Privacy Impact Assessment

Multi-Family Integrated System (MFIS)

Rural Development (RD)

- Date: August 2017
- Prepared for: RD

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	Sept 2014	JK	CLP Servicing conversion
1.1	Feb 2015	JK	Update to Add MFH Mobile Application references
1.2	July 2016	TGW	Annual Review/Roll up module into parent
1.3	August 2017	TGW	Annual Review

Abstract

MFIS was designed to assist Servicing Office personnel in monitoring the management of the Multi-Family Management program. It is an intranet application that provides the capabilities to track all of the activities related to the management and servicing of the Multi-Family Housing (MFH) property. MFIS Mobile App is an extension of MFIS used by field personnel to gather data for USDA properties electronically transferring data into the MFIS application. In addition, it provides budget tracking and analysis processes and computes the monthly project payment. Pre-Trac is an intranet-ready oracle database support system that allows the user to process Multi-Family Housing Prepayment requests in accordance with RD Instructions 1965-E.

Overview

(MFIS) is designed to assist Servicing Office personnel in monitoring the management of Multi-Family rental properties. MFIS is an intranet application that provides the capabilities to track all of the activities related to the management and servicing of the MFH property.

MOBILE APP is an extension of MFIS executing on iPad devices. The application allows users to gather data during an intensive visit to USDA properties and then electronically transfer that data to the MFIS application.

PRE-TRAC is an intranet-ready database support system that allows the user to process Multi-Family Housing Prepayment requests in accordance with RD Instructions 1965-E. The application assists the servicing office to track those projects requesting prepayment of their loan and determines if the project is needed.

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?

Customer Information: Management agent, borrower and key member names and tax identification numbers, borrower debt payment information and project housing unit and rent information.

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

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

Customer Information: Management agent, Service Bureaus, Borrower and Key members

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

Project Information: Tracking activities and effort, Units, Rents.
Inspection Information: Physical Inspection, Management Review and Tenant Review.

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

Customer Information is collected to record the borrower and management agents associated to a project as well as communicate project information between the AMAS, MINC, PAD and MFH Rentals applications.

Tenant information is collected via MINC and CSC 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.

Project Information is collected to track the viability of the project and to confirm that all required documentation and reporting as defined in the RD Housing Handbooks are completed or corrected as specified.

Inspection Information is collected to record and validate Physical Inspection, Management and Tenant data.

1.4 How is the information collected?

Web application executing on a Windows environment, to Linux, to Sun Solaris box containing Oracle DBMS executing java code.

Mobile applications executing on an Apple iPad iOS environment, to Linux, to Sun Solaris box containing Oracle DBMS executing java code.

1.5 How will the information be checked for accuracy?

Data transmitted as ASCII or HTML files 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.

Servicing offices enter project tracking information and physical inspection data and validate the interaction of these activities via MFIS Reports.

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: Is associated with customer information: Management agent, borrower and key member names and tax identification numbers, borrower debt payment information and project housing unit and rent information. Tenant Information: Tenant household information including name, social security numbers and financial information. The risk is in the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the client.

MITIGATION: Data is stored in a secure environment behind the NITC secure mainframe 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).

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.

Customer Information:

Management Agent Information: Used to relate the project to a management agent. Relationship controls access to MINC, Verification of data transmitted to authorized project, communication back to Management Agent about transactions received, authorization of online repayment of RD Loan.

Borrower and Key Member Information: Used to confirm loan status of project, IOI issues, and provide communication to borrower about any issue found at project that does not meet USDA regulations.

Borrower debt payment information: Used to build project worksheet that calculated the repayment of the USDA loan, pre-authorized debiting of bank account for calculated payment or check disbursement of RA assistance.

Project housing unit and rent information: Used to build project worksheet that calculates the repayment of the USDA loans.

Physical Inspection Information: Used to build MFIS report FRM2100 Physical Inspection (Mobile). This report contains all the forms necessary to perform the physical inspection part of a project management review. The forms are used to record findings and comments when conducting a physical inspection, and include forms for Desk/Management Review, Tenant Review, and Physical Inspection. The Physical Inspection form includes separate sections for Form RD 3560-11, Multi-Family Housing Physical Inspection and Tenant Interview forms.

Tenant Information:

Tenant household information including name, social security numbers and financial information: Used to verify eligibility of tenant household for rental assistance as well as used to build project worksheet that calculates the repayment of the USDA loan.

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

Data transmitted as ASCII or HTML files must meet file format specifications and then each transaction is evaluated to meet business rules and USDA Regulations.

50+ reports are used by servicing office to confirm project information maintained.

Online screen edits confirm integrity of business rules as well as date and numeric fields.

Analysis reports and online processes confirm consistency and completeness of data held about a project.

Online reports balance financial information regarding project worksheets accepted by management agents and other payment activities recorded in MFIS prior/after transmission to AMAS for payment processing.

Prepayment status reports and timeline reports are completed to confirm that prepayment regulations/requirements are met by the servicing office and the borrower.

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

N/A.

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) 800-53 controls for MFIS are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1-8, 12, 14, 17), 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 Active Directory (AD) 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, 20-23, 28, and 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?

The MFIS system stores 5 years (or last 3 items) for annual data. Non-annual data has infinite retention; Pre-Trac data has infinite retention

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

System of Record (SOR) was completed and submitted to NARA in accordance with Section 207(e) of the E-Government Act of 2002 [44 U.S.C. 3601] and NARA Bulletins 2008-03, Scheduling Existing Electronic Records, and 2006-02, NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002.

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

RISK: The MFIS system stores 5 years (or last 3 items) for annual data. Non-annual data has infinite retention; Pre-Trac data has infinite retention. With data stored for this length of time there is the potential of unauthorized access, unauthorized disclosure or illegal use of the customer PII data.

MITIGATION: Once data is no longer needed, it is properly destroyed. Methods such as overwriting the entire media, degausses, and disk formatting are used, but strict attention is paid to whatever process is selected to ensure that all unneeded data is completely destroyed. Papers and other soft materials, such as microfiche and CD's, are shredded. Also, the data is stored in a secure environment behind the NITC secure mainframe 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).

.

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?

PAD is an interface between USDA and US Treasury department to ensure timely transfer of funds from borrowers. MFH and PLAS borrowers that mail paper checks to RD for the installment payments may register for PAD transactions. When a borrower registers for PAD, his payment is made via EFT from his bank account or his designated management agent's bank account through an Automated Clearing House (ACH) to Rural Development. Authorized Rural Development personnel in MFH Servicing Offices and Finance Offices, Cash Management Branch use EFT. This application operates on a Linux Apache web server and a Tomcat Server container and connects to a DB2 database hosted on HP-UX servers.

The application is accessed at *https://mfh.sc.egov.usda.gov*.

Inter-system Dependencies

- AMAS (receive) nightly downloads of project and borrower information
- CLSS Link to the MFIS Tenant Tracked Account screen that links to the CLSS application
- AMP – (receive) printer for statements and tax forms
- BI (TDW) –receives data for reports
- MINC (receive) tenant, budget and collected project payment data
- MINC (send) project worksheets, tenant, budget, and payment status
- EFT/PAD (send) hourly feed of collected project payments
- MFH Rentals (send) project location and management information
- PLAS – Accounting systems providing transaction processing.

4.2 How is the information transmitted or disclosed?

Data entry screens are completed via the web by RD Area Specialists for borrowers who do not participate through MINC. Batch feeds are obtained nightly from the AMAS mainframe system for borrower and project detail information.

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: The risk to internal information sharing would be the unauthorized disclosure of lender status and loan closing reports, budget and payment status, statement and tax report information, borrower information and accounting information.

MITIGATION: The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality. The security and control of PII is the responsibility of the System Owner and RD employees. Risk is mitigated with the implementation of RD ISSS NIST policies, standards and procedures. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure.

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?

MFIS:

US Bank - Provides lockbox services for the Application's direct single family housing loan customers.

HUD/REAC – Physical inspection information collected is shared between systems

New York State Housing Trust Fund Corporation (HTFC - provides information contained in Form RD 3560-08 for monthly HTFC reporting.

Pre-Trac - There are numerous non-profit organizations that are listed in the monthly security verification report

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.

MFIS- No PII data is shared outside the department.

Pre-Trac- Yes, SORN USDA/Rural Development-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs.

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

MFIS and Pre-Trac communication resources consist of T1 data lines connecting the field offices, the National Office in Washington, D.C. and Rural Development offices in St. Louis, MO, to the National Information Technology Center (NITC) in Kansas City. The USDA Wide Area Network with frame relay capability is used.

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

RISK: The risk to external information sharing would be the unauthorized disclosure of lender status and loan closing reports, budget and payment status, statement and tax report information, borrower information and accounting information.

MITIGATION: Data is sent via VPN and a signed Interconnection Service Agreement are in place in CSAM and maintained by the ISSS. The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality. The security and control of PII is the responsibility of the System Owner and RD employees. Risk is mitigated with the implementation of RD ISSS NIST policies, standards and procedures. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure.

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, USDA/Rural Development-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs.

http://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records

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

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

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

Yes, but notice indicates that "failure" to disclose certain information may delay the processing of your eligibility or rejections. RHS will not deny eligibility if you refuse to disclose your Social Security Number."

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

No.

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.

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

Individual do not have direct access to the system as users. Individuals have the option to decline to proceed. If the user declines, no data is collected; therefore, no risk is associated. If the user accepts, 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?

Requests for the information are presented in writing to CSC or the Servicing Offices. Reports are then generated and returned to the individual requesting the information after verification that the requestor has authority to access that information.

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

The data is reviewed by area specialists, CSC and Management Agent. If data can be modified via MINC, transactions are sent in to make the modification. Otherwise changes are made via the online system once official change requests are received by the Area Specialist or CSC. Audit records are stored in the database recording who entered the change into the MFIS application. Notifications are sent back to the requestor or viewed and approved via the project worksheet by the management agent.

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

MFIS- Contact the CSC Help Desk for questions or contact the area servicing office handling the project.

Pre-Trac- Contact the Servicing Office processing the Prepayment Request.

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

Contact the CSC Help Desk for questions or contact the area servicing office handling the project. Also, individuals have access, redress, and amendment rights under the Privacy Act and the Freedom of Information Act.

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. Individuals or management agents contact the CSC Help Desk or servicing office handling the project to request changes to their information.

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?

SAAR requests are submitted by management to request access to the application and to establish the RD user's authority in the system. SAAR requests are entered by UAMT. Appropriate users lists are on file.

8.2 Will Department contractors have access to the system?

Contractors will only have 'READ ONLY' access to any production system.

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

USDA RD requires annual Information Security and Awareness training for all employees and contractors. RD is responsible for ensuring all new employees and contractors have taken the Department Security Awareness Training as developed by OCIO-Cyber Security (CS). Training must be completed with a passing score prior to access to a USDA RD System.

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

Yes, the current ATO is valid until 28 February 2020.

8.5 What auditing measures and technical safeguards 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 Cyber Security Assessment and Management (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: There is minimal risk given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system,.

MITIGATION: However, RD has the following controls in place - 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. Audit logs will be reviewed by the NITC Security Division 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?

The MFIS system is primarily an online web application system. Which is comprised of 300 + ASP pages which are contained on a Windows 2008 server running IIS.

The MFIS system software executes Java coded services on a Linux server to access data in an Oracle DBMS on a Sun Solaris server. MFIS also includes 58 pages which enable users to execute a total of 58 Oracle Reports. The reports are created on the fly utilizing Oracle BI Publisher using stored procedures to process report requests. Multiple development tools were needed to create these pages but Visual Studio 2010,JBoss Developer Studio 9, ORACLE 11g DBMS with SQL*Plus 8.1.7 and PL/SQL 8.1.7 as the brick and cornerstone applications.

The web architecture includes ASP and .NET objects on Microsoft IIS servers that communicate with java web services deployed on Linux servers that access an Oracle 11G database on a Sun Solaris server. It also uses J2EE on Apache Linux web servers, Tomcat application servers, accessing data in a DB2 Database on a Linux server. The Agency utilizes multiple tools in the development of Agency financial and management systems. Erwin is currently being used to model and generate DB2 and Oracle databases for the Multi-Family Housing suite of applications. Microsoft Visual Studio 2010 and JBoss Developer Studio are being used for the development and maintenance of the MFH applications. PTC Integrity (formerly MKS Integrity) is used for configuration management and version control.

The Mobile Apps are an electronic version of the Physical Inspection, Management Review and Tenant File review forms on the iOS iPad devices. Minimum data is downloaded to the device to allow servicing offices to fill out a questionnaire when verifying project and tenant data previously sent to RD by the Management Agent. The mobile apps interface to the MFIS ORACLE 11g database using a web service that was developed in Java and runs on Tomcat application server. The mobile apps were developed in Objective-C using the XCode IDE.

The PRE-TRAC system's web interface is a Linux Apache Web server accessing objects on an Oracle WebLogic server. After user has been authenticated to eAuth users request are retrieved from an Oracle 11G database on Sun Solaris server. The application is accessed at https://pretrac.sc.egov.usda.gov/pretrac/. The database is copied to the PIX database on a

nightly basis via a CTRL-MControlled U backup job. Copying of the database from the original location to PIX is required for PIX to access the same data for prepayment requests by nonprofit organizations.

The web architecture includes ASP and .NET objects on Microsoft IIS servers that communicate with java web services deployed on Linux servers that access an Oracle 11G database on a Sun Solaris server. It also uses J2EE on Apache Linux web servers, Tomcat application servers, accessing data in a DB2 Database on a Linux server. The Agency utilizes multiple tools in the development of Agency financial and management systems. Erwin is currently being used to model and generate DB2 and Oracle databases for the Multi-Family Housing suite of applications. Microsoft Visual Studio 2010 and JBOSS Developer Studio are being used for the development and maintenance of the MFH applications. PTC(MKS) is used for configuration management and version control.

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

No, MFIS or Pre-Trac does not employ technologies which would 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 guidance was reviewed, however, the system does not use 3rd party websites and/or applications.

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

MFIS nor Pre-Trac do 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.

MFIS nor Pre-Trac 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?

MFIS nor Pre-Trac 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?

MFIS nor Pre-Trac 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?

MFIS nor Pre-Trac 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?

MFIS nor Pre-Trac 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?

MFIS nor Pre-Trac 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)?

MFIS nor Pre-Trac do not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

MFIS nor Pre-Trac do 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?

MFIS nor Pre-Trac do not use web measurement and customization technology.

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.

MFIS nor Pre-Trac do not use 3rd party websites and/or applications.

Responsible Officials

TAMARA ORLET Digitally signed by TAMARA ORLET
Date: 2017.10.11 07:53:27 -05'00'

Tamara Orlet
Chief, Management Services Technologies Branch

Approval Signature

signed for

EUGENE TEXTER Digitally signed by EUGENE TEXTER
Date: 2017.10.06 11:22:31 -05'00'

Diego Maldonado
Rural Development Privacy Officer