Privacy Impact Assessment

CLP Shared Services 4 of 7 – Customer Portal (Customer Portal)

Technology, Planning Architecture, & E-Government

- Version: 1.4
- Date: May 26, 2021
- Prepared for: USDA RD

United States Department of Agriculture

Abstract

Customer Portal is a combination of applications which include, Lender Interactive Network Connection (LINC), Management Interactive Network Connection (MINC), RD Internet, and Service Center Agencies Online Services (SCA Online Services). MINC is the only application that requires a PIA to be completed.

Overview

Lender Interactive Network Connection (LINC) provides a link to public facing web applications used by private industry lenders who participate in the guaranteed loan programs for Rural Development login to the specific site(s) and enter loan closing/administration, application authorization, lender loan information, loss claim administration, loan underwriting data, and loan status reporting. Loan status information can also be provided via electronic data interchange. The data collected is integrated with the Guaranteed Loan System (GLS). The intermediaries enter loan status reports and financial portfolio information on-line into the relending subsystem.

Management Interactive Network Connection (MINC) is an interactive system collecting project budget and tenant residency status information from Management Agencies and service bureaus either through Electronic Data Interchange (EDI) files or direct data entered into the public facing web site. The data collected is integrated into Multiple Family Information System (MFIS).

RD Internet is the public facing web site available to anyone on the internet. RD Internet promotes the mission of the department and tells RD's story, provides a list of programs and services, eligibility for USDA loan programs, RD Home Loan information and account registration and online payments, and connection to the Lender Interactive Network Connection site (LINC). RD Internet is hosted on the USDA Office of Communications (OC) Enterprise Web Application Platform system (eWAPS). The eWAPS system provides FISMA Moderate level hosting, web application development, and cloud services integration through a reusable shared service delivering efficient and reliable website operation. The RD Office of External Affairs is the business owner and manages website operations and content in collaboration with the USDA Office of Communications and OCIO.

Service Center Agencies Online Services (SCA Online Services) is a public facing static web page that lists services provided by RD and the Farm Production and Conservation (FPAC) mission area to include Farm Services Agency (FSA) and Natural Resources Conservation Service (NRCS).

Only those components that collect, process or store PII will be evaluated in this PIA. LINC, RD Internet, and SCAOS will not be evaluated in this PIA.

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?

MINC:
Collect or store PII from:

- The general public
- Other – Management Agents for Multi-Family Property Owners

Data elements:

- Name
- Date and/or place of birth
- Personal identification number (SSN)
- Financial data (Bank Account Numbers)
- Employment History
- Miscellaneous Identification numbers

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

MINC: Tenant information is collected by the Management Agents, using the Form RD 3560-8, and added to MINC; Management Agent information is provided by the Management Agent.

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

MINC: The Customer/Tenant information is used to verify that the correct borrower/management agent is authorized to send/obtain information about the tenants in the project and are authorized to make/receive payments against the RD loan.

The Tenant information is used to verify the eligibility of the tenants to reside in the complex in accordance with the loan agreement for the project as well as produce a monthly project worksheet to calculate the total amount of repayment required for the RD loan by the user.

1.4 How is the information collected?

MINC: Data transmitted in ASCII or .xml File format from Management Agents, by using their own Service Bureaus Vendor Software, independent of the USDA. Software

creates the file that the Management Agent submits by logging into MINC. Management agents could also use the MINC fill-a-form available online in MINC to provide the information directly to MINC.

1.5 How will the information be checked for accuracy?

MINC: Management Agents submit monthly project tenant and budget transactions to MFIS, review transaction status, approve monthly project payment worksheets and debit payments from treasury through MFIS, as well as track when activities or forms are due to the RD Servicing Office overseeing the project. Internal checks by the MINC batch process would check the information for accuracy. Management agents submit budget proposals annually, actual and proposed, which are audited for accuracy. The reports are submitted to an RD specialist to be checked for accuracy and approved.

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

Information in the Customer Portal falls under the following:

- Privacy Act of 1974, as Amended (5 U.S.C. § 552a)
- OMB Circular A-130, Managing Information as a Strategic Resource, July 2016
- Freedom of Information Act, as amended (5 U.S.C. § 552)
- Federal Information Security Modernization Act of 2014 (also known as FISMA), (44 U.S.C. §3551), December 2014
- Consolidated Farm and Rural Development Act (7 U.S.C. §1921, *et. seq*.) and Title V of the Housing Act of 1949 as amended (42 U.S.C. §1471, *et. seq*.)
- Farm Bill 2018 (P.L. 115-334)
- Fair Credit Reporting Act, 15 U.S.C. §1681f
- Consumer Credit Protection Act, 15 U.S.C. §1601*, et. seq.*
- Equal Credit Opportunity Act, 15 U.S.C. §1691, *et. seq*.
- The Fair Debt Collection Practices Act, 15 U.S.C. §162, *et. seq*.
- 7 CFR Part 3550, Direct Single Family Housing Loans and Grants
- 7 CFR Part 3555, Guaranteed Rural Housing Program
- 7 CFR Part 3560, Direct Multi-Family Housing Loans and Grants
- USDA RD Instruction 2033-A – Records, Management of RD Records (updated as of 8-2020)
- NARA General Records Schedules (provides mandatory disposition instructions for records common to several or all Federal agencies)

1.7 <u>Privacy Impact Analysis</u>: 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 this PII and the potential adverse consequences this disclosure or use would have on the RD

customer. Only authorized RD staff can access the Customer Portal applications using eAuth Level 2. These measures mitigate the risks to privacy data in Customer Portal. Applications are located behind the DISC secure midrange infrastructure, which complies with all security and privacy protections required by USDA as a federal agency.

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.

MINC:
Customer Information:

- Management agent: Used to relate project to management agent for processing authorization.
- Borrower (entity): Used to relate project to management agent for processing of payments.
- Borrower debt payment information: Used in creation of Project Worksheet, Payments and Notice of Payment Due report.
- Project housing unit and rent information: Used in creation of Project Worksheet.

Tenant Information:

- Tenant household information including name, date of birth, social security numbers and financial information: Used in creation of Project Worksheet.

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

MINC security environment is fully functional, operational, and effective system. Agency testing and acceptance processes include validating the application security. This systems' platform is Sun Solaris Servers located within the DISC Midrange and consists of an Oracle DBMS executing code created using JBOSS 9.0 tools. A total of 5 screens access the MFIS database. Project worksheet reports contain information on tenants in a project or housing.

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

Not applicable, Customer Portal applications do 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 Customer Portal information include DISC audit logs/security logs and CEC audit logs. There are logs for eAuthentication, which is how the authorized RD staff identify and authenticate to access Customer Portal components.

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?

MINC does not retain application data. MINC is a display and collection system for the data held in MFIS; therefore, does not store or maintain any data unique to the application.

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

MINC does not retain application data. MINC is a display and collection system for the data held in MFIS; therefore, does not store or maintain any data unique to the application.

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

The Risk in minimal, specially data being altered. Since MINC is a display and a collection system for the data held in MFIS; therefore, MINC does not store or maintain any data unique to the application.

MITIGATION: Data integrity controls (DI 1-2) are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered.

Validation controls which refer to tests and evaluations used to determine compliance with security specifications and requirements are in place and it has not been altered. Customer Portal data is protected by DISC, which follow USDA federal agency requirements for data protection. DISC is accredited by FedRAMP.

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?

MINC: Data is sent through MINC to the MFIS system and to PAD, in the eServices system.

Customer Information:

- Management agent: Used to relate project to management agent for processing authorization.
- Borrower: Used to relate project to management agent for processing of payments.
- Borrower debt payment information: Used in creation of Project Worksheet, Payments and Notice of Payment Due report.
- Project housing unit and rent information: Used in creation of Project Worksheet.

Tenant Information:

- Tenant household information including name, social security numbers and financial information: Used in creation of Project Worksheet.

4.2 How is the information transmitted or disclosed?

With MINC, data is transmitted in ASCII or .xml file format, to MFIS and must meet file format specifications and then each transaction is evaluated to meet business rules. Any transactions that are outside the expected values must be accepted by servicing personnel.

Containment control is normally achieved by enforcing host network segmentation to isolate major portions of the host network from a security breach.

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 is the unauthorized access and potential compromise of PII data in the Customer Portal.

This privacy risk is mitigated by the DISC midrange, which hosts the Customer Portal applications and provides security and privacy data protection and complies with USDA requirements on protecting information. Also, only authorized RD staff access the Customer Portal applications using eAuth, so there are audit logs on this activity.

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 data is not shared outside of 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 data is not shared outside of USDA.

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

N/A, PII data is not shared outside of USDA.

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

Privacy risks include the potential compromise of PII and sensitive information. This is mitigated by the security protections, such as firewalls, DNSSec, encryption of data in

transit, and DISC audit logs. Authorized RD staff access LoanServ using ACF2 and RD has continuous monitoring from DISC in compliance with FISMA and as required by RD and USDA. LoanServ data is stored in a secure environment on the DISC platform.

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, under USDA/RD-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs. https://www.govinfo.gov/content/pkg/FR-2019-05-14/pdf/2019-09874.pdf

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

MINC: Yes. Users who log into MINC are provided with a privacy notice prior to collection of data.

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

Individuals have the opportunity and/or right to decline to provide information. With the RD Form 410-9, Statement Required by the Privacy Act, individuals agree to provide the information, so RD customers are aware of the collection of personal information.

MINC: Yes, however, if there is failure to disclose certain information, there will be a delay in processing of eligibility or rejections.

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

MINC: Notification to tenants is on Tenant Certification Document (Form3560-8), individuals have the option to decline to proceed. If the user declines, no data is collected; therefore, there is no risk associated. If the user accepts, then they provide their own data and are aware of the information being collected.

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.

MINC: Notification is on Tenant Certification Document (Form 3560-8), individuals have the option to decline to proceed. If the user declines, no data is collected; therefore, there is no risk associated. If the user accepts, then they provide their own data and are aware of the information being collected.

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?

MINC: Management Agents can see the tenant information held in MFIS via the Project Worksheet once they successfully log onto the application. Tenants do not have access to MINC.

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

Data inaccuracies with Customer Portal applications are managed by USDA employees, who provide workflow management and support to RD customers using MINC. At the time the information is initially processed, changes can be made. The Management Agents would not be able to correct information from previous submissions, however, if the information needed to be adjusted after the transaction was processed, the Management Agent would send in the new transaction with corrected information. USDA employees would check whether the corrections submitted by the Management Agents made changes to the information in MINC, then would issue a project worksheet adjustment.

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

MINC: Online help documents are provided in the application, as well as the contact information for USDA employees.

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

Individuals have access, redress, and amendment rights under the Privacy Act and the Fair Credit Reporting Act.

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

There would be no additional risk associated with the redress process available to users.

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?

Desk Procedures document the User Access Management (UAM) process for establishing, activating, and modifying individual users for Customer Portal. The group and account types are defined by the System Owners for the Customer Portal components. The Information System Point of Contact (ISPOC) assigns group membership and determines individual RD user access. The IT Helpdesk creates, modifies and deletes user requests approved by the System Point of Contact. RD employees and RD contractors access Customer Portal after being provisioned in E-Authentication by a UAM ticket, created by the ISPOC. Steps to provision RD employees and RD contractors follow desk procedures as set by the system owners for Customer Portal components.

MINC: Management Agents must be defined in the MFIS application and associated to at least one project before they register to use MINC. User Access procedures are documented in the Desk Procedures provided by the IT Helpdesk.

8.2 Will Department contractors have access to the system?

Yes, RD contractors are required to undergo the same access and authentication procedures that RD federal employees follow, as discussed in section 8.1.

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

Yes, all RD employees and contractors are required to complete annual information security and awareness training, which includes privacy training.

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

Yes, Customer Portal has an ATO, which is in CSAM

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

The Customer Portal 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, Rev. 4. The Customer Portal applications are hosted on the DISC midrange environment at USDA, which is FedRAMP certified and follow USDA security and privacy requirements.

Access to the Customer Portal applications is granted via eAuth once the IT Helpdesk completes the proper provisioning. Section 5 of this PIA describes security protections in place for Customer Portal data.

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?

Since Customer Portal is used by authorized RD staff using eAuthentication and there are group access management controls, the privacy risks are minimal. Potential compromise of privacy data is mitigated by DISC audit event monitoring and USDA network security protections in place to protect RD data for Customer Portal components.

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?

MINC: Web-based solution using .ASP and .NET objects on Microsoft IIS servers.

For all technologies chosen by RD, an Analysis of Alternatives (AoA) is completed to determine which technologies will be selected and ultimately purchased or built.

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 for Customer Portal, 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 system owner and the ISSPM have reviewed the OMB memorandums.

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

Not applicable, Customer Portal does not use 3rd 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, Customer Portal do not use 3rd 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, Customer Portal do not use 3rd 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, Customer Portal do not use 3rd 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, Customer Portal do not use 3rd 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, Customer Portal do not use 3rd 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, Customer Portal do not use 3rd 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, Customer Portal do not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

N/A, web measurement and customization technology are not used.

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

N/A, web measurement and customization technology are not used.

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, Customer Portal do not use 3rd party websites and/or applications.

Agency Responsible Officials

ANGELA COLE

Digitally signed by ANGELA COLE
Date: 2021.05.26 11:21:01 -04'00'

Angela Cole
Information Systems Security Program Manager (ISSPM)
USDA Rural Development

Agency Approval Signature

KELLI PETRIE

Digitally signed by KELLI PETRIE
Date: 2021.05.27 15:18:09 -04'00'

Kelli Petrie
Information System Owner
USDA Rural Development