Privacy Impact Assessment
RD – General Support Services

- Version: 4.0
- Date: April 25, 2023
- Prepared for: USDA Rural Development (RD)

Privacy Impact Assessment for the RD – General Support Services

April 25, 2023

Contact Point

RDPrivacy@usda.gov
Rural Development, Cyber Security Division
United States Department of Agriculture

Abstract

The Rural Development - General Support System (RD GSS) is the agency's method of modernizing application development to support modern methods of integration, testing, deployments, and agile methods of software deployment. The purpose of GSS is to provide an environment that supports multiple lower environments and facilitates the deployment of tools used for modern application development method. This PIA is required by Section 208 of the E-Government Act of 2002 for RD-GSS because an application within the system, Jira, collects, processes and/or stores Personally Identifiable Information (PII) and the PTA determined that a PIA is needed.

Overview

Rural Development - General Support System (RD GSS) is the agency's method of modernizing application development to support modern methods of integration, testing, deployments, and agile methods of software deployment. The purpose of GSS is to provide an environment that supports multiple lower environments and facilitates the deployment of tools used for modern application development method.

The RD GSS has been designed and tested as the agency's method of modernizing application development to support agile and incremental delivery of RD CIO Application Development. Currently across RD, there is a decentralized method of software development that is aging and does not support modern methods integration, testing, deployments, and agile methods of software deployment. The purpose of GSS is to provide an environment that supports and facilitates the deployment of tools used for modern application development. RD GSS is not publicly accessible.
The General Support Systems environment will host the DevOps and Security Tool Chain which consists of various applications, including Jira. A Privacy Threshold Analysis determined that the Jira application contains PII and requires a Privacy Impact Assessment.

Jira is comprised of Jira Service Desk and Jira Software. Service desk will be the intake method for all RD request to provide structure to RD works and give increased visibility into what different teams are working on. Jira software serve as a planning, tracking, release and reporting tool for security incidents and process tracking for documents and projects. Documents may contain PII.

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?

RD-GSS collects, uses, and maintains PII information to allow for the proper adjudication of security and privacy related incidents through the Jira application. PII include: name, address, date of birth, SSN, RD account numbers, financial data, employment history,

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

Incident reports entered into Jira are typically based on RD loans and grant related documents contain borrower and grantee personal information.

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

The information is collected as part of the investigation process whereby evidence of the breach and type of information exposed is ascertained.

1.4 How is the information collected?

Information is collected from loan and grant applications originally uploaded to the relevant financial systems.

1.5 How will the information be checked for accuracy?

Information collected is checked for accuracy at the initial point of collection.

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

Information collected is allowed under:

• Privacy Act of 1974, 5 U.S.C. § 552a, as amended

• OMB Circular A-130, Managing Information as a Strategic Resource, July 2016

• Federal Information Security Modernization Act of 2014 (44 U.S. Code § 3554 (c)) (requiring agencies to annual report information security incidents, major incidents, and data breaches)

• USDA RD Instruction 2033-A – Records, Management of RD Records

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

The privacy risk is the potential unauthorized disclosure or illegal use of the PII contained in the documents uploaded in RD-GSS. The initial assessment of privacy risk would be performed by the administrators who manage the data at its initial point of collection. Only authorized RD staff and contractors can access RD-GSS with eAuth Level 2 access. GSS is not publicly accessible.

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.

Within the Jira application, documents are uploaded as part of the incident response mitigation process. Jira serves as a document repository and incident related documents are stored in designated ticket assignments (from incident reporting to close out). The information collected is used to determine the incident level of impact.

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

Data is manually analyzed to determine incident response impact level and reporting documentation.

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

Not applicable. RD-GSS 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.

The controls in place to detect unauthorized access to information or applications in RD-GSS include encryption, controlled access, timeout for remote access, and system audit logs. eAuthentication is used to access the GSS applications and there are audit logs of user activity as well.

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?

Records collected in relation to incidents fall under General Records Schedule 3.2, Item 020, DAA-GRS-2013-0006-0002, Temporary Classification, destroyed three (3) years all necessary follow-up actions have been completed, but longer retention is authorized if required for business use.

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

Yes, RD-GSS applications follow data retention as provided by the RD Records Management policy, which is in accordance with NARA.

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

RD-GSS applications, specifically Jira, has the potential risks of unauthorized access, unauthorized disclosure or illegal use of the RD customer PII data.

As described under Section 2.4, security controls are in place to minimize risk.

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 information shared is within RD incident response team for the purpose of incident response mitigation.

4.2 How is the information transmitted or disclosed?

Information is uploaded and viewed on Jira.

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.

The privacy risk to internal information sharing would be the unauthorized disclosure of loan and grant information, including PII and financial data. RD-GSS follows the RD Records Management data retention requirements to manage risk associated with data retention. In addition, access to RD-GSS data is controlled and monitored by designated system administrators.

As described under Section 2.4, security controls are in place to minimize risk.

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

Not applicable, PII information is not shared externally.

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.

Not applicable, PII information is not shared externally.

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

Not applicable, PII information is not shared externally.

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

Not applicable, PII information is not shared externally.

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.

Yes, it follows System of Records USDA/Rural Development-*1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and other participants in RD programs*, Record Access Procedures, published to the Federal Register, 05/14/2019.

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

Yes, under RD-1 SORN Routine Use No. 21.

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

Notice of opportunity and/or right to decline to provide information was provided to individuals by the initial source systems prior to collection or processing of the information.

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

Consent of the individuals for uses of the information would have been obtained by the initial source systems, if required, prior to collection or processing of the information.

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 was provided to individuals by the initial source systems prior to collection or processing of the information. The initial assessment of privacy risk would be performed by the administrators who manage the data at its collection.

Individuals do not have direct access to the system. Notice of the purposes and uses for the collection of the information is provided in the SORN RD-1.

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 general public does not have direct access to RD-GSS; all data is received by USDA personnel from the original source components. In order for a user to gain access to RD-GSS, users must have a level 2 e-authentication account, attempt access RD-GSS from a USDA computer. and must have been added to the application by an RD-GSS administrator who determines what groups and access to which modules they are entitled to receive.

Individuals are notified of the procedure to gain access to their information in the Notification Procedure section as outlined in USDA/RD–*1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and other participants in RD programs*, Record Access Procedures. Individuals may file a records request with Rural Development, Freedom of Information Officer, United States Department of Agriculture, 1400 Independence Avenue SW, Stop 0742, Washington, DC 20250–0742.

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

The general public does not have direct access to RD-GSS; all data is received by USDA personnel from the original source components. See Section 7.1.

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

The general public does not have direct access to RD-GSS; all data is received by USDA personnel from the original source components. See Section 7.1.

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

The general public does not have direct access to RD-GSS; all data is received by USDA personnel from the original source components. See 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.

No additional risks are associated with the redress process. See Section 7.1.

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 general public does not have direct access to RD-GSS. In order for an employee or contractor user to gain access to RD-GSS, users must have a level 2 e-authentication account, attempt access RD-GSS from a USDA computer, and must have been added to the application by an RD-GSS administrator who determines what groups and access to which modules they are entitled to receive.

8.2 Will Department contractors have access to the system?

Yes, only authorized RD contractors with a need to know will have access to RD-GSS applications as part of their regular assigned duties. Contractors follow the same access and authentication procedures that USDA federal employees follow to access RD-GSS as described in Section 8.1.

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

All RD employees and contractors are required to complete annual information security and awareness training, which includes privacy training for RD-GSS related applications.

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

Yes, RD-GSS has an Authorization to Operate (ATO) in effect until January 7, 2023, which is stored in CSAM.

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

RD-GSS complies with the Federal Information Security Modernization Act of 2014 (FISMA) by documenting the Authorization and Accreditation, annual control self-assessments, and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5. These controls, including full compliance, inheritance, and risk acceptance descriptions, are available in USDA Cybersecurity Assessment and Management (CSAM) tool. RD-GSS is hosted on the DISC platform at USDA, which is FedRAMP certified and follows USDA security and privacy requirements.

Access to RD-GSS for authorized USDA personnel is controlled through eAuthentication, and access to sensitive information is controlled through DISC Profiles/Groups on a need-to-know basis with audit logs of user activity for RD-GSS.

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?

See Section 2.4

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?

RD GSS's Jira application software serve as a planning, tracking, release and reporting tool for security incidents and process tracking for documents and projects.

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

No, the project utilized USDA-approved technologies.

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 system owner and ISSPM have reviewed the OMB guidance.

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

Not applicable, RD-GSS does not use third party websites and/or applications.

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

Not applicable, RD-GSS does not use third party websites and/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?

Not applicable, RD-GSS does not use third party websites and/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?

Not applicable, RD-GSS does not use third party websites and/or applications.

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

Not applicable, RD-GSS does not use third party websites and/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?

Not applicable, RD-GSS does not use third party websites and/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?

Not applicable, RD-GSS does not use third party websites and/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)?

Not applicable, RD-GSS does not use third party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

Not applicable, RD-GSS does not use third party websites and/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?

Not applicable, RD-GSS does not use third party websites and/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.

Not applicable, RD-GSS does not use third party websites and/or applications. Not applicable, RD-GSS does not use third party websites and/or applications.

Signature page follows

Approval Signatures

Signed copy kept on record.