Privacy Impact Assessment

Automated Multi-Family Housing Accounting System (AMAS)

Rural Development (RD)

- August 24, 2017
- Prepared for: RD

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Auth**	**Comments**
1.0	07/15/16	ISSS/TW	Transition to new template
1.1	04/12/17	ISSS/TW	Update to include connection to US Treasury
1.2	8/24/2017	ISSS/JMK	FY18 review; added AMP interconnection

Abstract

The Automated Multi-Family Account System (AMAS) is an online transaction entry and inquiry financial and accounting system accessed by over 270 field offices, National Office, Centralized Service Center (CSC) and the National Finance and Accounting Operations Center (NFAOC). It is a loan and grant origination system that provides tracking and servicing capabilities for these MFH loans and grants. Updates are done nightly in a batch mode. AMAS supports the Multi-Family Housing direct loan and grant program. It provides loan making and servicing capabilities for 23,000 loans.

Major features include loan closing and servicing including calculating and applying rental assistance and cash application, general ledger and financial reporting.

Overview

AMAS is hosted by NITC Mainframe in Kansas City, MO. AMAS uses Access Control Facility 2 (ACF2) as the core user authentication and authorization system. The system is designed to positively identify and authenticate the identity of users prior to granting the appropriate system accesses based on the user's pre-defined access level.

The Electronic Fund Transfer (EFT) system is an interface between USDA and US Treasury department to ensure timely transfer of funds from borrowers through the Automated Multi-Housing Accounting System (AMAS).

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?

The following information is collected: Client names, borrower's / co-borrower's social security numbers, key member's addresses, and business financial data, debt payment information, voucher recipient name, voucher payment borrower name, and monthly voucher amount.

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

The sources include: RD, FSA loan officers, trusted lenders, monthly banking data file from Treasury via NITC.

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

AMAS is an online transaction entry and inquiry financial and accounting system accessed by over 270 field offices, National Office, and Finance Office of Rural Housing. The National Office is the primary user of AMAS and the Finance Office has overall operational, financial, and accounting responsibility for Rural Development. Approximately 1 million transactions are processed through the system annually. External users may include Freedom of Information Act (FOIA) requests, General Accounting Office (GAO) requests, Office of Inspector General (OIG) requests, Office of Management and Budget (OMB) requests, and Congressional requests.

AMAS functions include: Online appropriation accounting; Online inquiry and transaction input; Loan making and loan servicing transaction updates; Acquired property inventory; Daily register, balancing, and program reporting; and Fiscal and financial reporting.

1.4 How is the information collected?

This information is collected from the various application forms submitted by the borrower, voucher holder, and voucher landlord.

1.5 How will the information be checked for accuracy?

The data is reviewed by area specialists (subject matter experts).

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

Legal Authority: 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.). Executive Orders 10450, 10577, 10865, 12333, 12968, and for Social Security Numbers, 9397;

Homeland Security Presidential Directive 12; sections 3301, 3302, and 9901 of Title 5 of the United States Code; sections 2165 and 2201 of Title 42 of the United States Code; Chapter 23 of Title 50 of the United States Code; and Title 5, parts 2, 5, 731, 732, 735 and 736 of the Code of Federal Regulations.

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

Risks: As with all PII there will be some risk. Care must be taken to protect the PII if stored on our network or transmitted to and from RD employees.

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.

This information is needed in order to complete IRS reporting requirements. In addition, monthly voucher amounts are necessary to make payments out of AMAS.

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

Data transmitted in ASCII File format through the Gentran product must meet file format specifications. Each transaction is evaluated to meet business rules and USDA Regulations. Any transaction outside the expected values must be accepted by servicing personnel.

Subject Matter Experts (SME) validate tenant data prior to approval of project worksheets.

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 CLP Servicing - AMAS are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1-8, 12, 14, and 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 ACF2 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, 17, 18, 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 system stores three years of history data online. The remaining history is kept on archived tapes and has infinite retention. If/when the data is no longer required, it is

then properly destroyed.

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

Yes

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

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

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?

AMP: nightly downloads of project and borrow information.

EFT: Provides an interface between USDA and US Treasury Department to ensure timely transfer of funds from borrowers through the AMAS application.

FOCUS: Sends data for reports.

MFIS: nightly downloads of project and borrow information.

AMAS utilizes input from Program Loan Accounting System (PLAS) supplying input to PLAS through files during certain update cycles of the respective databases.

RD field Offices and NFAOC – online transaction entry and inquiry finance and accounting.

4.2 How is the information transmitted or disclosed?

RD field office personnel collect the loan obligation information from prospective borrowers/applicants.

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

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.

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?

U.S. Treasury - Online transaction entry and inquiry financial and accounting system to include a loan and grant origination system providing tracking and servicing capabilities. Data information includes name, date/place of birth, address information, personal identification number, biometric data, criminal history, and photographic image/identifying.

6 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.

Yes, under SORN Rural Development – 1 which is a shared artifact in CSAM.

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

VPN connection using AES-256 or 3DES encryption.

ISA and MOU agreements are in CSAM and maintained by the ISSS.

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

No risks to the privacy data; they are sent via VPN and signed Interconnection Service Agreement and Memorandum of Understanding agreements are in place in CSAM and maintained by the ISSS.

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, SORN1 (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, notice was provided to the individual prior to collection of information through the use of Form RD 410-4 "Statement Required by the Privacy Act".

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

Yes, individuals have the opportunity and/or right to decline to provide any information. Using the RD Form 410-4 "Statement Required by the Privacy Act", individuals agree to provide the information; if the individual declines, it will result in the rejection of the loan/grant application. Applicants are aware of the collection of personal 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?

Yes, users have agreements to consent to the use of their data through the use of Form RD 410-4 "Statement Required by the Privacy Act".

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.

RD ensures each system provides real time notice when PII is collected and a layered notice where warranted.

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 organization does the following:

1. Provides individuals to have access to their personally identifiable information (PII) maintained in its system(s) of records; http://www.usda.gov/wps/portal/usda/usdahome?navid=ACCESSIBILITY_STATEM
2. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; http://www.ocio.usda.gov/webform/accessibility-statement and
3. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests: http://www.usda.gov//wps/portal/usda/usdahome?navtype=FT&navid=PRIVACY_POLICY

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

The data is reviewed by area specialists (subject matter experts).

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

AMAS provides online transaction entry, batch processing and inquiry support for accounting, financial management and management information purposes for RD servicing offices, state offices, national office and finance office.

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

N/A

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

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?

Generally, the National Institute of Standards and Technology (NIST) 800-53 controls for Common Call Components 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.

Desk Procedures document the process for establishing, activating, and modifying IDs. This process is defined by System Owners. System Owners define Groups and account types. System Point of Contact (POC) assigns group membership and determines need-to-know validation. The POC is responsible for verifying user identification. The User Access Management (UAM) Team relies on a POC supplying the correct UserID and password. UAM tickets are the tool used to track authorized requests by approving Point of Contact (POC).

Currently, RD reviews reports from Human Resources (HR) on a Bi-weekly basis to include users that have either separated from the agency or transferred verifying the corresponding UAM ticket has been submitted. The organization employs automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are not used or authorized. Guest and Anonymous accounts are not managed by ISSS UAM Team. POCs (empowered by RD IT managers) are responsible for notifying UAM Team if access or roles need to be modified and periodically reviewing and certifying established access.

8.2 Will Department contractors have access to the system?

Yes

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 Awareness Training (ISAT) for all employees and contractors. RD is responsible for ensuring all new employees and contractors have taken the Department Security Awareness Training developed by Office of Chief Information Officer-Cyber Security (OCIO-CS). Training must be completed with a passing score prior to access to a USDA RD system. All RD employees/contractors are required to complete ISAT and USDA Privacy Basics on an annual basis.

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?

RD has an Application Auditing and Monitoring Policy in place that defines the following auditable events: server startup/shutdown, loading/unloading of services, installation/removal of software, system alerts/error messages, user logon/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.

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?

Mainframe - an online transaction entry and inquiry financial and accounting system.

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

No, AMAS does not have any technology that 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"?

No, 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?

System 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.

No, does not use 3rd party websites and/or applications.

10.4 How will the PII that becomes available through the agency's use of 3rd partywebsites and/or applications be used?

No, does 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?

No, does 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?

No, does 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?

No, does 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?

No, does 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)?

No, does not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

No, does not use 3rd 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?

No, does not use 3rd 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.

No, does not use 3rd party websites and/or applications.

Responsible Official

TAMARA ORLET Digitally signed by TAMARA ORLET
Date: 2017.10.11 10:24:18 -05'00'

Tamara Orlet
Chief, Management Services Technologies Branch

Approval Signature

signed for

EUGENE TEXTER Digitally signed by EUGENE TEXTER
Date: 2017.10.13 13:42:44 -05'00'

Diego Maldonado
Rural Development Privacy Officer