Privacy Impact Assessment

Customer Portal

Rural Development (RD)

- Date: July 11, 2016
- Prepared for: RD

United States Department of Agriculture

Abstract

Customer Portal is a combination of applications which include, Lender Interactive Network Connection (LINC), and Management Interactive Network Connection (MINC) (both have internal functionality), RD Internet, Service Center Agencies Online Services (SCA Online Services) and MyRD.

Lender Interactive Network Connection (LINC) are public facing web applications used by private industry lenders who participate in the guaranteed loan programs for Rural Development (RD) and Farm Service Agency (FSA) and by intermediaries who participate in the RD Intermediary Relending Program.

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 enter into the public facing web site website.

RD Internet is the public facing web site available to anyone on the internet promoting the mission of the RD site.

Service Center Agencies Online Services (SCA Online Services) is a public facing static web page that lists services provided by Farm Services Agency (FSA), Natural Resources Conservation Service (NRCS) and RD.

MyRD (in dev) authenticated, external customers provide known account information to register the application. Upon successful registration, customers are presented with a user interface allowing them to browse account information.

Overview

LINC: lenders 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 (EDI). The data collected is integrated with the Guaranteed Loan System (GLS). However, once a user attempts to go past the main page, the access rights into these links is restricted by the AASM security module. AASM is a module under Security Management in the Official Systems Inventory. https://usdalinc.sc.egov.usda.gov

MINC provides a web based access system for the RD borrowers managing rural rental housing and farm labor housing projects funded by the Rural Housing Service. It allows Management Agencies to transmit EDI files of project budgets, payments, and tenant transactions directly to MFIS from files created on their own management software via MINC or through the MINC application Fill-A-Form function 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.

RD Internet promotes the mission of the department, 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

SCA Online Services managers of the application access AppDocs using .NET secure socket layer to access: http://www.sc.egov.usda.gov

MyRD (in dev): External customers require a Level 2 eAuthentication (eAuth) Identification (ID) to provide known account identification information.

NOTE

Per the PTA, LINC and SCA Online Services do not require a PIA and will not be included in the remainder of the document.

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 has two forms of information consisting of Customer Information and Tenant Information:

Customer Information: Management agent, borrower and key member names and social security numbers. Borrower debt payment information. Project housing unit and rent information.

Tenant Information: Tenant household information including name, social security numbers and financial information.

MyRD

- Non-persistent items used to register account
  - Loan account or borrower Identification (ID)
  - Last 4 digits of Social Security Number (SSN) / Tax Identification Number (TIN)
  - Bank routing number (RUS) only
- Item used to persist account registration
  - Loan account or borrower ID
  - Internal eAuthentication ID (eAuth ID)

RD Internet static web pages containing popular topics, programs and services, latest news releases, publications, USDA RD contact information, lender portal, home loan servicing

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

MINC:

Customer Information: Management agent, borrower and key members

Tenant Information: The tenant applying to reside in the units of the project.

MyRD: User form input for items used to register the account and eAuth header is source of internal eAuth ID.

RD Internet: Section 207(f)(2) of the E-Government Act of 2002 requires federal agencies to develop an inventory of information to be published on their Web sites, establish a schedule for publishing information, make those schedules available for public comment, and post the schedules and priorities on the Web site.

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

MINC: The information collect is stored in the MFIS application. The Customer 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.

MyRD: The information is collected to associate a borrower user with accounts for which they have account information and to retrieve the selected loan account details from the appropriate servicing system using read only permissions, via web services.

RD Internet: The information is collected to keep the general public informed about USDA programs and services.

1.4 How is the information collected?

MINC: Data transmitted in ASCII or .xml File format from Management Agents/Service Bureaus Vendor Software.

MyRD: The information is collected from the user via a web based form and from the http header information appended to the web session by the eAuthentication (eAuth) system when the user authenticates.

RD Internet: Information is not collected.

1.5 How will the information be checked for accuracy?

MINC: The data is reviewed verified to fit business rules via a batch process in MFIS. If any errors are generated the information is rejected. If business rules are within a specific margin of error, then they are held for review by the Customer Servicing Center (CSC) specialist for tenant information or area specialists for budgetary information.

MyRD: The information is checked for accuracy against data in CSC.

RD Internet: No data is collected.

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

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.).

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

Risk: Minimal.

Mitigation: Applications are located behind the NITC secure midrange infrastructure. See the System Security Plan (SSP) security controls: Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM). These applications are behind eAuthentication (eAuth) with a Level 2 access authority. Users of the system are required to complete annual privacy act training to ensure the proper handling of privacy data.

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: 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.

MyRD:

- Loan account or borrower ID, last 4 digits of SSN/TIN, and bank routing number (for RUS only) are used to retrieve account information from servicing systems using read only permissions, via web services.
- The loan account or borrower ID and the internal eAuth ID persisted to retain association of the account to the user id that registered to view account data.
- Data that is retrieved from the servicing systems is displayed on web pages.

RD Internet: No data is collected.

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

MINC:

Data transmitted in ASCII or .xml file format must meet file format specifications and then each transaction is evaluated to meet business rules and USDA Regulations. Any transactions outside the expected values must be accepted by servicing personnel.

Management Agents validate tenant data prior to approval of project worksheets.

MyRD: No analysis of data is performed.

RD Internet: No data is collected

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

MINC and **MyRD** do not use any commercial or publicly available data

RD Internet: No data collected

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 National Institute of Standards and Technology (NIST) 800-53A controls for the Shared Services system are discussed in detail in the System Security Plan and specifically the Access Controls (AC 1-8, 12, 14, 17, 19-22). Identification and Authentication (IA 1-

7) controls are in place to prevent unauthorized access restricting users from accessing the operating system, other applications or other system resources not needed in the performance of their duties and is restricted by eAuth User Identification (User ID). Authority and Purpose (AP) compensating control gives explanation of why PII is allowed on the system. Systems and Communication Protection (SC 1, 2, 4, 5, 7, 8, 10, 12, 13, 17, 18, 20-23, 28, 39) controls are in place to prevent unauthorized access.

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 and **MyRD** do 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.

RD Internet: Information is not collected.

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

MINC or **MyRD** do 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.

RD Internet: Information is not collected.

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

MINC, **MyRD** and **RD Internet** do not retain application data.

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?

MY RD: Provides accounting system of record and official reporting mechanism to CLSS and PLAS.

LINC: Portal for AASM and GLS.

MINC: Data may be sent through MINC to the MFIS system; however, data is not shared from MINC to vendor software.

RD Internet: Data is not shared

4.2 How is the information transmitted or disclosed?

Data transmitted in ASCII or .xml file format must meet file format specifications and then each transaction is evaluated to meet business rules and USDA Regulations. Any transactions outside the expected values must be accepted by servicing personnel.

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.

Risk: Minimal

Mitigation:

The security and control of PII is the responsibility of the System Owner and RD employees.

NIST 800-53 security controls are place and are discussed in the System Security Plan (SSP). System and Communication (SC) controls provide integrity and confidentiality.

Interconnection Service Agreement (ISA) and Memorandum of Understanding (MOU) agreements are in Cyber Security Assessment and Management (CSAM) and maintained by the Information Systems Security Staff (ISSS).

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?

MINC, MyRD: N/A

RD Internet: public facing website – information is available to the general public

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.

MINC, MyRD and **RD Internet:** N/A

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

MINC, MyRD and **RD Internet:** N/A

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

MINC, MyRD and **RD Internet:** N/A

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.

MINC and MyRD: Yes, https://www.federalregister.gov/articles/2016/04/28/2016-09938/privacy-act-of-1974-system-of-records-usdarural-development-1-current-or-prospective-producers-or

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

MINC: Yes. Notification is on all specialized USDA Forms used to collect the data which must be signed by the individual providing the data.

MyRD: Yes, on the Welcome page and Privacy Policy link on the website.

RD Internet: NA

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

MINC: Yes, however, if there is failure to disclose certain information, there will be a delay in processing of eligibility or rejections. RHS will not deny eligibility if there is refusal to disclosure the social security number (SSN).

MyRD: N/A

RD Internet: NA

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 is on Tenant Certification Document (Form3560-8), Rental Assistance Agreement (Form RD 3560-77)

MyRD: N/A

RD Internet: NA

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.

N/A – refer to SORN RD1 for the RD systems of record

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.

MyRD: External customers authenticate to the system with a level 2 eAuth id and provide known account identification information including the SSN/TIN, account number, and banking information to register to the application. Upon successful registration customers are presented with a user interface that allows them to browse account information.

RD Internet: NA – public website

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

MINC: Send in one of 34 transactions that allow modification of the data or contact CSC for assistance with modification of data.

MyRD: Procedures for fixing incorrect data is the responsibility of the servicing offices: CSC for Single Family Housing and NFAOC for RUS.

RD Internet: NA **–** public website

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

MINC: Online Help documents as well as contact information is provided in the application.

MyRD: Information Quality link on the website.

RD Internet: NA **–** public website

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

MINC: Contact the CSC Help Desk for questions.

MyRD: A Contact tab and FAQ page is provided in the application.

Persons who wish to file a Request for Reconsideration should submit the request by letter, fax, or e-mail to the Reconsideration Official identified in the final determination of the request for correction that the requestor receives from USDA. For requests for reconsideration that involve *influential* scientific, financial, or statistical information, or regulatory information, USDA will designate a panel of officials to perform this function. Typically, such a panel would include a Reconsideration Official from the USDA agency that made the initial determination and two from other USDA agencies.

Persons requesting reconsideration should submit written material to support their case for reconsideration, as well as a copy of the information originally submitted to support the request for correction and a copy of USDA's response. Requests for Reconsideration must be filed with the appropriate designated Reconsideration Official (postmarked, shipped by an overnight delivery service, faxed, or sent by e-mail) within 45 days after the date that the USDA agency transmitted its decision on the original request for correction. Requests for Reconsideration that are filed after the 45-day deadline may be denied as untimely.

RD Internet: NA – public website

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

MINC: N/A. This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application.

MyRD: Customer redress options are provided by Agency staff in accordance with Agency procedures.

RD Internet: N/A

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?

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 to User Access Management (UAM) Team.

MyRD: Customers are required to authenticate to the system with a level 2 eAuth ID. Level 2 eAuth ID's require identity proofing. The customer must also provide known account and customer information.

Generally, the National Institute of Standards and Technology (NIST) 800-53controls for the Shared Services system are discussed in detail in the System Security Plan and specifically the Access Control (AC), Identification and Authentication (IA) and Systems and Communication Protection (SC) controls are in place to prevent unauthorized access. Access control is also addressed in the individual systems desk procedures.

RD Internet: Is an open public facing site that provides citizens with information, contacts and links to various RD programs.

8.2 Will Department contractors have access to the system?

Yes, Contractors will have access to the application.

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

The NIST 800-53 controls for the Shared Services system are discussed in detail in the System Security Plan and specifically the Information Security Awareness and Training (ISAT) controls are in place to provide privacy training. USDA RD requires annual ISAT for all employees and contractors

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

Yes

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

The NIST 800-53 controls for the Shared Services system are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls are in place to prevent misuse of data.

RD has an Application Auditing and Monitoring Policy in place that defines the following auditable events: server startup and shutdown, loading and unloading of services, installation and removal of software, system alerts and error messages, user logon and logoff attempts (both successful and unsuccessful), granting of elevated privileges (root access success and failure), modifications of privileges and access controls, all root commands (success and failure), and sensitive files accessed, modified and added. These controls, including full compliance, inheritance and risk acceptance descriptions, are available in CSAM.

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?

Risk is mitigated by collecting auditable events: date and time of the event, the component of the information system where the event occurred, type of event, user/subject identity, and the outcome (success or failure) of the event.

The NIST 800-53 controls for the Shared Services system are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls are in place to prevent misuse of data. At a minimum, the following information will be collected for each of the auditable events: date and time of the event, the component of the information system where the event occurred, type of event, user/subject identity, and the outcome (success or failure) of the event.

Audit logs will be reviewed by security personnel every two weeks and suspicious activity will be investigated. Suspicious activity includes, but not limited to: modifications or granting of privileges and access controls without proper request submitted, consecutive

unsuccessful log-on attempts that result in a user being locked, multiple unsuccessful log-on attempts without lock out by the same User Identification (UserID), modifications or attempted modification of sensitive files without authorization and within the applications repeated attempts to access data outside a user's privilege.

Per the General Records Schedule 20, Section 1C, the following items will be deleted/destroyed when the agency determines they are no longer needed for administrative, legal audit or other operational purposes: electronic files and hard copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files and cost-back files used to assess charges for system usage.

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.

MyRD: Web-based solution using DRUPAL content management solution.

RD Internet: web-based solution

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

No

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"?

Third party websites are not used.

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

Third party websites 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 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 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 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 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 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 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 are not used.

10.10 Does the system use web measurement and customization technology?

Third party websites 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?

Third party websites 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.

Third party websites are not used.

Responsible Officials

MICHAEL SUTTON

Digitally signed by MICHAEL SUTTON
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=MICHAEL SUTTON, 0.9.2342.19200300.100.1.1=12001000317363

Date: 2016.11.15 15:17:10 -06'00'

Michael Sutton
Chief, Enterprise Technology Branch

TAMARA ORLET

Digitally signed by TAMARA ORLET
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=TAMARA ORLET, 0.9.2342.19200300.100.1.1=12001001543736

Date: 2016.11.16 06:14:39 -06'00'

Tamara Orlet
Chief, Management Services Technology Branch

Approval Signature:

EUGENE TEXTER

Digitally signed by EUGENE TEXTER
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=EUGENE TEXTER, 0.9.2342.19200300.100.1.1=12001000317346

Date: 2016.11.16 11:46:11 -06'00'

Diego Maldonado
Information Systems Security Program Manager