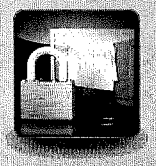
Privacy Impact Assessment
zRoles

Technology, Planning, Architecture, & E-Government

- Version: 1.0
- Date: September 27, 2012
- Prepared for: USDA OCIO TPA&E

USDA

United States Department of Agriculture



Privacy Impact Assessment for the

zRoles

September 27, 2012

Contact Point
Paige Niederer/George Schrader
Project Manager, USDA-NRCS-ITC
Information Technology Center
United States Dept of Agriculture
Natural Resources Conservation Service
2150 Centre Avenue, Building A
970-295-5496

Reviewing Official
Ray Coleman
Director of IT Security
United States Dept of Agriculture
Natural Resources Conservation Service
1400 Independence Ave. SW 20250; Rm. 6164-S
202-205-7712

Abstract

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

> The purpose of the zRoles application is to provide a streamlined, single source for the assigning of application roles and scope to NRCS agency employees, affiliates and technical service providers to access NRCS applications. Daily feeds into zRoles from the human resources systems of empowHR for federal employees, Affiliates for non-federal employees and TechReg for Technical Service Providers give active/inactive status that is then given to all downstream applications. This provides a single cutoff when a deactivation occurs. It also provides information on new users added from the source data feeds.

This Privacy Impact Assessment (PIA) is being conducted to comply with 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 zRoles system also provides the ability for user role and scope assignments by application that is utilized by the specific application. The zRoles system is located in the ITS (Information Technology Service) NITC (National Information Technology Center) data center in Kansas City.. Reports are provided to be able to see a user's particular roles, what roles are able to grant other roles as well as how certain roles are excluded from other roles (separation of duties).

- For applications that are not using zRoles to manage roles, zRoles provides a User Access Web Service that determines whether a user that is logging in to an application is a valid user.
- User information in zRoles is maintained by the authoritative source for each user type. E.g., employee information is maintained by jobs that look at employee data from Empower; affiliate information is maintained by the Affiliate application. The authoritative systems are responsible for maintaining an 'Enabled' indicator for each user. Within zRoles the Security Officer has the ability to override any user's access by turning off a user's 'Access' indicator. This is used for cases when the authoritative system is behind in adjusting a user's 'Enabled' indicator, e.g., an employee's termination record is late.

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?

The zRoles application generally provides the following:

Categories of Data:

- EAuth accounts- (i.e., ID)
- User data
- Role and Scope Management
- Reports

Categories of Users:

- NRCS Employees
- NRCS Affiliates – (i.e., Contractors, TSP, etc…)
- NRCS Customers

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

The zRoles receive sources of information from NRCS Affiliates databases, feeds from EmpowHR, direct data entry from users and Webservices that provide data to the zRoles database.

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

Information being collected, used, disseminated, or maintained to provide the ability for user role and scope assignments by application that is utilized by the specific application.

1.4 How is the information collected?

The zRoles application user accounts are managed by Eauth. There are two types of users allowed to use the zRoles system, Employees and affiliates.
Employees are granted a user account when they are entered into EmpowHR, the USDA HR system. EmpowHR has a data feed to NFC, which in turn sends data to eAuth. EAuth has an automated process to create a user account for new employees when a record is received from NFC. An automated process deactivates the account when an employee is terminated.

Affiliates register for a level 2 eAuth user account using the self registration web pages. Then they find a Local Registration Authority (LRA) to identity proof them and link the account to an Affiliate record. The affiliate record has a type. The following affiliate types are allowed access to IAS applications: State Government Employees, Local Government Employees, conservation District Employees and RC&D Employees. The LRA is responsible for deactivation of the affiliate record when the person is terminated.

1.5 How will the information be checked for accuracy?

The zRoles application user accounts and information are managed for data accuracy, relevance, timeliness, and completeness by the appropriate business requirements and business sponsor by eAuth. The Affiliates, Non-NRCS and NRCS employee information owner's verifies information, with USDA oversight.

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.)

SLA with ITS Hosting: NRCS_ITS_SLA_FY2010.pdf

ISA with USDA eAuthentication: FY10_EAuth_SLA_2010.pdf

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

The following are risk for the applications:

- Unauthorized system access through the USDA OCIO eAuthentication system.
- Improper identification through the USDA OCIO eAuthentication system.

Mitigation: Common mitigation is provided by the USDA-OCIO-eAuthentication application, which provides user Authentication for NRCS. When required by the application business, Role-based Access Control, granted through the NRCS Delegation of Authority and using eAuthentication to verify user authentication, the software utilities called 'ZRoles' or 'IASRoles' set application level permissions for access to the specific Application. Other access requirements can include the need for users to be on the USDA network backbone, using a CCE computer.

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.

The zRoles application is to provide a streamlined, single source for the assigning of application roles and scope to NRCS agency employees, affiliates and technical service providers to access NRCS applications. Daily feeds into zRoles from the human resources systems of empowHR for federal employees, Affiliates for non-federal employees and TechReg for Technical Service Providers give active/inactive status that is then given to all downstream applications. This provides a single cutoff when a deactivation occurs. It also provides information on new users added from the source data feeds.

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

zRoles is a database application that provides the capability of reporting and does not have the ability to analyze data. The data is stored within zRoles database and accessed via webservices and through a UI (user interface).

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

zRoles 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.

zRoles will use eAuthenication for login access. Automated feeds are used to enable and disable accounts ensuring information is handled accordingly.

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?

Data is not normally purged from the zRoles application. It may be purged or archived, per zRoles member's discretion. Refer to Section 3.2 regarding the NARA guidelines.

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

Per NARA Code of Federal Regulations - 36 CFR 1220, Subchapter B – Records Management and USDA OCIO Department Regulation 3080-001 at http://www.ocio.usda.gov/directives/doc/DR3080-001.htm:
NARA Approval: NARA approval is required for all official records schedules. SF-115 shall be submitted to NARA for approval. External approval has already been granted for records covered by the General Records Schedules (GRS). No external approval is required for the disposition of nonrecord materials. An informational copy of the SF-115, in both hard copy and electronic format, shall be provided to the Departmental Records Officer at the same time that the original is sent to NARA.
Electronic Records: Electronic records should be scheduled in the context of entire information systems, along with appropriate documentation and related indexes, and provide the necessary elements:

(a) All input records or source documents;
(b) All information recorded on electronic media;
(c) All output records;
(d) The documentation associated with the system; and,
(e) Any related indexes.

As with audiovisual and microform records, permanent electronic records should not be proposed for long-term storage at Federal records centers, but should be transferred directly to the National Archives.

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

Section 3.3 is not applicable to the Zroles application. There is no restriction as to how long data is retained within zRoles, therefore no risks are to be mitigated.

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?

The zRoles application receives daily feeds into zRoles from the human resources systems of empowHR for federal employees, Affiliates for non-federal employees and TechReg for Technical Service Providers to give active/inactive status that is then given to all downstream applications. zRoles does not share information between various systems or applications.

4.2 How is the information transmitted or disclosed?

zRoles information is transmitted via Secure Socket Layer (SSL), Level 1 and Level 2 eAuthentication and Role Base Access Control (RBAC) at the database administrator level.

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.

zRoles information is available internally to zRoles members and entities that are granted permission to access zRoles via eAuthentication.

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?

Section 5.1 is not applicable to the zRoles application. There is no information shared.

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.

Section 5.2 is not applicable to the zRoles application. There is no information shared.

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

Section 5.3 is not applicable to the zRoles application. There is no information shared.

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

Section 5.4 is not applicable to the zRoles application . There is no information shared.

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?

There is no active collection of individual data. Data in zRoles cannot be modified or added. Consequently, a zRoles privacy statement is unnecessary at this time.

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

Section 6.2 is not applicable to the zRoles application. This information is solely based on the rules of the source database.

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

Section 6.3 is not applicable to the zRoles application. This information is solely based on the rules of the source database.

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.

Section 6.4 is not applicable to the zRoles application. This information is solely based on the rules of the source database.

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?

The user information entered in source database is outside this PIA's scope. Refer to USDA-NRCS SORN for further guidance.

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

The user information entered in source database is outside this PIA's scope. Refer to USDA-NRCS SORN for further guidance.

USDA Information Quality guidelines can be accessed at: http://www.ocio.usda.gov/qi_guide/index.html. Data is reviewed and audited by application users and application data stewards, or by application code, data definitions, and validations.

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

Section 7.3 is not applicable to the zRoles application. The source data base administrator is responsible for correcting any information that is fed to the zRoles database.

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

Section 7.4 is not applicable to the zRoles application. Refer to Section 7.1.

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

Section 7.5 is not applicable to the zRoles application. Refer to Section 7.4. Any risks associated to the zRoles application will be addressed via the Security Authorization process.

One possible risk is unauthorized system access through the USDA OCIO eAuthentication system. Access authentication is not an NRCS controlled feature, but a service provided to NRCS Applications by the USDA OCIO eAuthentication system at the Department level for all Applications with personal information. The USDA OCIO eAuthentication PIA is available at http://www.usda.gov/documents/eAUTH_PIA.doc.

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?

The zRoles application is required to have Access Control Policy and Procedures as part of the security Certification and Accreditation package. Access, roles and permissions are determined by the application business function, with all using common supporting systems for user access.

8.2 Will Department contractors have access to the system?

Yes.

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

NRCS ensures every employee, contractor, partner, and volunteer receive 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 a FISMA and USDA policy and is tracked by USDA.

NRCS is also developing Privacy Training which should be administered to NRCS units in the near term.

Non-NRCS entities should also have the above training. However, NRCS should not be held responsible to ensure this training for every third party individual takes place AgLearn onboard and ongoing security training on privacy should be administered before accessing all NRCS applications.

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

No, zRoles is currently undergoing a Security Authorization (SA) this year.

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). Certification and Accreditation, Annual Key Control assessments, and Continuous Monitoring procedures are implemented per law following the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3 located at: ***http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf*** for applications.

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?

Section 8.6 is not applicable to the zRoles application. There is no active collection of information within the zRoles application.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

The zRoles application is an User Role and Access Management System.

The purpose of the zRoles application is to provide a streamlined, single source for the assigning of application roles and scope to NRCS agency employees, affiliates and technical service providers to access NRCS applications.

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

The zRoles application does not use technology that raises minimal if any privacy concerns. zRoles utilize the following technologies which eAuth and source data is transmitted via SSL:

- zRole Front End GUI
- WebBase UI
- Microsoft .NET Framework 4.
- Internet Information Services 7.5
- 2008 Microsoft Windows R2 Enterprise Server
- 2008 SQL Server Enterprise Edition R2 (feeds data to and from other applications via Internet Information Services 7.5)

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"?

Section 10.1 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Section 10.2 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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

Section 10.3 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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

Section 10.4 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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?

Section 10.5 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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

Section 10.6 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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

Section 10.7 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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?

Section 10.8 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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)?

Section 10.9 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

10.10 Does the system use web measurement and customization technology?

Section 10.10 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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?

Section 10.11 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

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.

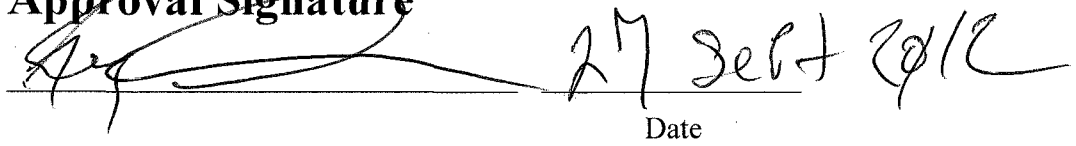
Section 10.12 is not applicable to the ZRoles application. The ZRoles application does not utilize third-party websites or applications.

Responsible Officials

Mr. George Cleek
Director, ITC
United States Dept of Agriculture
Natural Resources Conservation Service
2150 Centre Avenue, Building A
970-295-5540

Gary S. Washington
Chief Information Officer & Director of Information Technology Division
United States Dept of Agriculture
Natural Resources Conservation Service
1400 Independence Ave. SW 20250; Rm. 6233-S
202-205-1442

Approval Signature



27 Sept 2012
Date

Ray Coleman
Senior Official for Privacy
Director of IT Security
United States Dept of Agriculture
Natural Resources Conservation Service
1400 Independence Ave. SW 20250; Rm. 6164-S
202-205-7712

APPENDIX A