Privacy Impact Assessment

CLP Servicing; 1 of 7 - Automated Multi-Family Accounting System (AMAS)

USDA – Rural Development

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

Privacy Impact Assessment for the

CLP Servicing; 1 of 7 - Automated Multi-Family Accounting System (AMAS)

April 25, 2023

Contact Point

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

Abstract

The Automated Multi-Family Account System (AMAS) is an online transaction entry that serves as a loan and origination system. AMAS provides tracking and servicing capabilities for USDA RD's Multi-Family Housing (MFH) loans and grants. This PIA is required for AMAS because the system processes personally identifiable information (PII) from individuals.

Overview

Automated Multi-Family Accounting System (AMAS) is an online transaction entry and inquiry financial and accounting system. AMAS processes loan obligations and disbursements, loan closing and loan servicing, including calculating and applying rental assistance and cash application, and general ledger and financial reporting. The purpose of AMAS is to support the Multi-Family Housing (MFH) direct loan and grant program and share information with Farm Loan Accounting and Allotments System (FLAAS) under the USDA Farm Production and Conservation (FPAC) mission area. AMAS provides loan making and servicing capabilities for approximately 23,000 loans.

AMAS functionality includes: cash tracking, general ledger files, online inquiry and transaction input; loan making and loan servicing transaction updates; acquired property inventory & location lookup; daily register, balancing, and program reporting; and fiscal and financial reporting.

AMAS had both internal and external users. Internally, RD field offices, USDA National Office, Servicing and Asset Management Organization, and RD Finance Office use AMAS. Externally, AMAS is used to fulfill information requests from: Freedom of Information Act (FOIA) applicants, General Accounting Office (GAO), Office of Inspector General (OIG), Office of Management and Budget (OMB), and Congress.

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?

AMAS processes: name, street address, social security numbers (or tax identification numbers if SSNs are not used), agency assigned numbers, and demographic data (sex, marital status, veteran code, ethnicity, race).

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

RD program participants (borrowers and grantees) provide their information.

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

RD collects the information for AMAS loan and grant applications to meet the RD mission/business needs of providing financial opportunities to foster economic development, growth, and support to rural areas.

1.4 How is the information collected?

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

1.5 How will the information be checked for accuracy?

AMAS loan and grant applications are manually reviewed by the authorized RD area specialist to verify the accuracy of the data as part of the standard workflow process. If a RD applicant or RD customer notices any data inaccuracy, then they can reach out to the RD area specialist to get the necessary correction made to the AMAS loan or grant information.

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

- 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

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

MODERATE RISK: Current risks are the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the borrower, if an individual, and on the tenant.

MITIGATION: Data is stored in a secure environment. Authorization is required to access the applications.

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.

AMAS loan and grant information is used to support the RD mission and business needs of providing financial services to support economic development and support to rural areas. AMAS information is shared with Treasury to meet IRS reporting and comply with financial regulations for federal agencies.

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

Not applicable, AMAS does not use tools.

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

Not applicable, no commercial or publicly available data is used.

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.

AMAS enforces user authentication and authorization. The system is designed to confirm the identity of authorized AMAS users prior to granting the appropriate system access based on the user's pre-defined access level.

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?

AMAS records are unscheduled and thus permanent until scheduled.

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

No, records are not scheduled and will remain permanent until a records control schedule is developed/approved.

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

MODERATE RISK: AMAS is not connected to the internet and unauthorized access, unauthorized disclosure, or illegal use activity of the customer PII data is unlikely given the controls in place. However, maintaining records indefinitely increases the risk of unauthorized access and/or use.

MITIGATION: Until AMAS records are scheduled, the data is safeguarded in accordance with NIST 800-53 security controls and include the physical, administrative, and technical controls described in the protected system security plan.

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?

Farm Production and Conservation (FPAC), Program Accounting System (PLAS), sends data to AMAS for cash tracking, general ledger files and location lookup. PLAS receives AMAS data to complete select reports and datasets.

4.2 How is the information transmitted or disclosed?

Data is transmitted between RD and FPAC via Secure FTP, Webservice or via Mainframe.

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.

MODERATE RISK: Privacy risks include the potential compromise of PII data with AMAS.

MITIGATION: This risk is mitigated with internal security and privacy controls outline in the System Security Plan. Access is limited to authorized personnel using E-Authentication. Audit logs are maintained to monitor 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?

- Experian
- Equifax
- Dunn & Bradstreet
- TWAI – information shared: name, date/place of birth, address information, personal identification number, biometric data, criminal history, and photographic image/identifying characteristics; signed Jan 2020; for the purpose of ensuring timely transfer of funds from borrowers.

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.

Yes, sharing with Equifax, Experian, and Duns are covered under USDA/Rural Development 1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs, Routine Use #7. US Department of Treasury is covered under Routine Uses #3, 8, 25.

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

Equifax, Experian, and Duns: POAM #34383 is tracking the updated Information Security Agreements (ICAs).

Treasury*:* Secured transmissions are used for transferring data.

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

MODERATE RISK: Privacy risks include the potential compromise of PII data with AMAS.

MITIGATION: This risk is mitigated with internal security and privacy controls outline in the System Security Plan and the ISAs. Access is limited to authorized personnel using E-Authentication. Audit logs are maintained to monitor activity.

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, the system is covered by SORN 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?

Yes, notice was provided to the individual prior to the collection of information through the use of Form RD 410-9, Statement Required by the Privacy Act, which is provided before a RD applicant applies for an AMAS loan or grant.

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, but if they decline, then they will not be able to apply for the AMAS loan or grant. With the RD Form 410-9, Statement Required by the Privacy Act, individuals agree to provide the information, so RD 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?

No, to apply for an AMAS loan or grant the RD applicant consents to the collection of personal information as required for AMAS loan or grant processing. The RD applicant provides their consent as part of the AMAS loan or grant application with RD Form 410-9, 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.

MODERATE RISK: RD applicants consent to providing information for the completion of AMAS loan and grant requirements. RD applicants are notified with the privacy form, RD Form 410-9, when they apply for loans or grants and consent to the use of their data before applying for the AMAS loan or grant.

MITIGATION: Risks associated with individuals being unaware of the collection are mitigated because RD individual applicants must consent to the use of their data and this notification is included in the privacy form that is completed as part of the process for applying for AMAS loans and grants with RD.

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?

RD applicants have access to their AMAS loan or grant application information from the review and workflow processing by RD staff. The RD staff member will keep the RD applicant informed as to the status of their AMAS grant or loan application.

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

If an RD applicant notices inaccurate information with their AMAS loan or grant application, then they will contact the RD area specialist for correction of any erroneous information. The RD area specialist will facilitate the correction of any inaccurate information for the RD applicant.

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

Notification is part of the application process for AMAS loan and grant applications, so the RD borrower/applicant can contact the RD area specialist to correct any inaccurate information. Also, RD area specialists involved in processing the loan or grant application do manual review and will contact the RD applicant for any information corrections with their AMAS loan or grant application.

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 is 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?

AMAS enforces user authentication and authorization to information contained within the system prior to granting the appropriate system access based on the user's pre-defined access level.

Authentication and authorization is documented with desk procedures and approved by the AMAS system owner.

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?

All RD employees and contractors are required to complete an annual training. In addition, 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, AMAS has an ATO which is set to expire 12/05/2025.

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

NIST 800-53 controls are discussed in detail in the AMAS documentation including the Audit and Accountability (AU) controls in place to prevent misuse of data. Access to AMAS is enforced with authentication and access to sensitive information is controlled on a need-to-know basis and with audit logs of user activity. Section 5 of this PIA describes security protections in place for AMAS 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?

MODERATE RISK: There is moderate risk given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system.

MITIGATON: AMAS implements the relevant National Institute of Standards and Technology (NIST) 800-53 controls to prevent unauthorized access. Systems and Communication Protection controls are in place to prevent unauthorized access.

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?

AMAS records and manages obligations, disbursements collections and servicing for multi-family housing (MFH) loans/grants. Updates are done nightly in a batch mode. AMAS supports the MFH direct loan and grant program.

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 AMAS, 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 memoranda

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

N/A, AMAS does not use 3rd party websites or applications.

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

N/A, AMAS does not use 3rd party websites 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?

N/A, AMAS does not use 3rd party websites 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?

N/A, AMAS does not use 3rd party websites or applications.

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

N/A, AMAS does not use 3rd party websites 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?

N/A, AMAS does not use 3rd party websites 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?

N/A, AMAS does not use 3rd party websites 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)?

N/A, AMAS does not use 3rd party websites or applications.

10.10 Does the system use web measurement and customization technology?

N/A, AMAS does not use 3rd party websites 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?

N/A, AMAS does not use 3rd party websites 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.

N/A, AMAS does not use 3rd party websites or applications.

Approval Signature

Signed copy kept on record