eAuth account request form. PII data within eLearn is derived from the user's eAuth account, or manually updated by the user themselves after their first authentication via eAuth.

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

Users are notified that disclosure is voluntary when they complete the eAuth Account Request form. eAuth accounts are denied if the user-supplied PII cannot be verified by a Local Registration Authority.

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

Potential use of PII is described during the eAuth registration process. Consent of use is explicitly granted by users through submittal of an eAuth Account Request form. The USDA Office of General Counsel (OGC) can be contacted regarding privacy issues.

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.

The use notice is provided to users when they complete their application for eAuthentication access on the web site. The access request will not continue for processing unless the user acknowledges the notification.

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?

Users can gain access to their PII within eLearn at any time, by logging in and selecting the user profile information.

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



Users are able to modify their PII at any time from within eLearn. Note that changes made to information within eLearn will not be propagated to eAuth or any other USDA system.

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

Users are prompted to review and save their PII within eLearn when they first log on to the system. Any follow-on changes within the application are at the discretion of the user.

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.

Minimal privacy risks have been identified related to redress of incorrect information within eLearn. Privacy risks are mitigated since only the individual has access to their profile—the public does not have access. System administrators would have security background checks.

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?

Any user who has received an approved eAuthentication account may access eLearn. The process for obtaining access authorization is available on the eLearn web site for all interested parties.

8.2 Will Department contractors have access to the system?

Department contractors will have access to eLearn.

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 most personnel at other State, local, and partner agencies, receive annual PII security training. Members of the general public can seek PII security training at their discretion.

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

eLearn is seeking ATO for the first time.

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. Additionally, NRCS 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 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).
- **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?

eLearn does not “directly” collect any PII from individuals, however it does utilize PII that is obtained from eAuthentication.



eLearn does not “share/transmit” any PII internally (to other USDA agencies) or externally (outside of the USDA). eLearn does utilize PII within the system (see section 1.0 above). Data extracts are not regularly obtained from the system, therefore, privacy risks from this area is limited and addressed through IT data extract process controls.

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?

eLearn is a legacy application hosted on devices using common COTS hardware and software configured in accordance with USDA baseline configurations for servers and web portals. eLearn is not undergoing new development activities at this time.

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 3rd party websites and/or applications?

The agency does not use third party websites.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd 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 3rd 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 3rd 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 3rd 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 3rd 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 3rd 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 3rd 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 10.10.

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.

Privacy risks are nominal. eLearn's focus is on non-PII data. However, data is always subject to human error. There is the unlikely event that data which falls within the PII definition may be erroneously engaged. The security/privacy training administrator/operator would dispose of such rarely encountered PII immediately. Disaster recovery related error may occur. PII is collected only for registration (and certificate mailing) purposes and only NRCS staff/administrators (with background checks and training) have access to that PII.

Responsible Officials

paige.niederer@
usda.gov

Digitally signed by
paige.niederer@usda.gov
DN: cn=paige.niederer@usda.gov
Date: 2013.08.02 08:58:52 -06'00'

Ms. Paige Niederer
NRCS
United States Department of Agriculture

Approval Signature



Privacy Impact Assessment – eLearn

A handwritten signature in black ink, appearing to read "Lian Jin", written over a horizontal line.

8/2 / 2013

Mr. Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture