Privacy Impact Assessment
zRoles (zRoles)

Policy, E-Government and Fair Information Practices

- Version: 1.4.2
- Date: December 27, 2021
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

zRoles (zRoles)

December 6, 2021

Contact Point

Paul "Ed" Sperling
FPAC zRoles Program Manager
FPAC BC
816-926-2148

Reviewing Official

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

Abstract

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

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 business information on new users added from the source data feeds. The zRoles system also provides the ability for user role and scope assignments by application that is utilized by the specific application. 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.

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

zRoles 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 landowners 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.

The zRoles system provides the ability for user role and scope assignments by application that are utilized by the specific application. The zRoles system is located in the DISC Enterprise Data Center in Kansas City, Missouri. 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).

The zRoles application user accounts are managed NRCS in conjunction by eAuthentication (eAuth). There are two types of users allowed to use the Integrated Accountability Systems (IAS), Employees and four types of affiliates. Each user will be represented in the zRoles database table automatically after registering for of an account. zRoles is not publicly accessible.

Authority to operate was most recently updated on 3/11/2019.

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).

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)
  - Name
  - User data
  - Role and Scope Management
  - Reports

  Categories of Users:
  - NRCS Employees
  - NRCS Affiliates — (i.e., Contractors, TSP, etc...)
  - Landowners using NRCS systems

- zRoles receives PII from the SCIMS database copy (see Section 1.2). The PII that is used and maintained by zRoles includes the names and typical contact information for affected individuals (e.g. Customers, Affiliates and Technical Service Providers), including name and address.
- As reflected on the FSA PIA for Customer Name/Address Systems (CN/AS) Service Center Information Management System (SCIMS), in response to 1.1, the following information is collected, used, disseminated, or maintained:
  - Customer: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation. Name & Address (MF) includes Farm Service Agency employees, farm owners, farm operators, and Technical Service Providers. Additionally business customers can be identified by business entity type (i.e. general partnership, Limited Liability Company, corporation, etc.)
  - Employee: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation

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

- zRoles receives information from NRCS Affiliates databases, feeds from EmpowHR, direct data entry from FPAC user and Webservices that provide data to the zRoles database. Members of the Public do not have access to this application, therefore no data is obtained directly from a non-FPAC user.
- zRoles also receives information from SCIMS. The *Service Center Information Management System* (SCIMS), maintained by FSA, Service Center Information Management System (SCIMS), CSAM ID # 1672, is the database of customer information that is shared by the three Service Center Agencies, FSA, NRCS, and RMA. SCIMS is a repository for USDA business entity and conservation compliance information. This link allows the most current customer information to be printed on forms and letters. It also allows NRCS managers to generate reports on the race, sex, national origin, and disability of program applicants and participants.
- NRCS has access to a copy of the SCIMS database via replication and access to the data from SCIMS for NRCS users is via National Planning and Agreements Database (NPAD) [which resides on PT-FM] and through eAuthentication (eAuth); this route is used because NRCS users do not have direct access to SCIMS. The landowners and general public applicants may provide information to populate SCIMS, which is the source of the PII. All information is obtained through a database copy. zRoles does not modify or update any information in SCIMS.

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

- Information is being collected, used, disseminated, or maintained to provide the ability for user roles and scope assignments by the application that is utilized by individuals with specific, authorized roles respectively

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 given a user account when they enter into EmpowHR, the USDA HR system. EmpowHR is a USDA National Finance Center (NFC) system. EmpowHR has a data feed to USDA's NFC, which in turn sends data to eAuth. eAuth has an automated process to create user accounts for new employees when a record is received from NFC. An automated process (initiated by EmpowHR) will deactivate the zRoles account when an employee is terminated.
- Affiliates register for a level 2 eAuth user account using the self-registration web pages. Once they have the user account, the affiliate should find a Local Registration Authority (LRA) to verify their identity and link the account to an Affiliate record. The affiliate record will have one of these types: 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.

- zRoles collects landowner information, including the names and addresses, using the SCIMS ID of the affected individual and the SCIMS IDs from the SCIMS database copy. NRCS users do not have a direct access to SCIMS. All information is obtained through a database copy.

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 verifies information with USDA oversight.
- The accuracy of PII obtained from SCIMS or other applications not maintained by NRCS is not within the scope of zRoles. zRoles does not have the ability to update any information in SCIMS, nor does it have the ability to update the information in any other application databases not maintained by NRCS.

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

- Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397, the Agricultural Act of 2014 (Pub. L. 113-79), the Agricultural Improvement Act of 2018 (Pub. L. 115-334), and the Coronavirus Aid, Relief, and Economic Security Act (CARES ACT) (Pub. L. 116-136)
- USDA RCPP Program (http://www.grants.gov/view-opportunity.html?oppId=291192)
- The Regional Conservation Partnership Program (RCPP) is authorized by Subtitle I of Title XII of the Food Security Act of 1985 (the 1985 Act), as amended by Section 2401 of the Agricultural Act of 2014 (the 2014 Act). The Secretary of Agriculture has delegated the authority to administer RCPP to the Chief of the Natural Resources Conservation Service (NRCS), who is Vice President of the Commodity Credit Corporation (CCC). NRCS is an agency of the Department of Agriculture (USDA).
- USDA CAET program
- USDA TSP Program: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/programs/technical/tsp/

These regulations pertain:

- 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.

- Privacy risks are minimal as privacy information is inputted only by partners and NRCS government employees that have access to the application. Under our current plan, users

must be authenticated via USDA ICAMs eAuth system and authorized via USDA's role-based authorization

- The minimum amount of personally identifiable information is collected to satisfy the purpose of this system. The risks are mitigated using various control mechanisms, these include:
  - All users must be uniquely identified and authenticated prior to accessing the application.
  - Access to data is restricted.
  - Information is encrypted at rest and in transit.
  - Masking of PII
  - System audit logs are retained and reviewed weekly

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 provides 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.. Further, other NRCS systems utilize zRoles for the assigning of application roles and scope. 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. No new data records are generated. The data is stored within zRoles database and accessed via webservices and through a UI (user interface).
- No additional "tools" (other than the application and database itself) are used to analyze the data.

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.

- Access to the system and data are determined by business need and individual roles. Controls are in place to provide reasonable assurance that data integrity and confidentiality are maintained during processing. Controls in place to ensure the correct handling of information include the following:
  - End users are correctly identified and authenticated according USDA and FSA security policies for access managements, authentication and identification controls.
  - Audit logging is performed at the Department-level to ensure data integrity.

- 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?

The information is retained indefinitely (permanent records).

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

Yes, in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records.

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

- Risks include failure to comply with records management (e.g., NARA guidelines not followed). Risks may also include those related to technical disaster recovery. Human error such as leaked data exists. Hackers may intentionally attempt to break through system security.
- The above risks are mitigated by active zRoles practices to ensure that relevant documentation is maintained to support.
- 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?

- 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 obtains information related to landowners from SCIMS. zRoles does not share or transmit any information to SCIMS, nor does it update any information in SCIMS.
- zRoles does not share information between various systems or applications. Various other NRCS systems utilize zRoles for the assigning of application roles and scope, including: Affiliates, CDSI_NITC, Collaborative Software Development Laboratory (CoLab), Comprehensive Agency Reporting System (CARS), Conservation Practice Data Entry System (CPDES), Conservation Program Delivery System-Integrated Database for Enterprise Analysis (IDEA), Core Services, DamWatch, Digital Record Management System (DRMS), Document Management System (DMS), eDirectives, Emergency Watershed Protection (EWP), Field Office Technical Guide (FOTG), Financial Assistance Tracker (FA Tracker), FPAC DevSecOps Pipeline FPAC Moderate (Pipeline FPAC Mod), FPAC DevSecOps Pipeline NRCS HVA (Pipeline NRCS HVA), FPAC Salesforce, FPAC ServiceNow, FSA Compliance Review , Office Information Profile (OIP), Payment Schedule Application (PSA), Performance Results System (PRS), PhotoGallery, Practice Average Annual Cost (PAAC), Program Operations Information Tracking System (POINTS), ProTracts-FundManager (PT-FM), Receipt for Services (RFS), Resource Stewardship (RS), Review of Open Obligation Tool (ROOT), Steward Management Application (SMA), Technical Service Provider Registry (TechReg), and Water Quality Index (WQI)

4.2 How is the information transmitted or disclosed?

- zRoles information is transmitted via Secure Socket Layer (SSL), Level 1 and Level 2 eAuth and RBAC at the database administrator level.
- NRCS has access to a copy of the SCIMS database via replication. Access to the data is through established security rules via eAuth.

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 zRoles information is available internally to zRoles members and entities that are granted permission to access zRoles via eAuth.
- Any residual risks are mitigated by the controls discussed in Section 2.4 above.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

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

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

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

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.

No. zRoles provides role access information to applications, as a result the NRCS 1 SORN would apply to the records which zRoles users access, but not to zRoles.

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

N/A. zRoles does not collect any information. Therefore, this item would apply to the applications that collected information from individuals, but not to zRoles.

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

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

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

- No. The information in zRoles is based on the rules of the source database.
- Any PII information is obtained from the SCIMS system, which is maintained by FSA. Members of the Public do not have access to this application.

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.

- The information in zRoles is based on the rules of the source database.
- Any PII information is obtained from the SCIMS system, which is maintained by FSA. Also, prior to accessing any system of record, all users are provided a notice prior to logging in via eAuth.

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?

- zRoles provides role access information to applications, not the records which zRoles users access. As a result, zRoles users would contact their administrative point of contact to correct information.

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

- zRoles provides role access information to applications, not the records which zRoles users access. As a result, the procedures to correct inaccurate or erroneous information is for zRoles users to contact their administrative point of contact.

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

- zRoles provides role access information to applications, not the records which zRoles users access. As a result, formal procedures for correcting information are not needed. Instead, zRoles users can directly contact their administrative point of contact.

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.

- zRoles provides role access information to applications, not the records which zRoles users access. As a result, there are no privacy risks associated with the redress unavailable to individuals. zRoles users can directly contact their administrative point of contact.

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

8.2 Will Department contractors have access to the system?

- Yes. Department contractors with a need to know will have access to this application as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements and must obtain Level 2 eAuthentication access
- As part of the FPAC onboarding process, contractors must meet all requirements for access to applications. Through the USDA Rules of Behavior, they are not allowed to download, share, store or print any USDA specific data.
- All roles are approved on a need-to-know basis via FPAC-BC management
- Contractors are required to sign NDAs as per the USDA FPAC BC Onboarding process.

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 receive 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?

- zRoles is a Moderate system
- zRoles initial ATO was granted 1/13/2016
- Current ATO was granted 3/11/2019; this ATO expires on 3/11/2022

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).
  - 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).

  Additionally, these and other safeguards are in place:

  - 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.
  - Audit: Logging is implemented for this application (e.g. by logging infrastructure).
  - Attack Mitigation: The system implements security mechanisms such as input validation.

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?

- Mitigation occurs through policies that address separation of duties (SOD) which ensures that system operators and system administrators have limited, if any, access to PII.
- zRoles does not directly collect any PII from any affected landowner (i.e., member of the public), but zRoles does utilize PII within the system which is obtained from SCIMS, which is maintained by FSA (see Section 1.0 above). Data extracts containing PII are not regularly obtained from the system, therefore, privacy risk from this area is limited and addressed through IT Data Extract processes controls. Any PII information is obtained from the SCIMS database, copied from the SCIMS system, which is maintained by FSA.
- Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5, and by the security controls discussed in Section 2.4 above. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5, respectively.

Section 9.0 Technology

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

9.1 What type of project is the program or system?

- 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, technical service providers, and applicable landowners to access NRCS applications.

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

- No, the zRoles 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, the SO and ISSPM have reviewed M-10-22 and M-10-23. No 3rd party website (hosting) or 3rd party application is being used

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

- Not Applicable - Third party websites / applications are not used.

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

- Not Applicable - Third party websites / applications are not used.

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

- Not Applicable - Third party websites / applications are not used.

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

- Not Applicable - Third party websites / applications are not used.

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

- Not Applicable - Third party websites / applications are not used.

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

- Not Applicable - Third party websites / applications are not used.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

- Not Applicable - Third party websites / applications are not used.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

- Not Applicable - Third party websites / applications are not used.

10.10 Does the system use web measurement and customization technology?

- No, the system does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

- Not Applicable - 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.

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

Appendix A. Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the zRoles system.

Agency Responsible Officials

JENNIFER ZWICKE
Digitally signed by JENNIFER ZWICKE
Date: 2022.01.04 15:44:55 -07'00'

Jennifer Zwicke
FPAC zRoles Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS
Digitally signed by LANITA THOMAS
Date: 2022.01.07 10:31:03 -05'00'

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

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2022.01.07 12:31:26 -06'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture