Privacy Impact Assessment
Collaborative Software Development Laboratory (CoLab) System

Policy, E-Government and Fair Information Practices

- Version: 1.6
- Date: February 20, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department
of Agriculture

Privacy Impact Assessment for the

Collaborative Software Development Laboratory (CoLab) System

February 20, 2020

Contact Point

Ken Kinard
Production and Conservation,
Natural Resources Conservation Service
970-295-5708

Reviewing Official

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

Abstract

This PIA addresses the Collaborative Software Development Laboratory (CoLab) application, which is a system of the Natural Resources Conservation Service (NRCS).

CoLab manages the changes, revisions, upgrades, and modifications that NRCS-ITC applications undergo throughout the software development life cycle (SDLC), by implementing a formal, documented, systematic process for requesting, evaluating, tracking, and approving changes to these applications. CoLab is the Internet-based "Collaborative Software Development Laboratory," which is Intland Software's industry standard Commercial-Off-The-Shelf (COTS) software application based upon the codeBeamer ALM (Application Lifecycle Management) platform.

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) 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

CoLab is the Internet-based “Collaborative Software Development Laboratory” that is Intland Software’s industry standard Commercial-Off-The-Shelf (COTS) software application, based upon the codeBeamer ALM (Application Lifecycle Management) platform. USDA uses CoLab as a solution to improve agility and collaboration in their software development processes. CoLab enables web-based team communication, project management, collaborative code and document management. CoLab also enforces version control for documents, source code and deployment packages.

CoLab manages the changes, revisions, upgrades, and modifications that an application is expected to undergo throughout its life cycle. CoLab implements a formal, documented, systematic process for requesting, evaluating, tracking, and approving changes to NRCS-ITC applications.

CoLab contains a minimal amount of contact information related to CoLab users. This PII is used to establish a user's authorization to CoLab projects by following these transaction steps:

1. User gets a USDA User ID and password.

2. User requests CoLab Membership. USDA eAuth User ID from step 1 is required.

3. User logs in into the CoLab Site.

4. User requests to join CoLab Projects.

5. CoLab Access Managers will authorize the user's access to CoLab projects.

The CoLab system is accessible to NRCS employees and affiliates. When establishing authorization privileges for users to access CoLab, the identity of the person must be known to NRCS via their USDA eAuth User ID. CoLab does not share PII with any other systems.

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?

- Privacy related information is collected and maintained by CoLab in 'profiles' that include the individual's name and work contact information. For some individuals, personal contact information is maintained in their profile.
- Personal Contact Information is comprised of the following elements: o First name
  - Last name
  - Email
  - Phone
  - Company Address
  - Note that CoLab does not "disseminate" any PII.

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

Documents generated as part of Systems Development Life Cycle (SDLC) for any NRCS project

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

See Section 1.1 above

1.4 How is the information collected?

eAuthentication and via access requests

1.5 How will the information be checked for accuracy?

By the user about whom the information was collected

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.

- CoLab does not directly collect any PII from any individual user, but does collect minimal PII with the login/profile set-up, which is obtained from other sources (see Section 1.0 above). Data extracts containing PII are not obtained from the system, therefore, there is no privacy risk from this area.
- 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. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5 respectively.

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.

CoLab uses the PII that was initially obtained from eAuth to establish the user’s profile. CoLab can also be used to update the PII that is maintained for individual users, if they choose to modify their own profile.

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

PII data is not “analyzed” by any tools. No PII data is “produced” by CoLab

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

CoLab 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 Modernization Act of 2014 (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 4 guidance.

- Access Control (AC)
- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- 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 PII information is retained while the application remains in production. Per NARA General Records Schedule 20, this application-specific PII.
- 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.
- Individuals have control of the shelf life for retention. If the user leaves, their account gets disabled.

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 inappropriate release of PII Information related to CoLab user(s). 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?

- CoLab's PII information is not shared with any other internal USDA organizations, noting that CoLab obtains initial PII information from eAuth. An individual needs an eAuth ID to get into CoLab in order to edit the profiles. This is what creates the profiles that are editable.

4.2 How is the information transmitted or disclosed?

CoLab's PII information is not transmitted or disclosed to any 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?

- CoLab's PII information is not shared with organizations external to NRCS.
- CoLab does not transmit any information to eAuth.

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.

CoLab's PII 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?

CoLab's PII information is not shared with organizations external to NRCS

5.4 <u>Privacy Impact Analysis</u>: 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 Does this system require a SORN and if so, please provide SORN name and URL.

- No PII is directly solicited from any individual to support this application, so no "Notice" is provided to individual users. User information is NOT retrieved by a personal identifier.

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

- No PII is directly solicited from any individual to support this application, so no "Notice" is provided to individual users.

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

- Individuals are not required to provide business contact associated information as part of the CoLab application process. No PII information is directly solicited from any individual to support this application.

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

- The only use of the PII in CoLab is to establish the user's profile. While this does not involve the exercising of a "right to consent" on the part of the user, the user can choose to modify their own profile.

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.

- "Notice" does not need to be provided to any individual users by CoLab. There is no risk that an individual would be unaware of "collection," because no PII is solicited from any individual user 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?

- No procedures are required. Individuals have automatic access to their own profiles. Individual users can modify their own profiles by clicking the "Edit" link.

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

- Individuals can correct inaccurate or erroneous information in their own profiles by clicking the "Edit" link.

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

See Section 7.2

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

See Section 7.2

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 for this application. There is no risk that an individual would be unaware of "redress" that is available. While no PIT is solicited from any individual user by this application, users can correct any inaccurate or erroneous information in their own profiles.

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?

- Yes, authorized contractors and partners will have access to the system consistent with their roles and responsibilities. Access to CoLab is controlled through eAuth and Role Based Access Control (RBAC).

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?

- Initial authorization to operate (ATO) was granted in 2013. New ATO is in progress and pending this security artifact.

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 enc1yption). The documents that are passed to and maintained in DMS are enc1ypted in transit.
- Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).
- Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC). Administrative and management operational controls in place to ensure proper access termination.
- Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: Logging is implemented end to end 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?

- CoLab does not directly collect any PII from any individual user, but does collect minimal PII with the login/profile set-up, which is obtained from other sources (see Section 1.0 above). Data extracts containing PII are not obtained from the system, therefore, there is no privacy risk from this area.
- 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?

- CoLab 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?

- 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.

- 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?

- 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?

- 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?

- 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?

- 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?

- 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)?

- 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?

- 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.

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

Agency Responsible Officials

JAKE ZEBELL Digitally signed by JAKE ZEBELL Date: 2020.03.04 07:42:40 -07'00'

Jake Zebell
CoLab Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS Digitally signed by LANITA THOMAS Date: 2020.03.05 13:24:46 -05'00'

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

Department Approval Signature

AMBER ROSS Digitally signed by AMBER ROSS Date: 2020.03.10 11:30:32 -05'00'

Amber Ross
FPAC-BC Privacy Officer
United States Department of Agriculture