Privacy Impact Assessment
Farm Loan Accounting and Allotments System (FLAAS)

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: August 13, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

Farm Loan Accounting and Allotments System (FLAAS)

July 30, 2020

Contact Point

Nimal Gunasinghe
FPAC
314-679-6619

Reviewing Official

James Flickinger
Associate Chief Information Security Officer, FPAC
United States Department of Agriculture
(816) 926-6010

Abstract

The Farm Loan Accounting and Allotments System (FLAAS) supports the loan/grant making, servicing, and General Ledger and reporting requirements for all program areas. The application is also used to view borrower status information and detailed history of transactions processed to a borrower's account.

FLAAS is comprised of the following applications:

- Program Loan Accounting System (PLAS)

- Status of Allotment Ledger Accounts (SALA)

The PIA is being conducted to support federal law, regulations and policies.

Overview

The Farm Loan Accounting and Allotments System (FLAAS) is the user interface used to record transactions and to analyze and correct rejected transactions (discrepancies). The application is also used to view borrower status information and detailed history of transactions processed to a borrower's account.

Typical Transactions include field office input transactions, daily transmission of loan payments, and recoverable cost charges paid by the National Finance Center (NFC). Information is shared with FSA and RD application users & accounting managers, FPAC IT support personnel (system, operations, DBAs), and FSA application developers. Additional sharing of information (which are outside the boundaries of this application) include Treasury, NFC, HUD, IRS, Dan & Bradstreet, US Bank, Credit Bureaus, and Borrowers.

The Legal Authority to Operate is the Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397.

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?

ADPS uses the customer's name, address, Social Security Number.

SALA does not use any PII.

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

ADPS obtains information from the customer, the State and County Office and SCOAP, FMMI, Farm Service Agency (FSA), Rural Development (RD).

SALA does not use any PII.

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

The information is used by ADPS to provide an accounting system of record and official reporting mechanism supporting loan and grant programs for insured, direct, and guaranteed loans. Information is reported to the IRS for taxation purposes as legally required by Section 6050J of the IRS Code.

SALA does not use any PII.

1.4 How is the information collected?

The system receives information from customers, State and County Offices, SCOAP, FMMI, Farm Service Agency (FSA), Rural Development (RD).

SALA does not use any PII.

1.5 How will the information be checked for accuracy?

Information is checked for accuracy by using Standard Accounting Practice of Balancing, GAO Audit, FOI; Edit validations. The WDC FLP Program Staff, Program Accounting Managers from FSA, and RD are responsible for assuring proper use of system data.

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

The Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and the Executive Order 9397. In addition, appropriate signed Interconnection Security Agreements (ISA) and Memorandums of Understanding (MOUs) are in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected.

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

The privacy risks are moderate. The minimum amount of Personally Identifiable Information is collected to satisfy the purpose of this system. The risks are mitigated using various control mechanisms. See below:

- Initial and ongoing employee security awareness training informs users of their responsibilities with regard to safeguarding PII and/or Privacy Act data.
- Access must be requested through FSA-13A security forms with justification.
- Access is restricted and issued only on a need to know basis.
- Access to the data center is restricted by physical security measures.
- A warning banner is displayed.
- All users must be uniquely identified and authenticated prior to access.
- Social Security numbers are masked so that it is not displayed on the terminal.
- Interconnection Security Agreements (ISA).
- Memorandums of Understanding (MOUs)

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.

ADPS uses the information to provide an accounting system of record and official reporting mechanism supporting loan and grant programs for insured, direct, and guaranteed loans.

SALA does not use any PII.

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

No additional “tools” (other than the application and database itself) are used to analyze the data.

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

The system does not use commercial or public data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Identification and authentication to operating systems are in place where the GIMS application resides (Mainframe). Access to the system and data are determined by business need and individual roles. Controls are in place to provide reasonable assurance that data integrity and confidentiality are maintained during processing. Controls in place to ensure the correct handling of information include the following:

- End users are correctly identified and authenticated according USDA and FSA security policies for access managements, authentication and identification controls.

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 information is retained indefinitely (permanent records).

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

Yes, in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records.

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

The retention period is based on a combination business need (i.e., how long do we need this information for our business process) and long term usefulness. When records have reached their retention period, they are immediately retired or destroyed in accordance with the USDA Record Retention policies and procedures.

During this period, the stored information may be at risk for viewing by unauthorized parties, data loss or destruction and non-availability. Access to computerized files are

protected by access control software, physical access controls and if warranted, password-protected.

SORN USDA/FSA-2 States: Program documents are destroyed within 6 years after end of participation. However, FSA is under a records freeze.

According to Records Management DR3080-001 Disposition of Inactive Records:

Records and other documents that are no longer sufficiently active to warrant retention in office space shall be removed as rapidly as possible by: (a) transfer to a Federal Records Center, or (b) transfer to a records retention facility meeting the requirements of 36 CFR Chapter 12, Subchapter B Records Management, Subpart K, 1228.224 through 1228.244, or (c) if authorized, by disposal. (See Appendix B – Records Disposition Procedures.)

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?

FLAAS supports all of FSA's and RD's 30 plus loan and grant programs for farm, business, and community development in rural areas. This major system contains the Agencies' official accounting records and is supported and maintained by the Finance Office and Information Systems Management in St. Louis.
RD shares with Treasury, NFC, HUD IRS Dan & Bradstreet, US Bank Credit Bureaus, Borrowers – Borrower information including loan account information. processes include the following topics:

- Treasury Reporting - The DCIA processes evaluate accounts for amount and date of delinquency and reported to Treasury for offset. (An offset being a treasury payment transferred to satisfy a debt instead of going to the recipient.)
- IRS Reporting/Administrative Offset – Provides information to IRS for various reporting requirements which includes IRS tax refund offset to delinquent borrowers
- Credit Reporting – Provides information to Equifax, Dun & Bradstreet, and Experian
- Housing and Urban Development Reporting – Provides information to HUD for Credit Alert Interactive Voice Response System
- Deposit Fund Process – Facilitates the control and reconciliation of the deposits in the Agency collections clearing account. The system produces reports, which are used to reconcile Treasury deposits to processed and suspended cash transactions

- Collection Only Borrowers – Reports on borrowers coded for Collection Only servicing (an unsatisfied account that the borrower is legally liable for but the only servicing actions we accept are payments)
- Cost Items – NFC Interface

4.2 How is the information transmitted or disclosed?

Information is accessed on ADPS through online queries and batch processing using name or Social Security Number.

SALA does not use any PII.

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.

Sharing is internal and all users must have security clearance and granted access through the FSA13-A and RD Log book process. The risks are mitigated using various control mechanisms. See below:

- Initial and ongoing employee security awareness training informs users of their responsibilities with regard to safeguarding PII and/or Privacy Act data.
- Access must be requested through FSA-13A security forms with justification.
- Access is restricted and issued only on a need to know basis.
- Access to the data center is restricted by physical security measures.
- A warning banner is displayed.
- All users must be uniquely identified and authenticated prior to access.
- Social Security numbers are masked so that it is not displayed on the terminal.
- Interconnection Security Agreements (ISA).
- Memorandums of Understanding (MOUs).

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?

Treasury, NFC, HUD IRS Dan & Bradstreet, US Bank Credit Bureaus, Borrowers – Borrower information including loan account information.

Processes include the following topics:

- Treasury Reporting - The DCIA processes evaluate accounts for amount and date of delinquency and reported to Treasury for offset. (An offset being a treasury payment transferred to satisfy a debt instead of going to the recipient.)

- IRS Reporting/Administrative Offset – Provides information to IRS for various reporting requirements which includes IRS tax refund offset to delinquent borrowers
- Credit Reporting – Provides information to Equifax, Dun & Bradstreet, and Experian
- Housing and Urban Development Reporting – Provides information to HUD for Credit Alert Interactive Voice Response System
- Deposit Fund Process – Facilitates the control and reconciliation of the deposits in the Agency collections clearing account. The system produces reports, which are used to reconcile Treasury deposits to processed and suspended cash transactions
- Collection Only Borrowers – Reports on borrowers coded for Collection Only servicing (an unsatisfied account that the borrower is legally liable for but the only servicing actions we accept are payments)
- Cost Items – NFC Interface

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.

USDA/FSA-2, Farm Records File Automated and USDA/FSA-14, Applicant/Borrower.

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

Secure FTP (mainframe).

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

The privacy risks are moderate. The minimum amount of Personally Identifiable Information is collected to satisfy the purpose of this system. The risks are mitigated using various control mechanisms. See below:

- Initial and ongoing employee security awareness training informs users of their responsibilities with regard to safeguarding PII and/or Privacy Act data.
- Access must be requested through FSA-13A security forms with justification.
- Access is restricted and issued only on a need to know basis.
- Access to the data center is restricted by physical security measures.
- A warning banner is displayed.
- All users must be uniquely identified and authenticated prior to access.
- Social Security numbers are masked so that it is not displayed on the terminal.
- Interconnection Security Agreements (ISA).

- Memorandums of Understanding (MOUs).

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.

The legal authority to capture limited PII data for FSA systems is established by USDA SORN System of Records Notices (SORN) FSA-2 and FSA-14

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

Yes.

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

Yes. FSA Privacy Policy states that "Submitting information is strictly voluntary."

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, in accordance with FSA Privacy policy and the individual's written consent.

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.

The risk is considered moderate. Notification is automatically provided in the system of records notice (Federal Register publication): SORN: USDA/FSA–2 - Farm Records File (Automated) and USDA/FSA-14 - Applicant/Borrower.

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?

As published in SORN USDA/FSA-2 and SORN USDA/FSA-14: “An individual may obtain information about a record in the system which pertains to such individual by submitting a written request to the above listed System Manager. The envelope and letter should be marked ``Privacy Act Request.'' A request for information should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file.”

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

As published in SORN USDA/FSA-2 and SORN USDA/FSA-14: “Individuals desiring to contest or amend information maintained in the system should direct their request to the above listed System Manager, and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file.”

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

Formal redress is provided via the FSA Privacy Act Operations Handbook.

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.

The risk associated with redress is considered low, as the public does not have access to the system or the data. While the public cannot access the system to update or change their personal information, they may update their information using form AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

There is work going on for Customer Self Service which will be public facing. SCIMS is no longer the source of entry since Business Partner was implemented in December 2014.

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?

FSA-13-A is used to request user access to USDA and FSA information technology systems including specifying authorization for accessing the system. (Refer to Notice IRM-440) In addition, access to FSA web applications is gained via an on-line registration process similar to using the FSA-13- A form. For system specific detailed access see SSP.

8.2 Will Department contractors have access to the system?

Department contractors do not have access to the System.

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

Once hired, privacy training and security awareness training is completed prior to gaining access to a workstation. The privacy training addresses user's responsibilities to protect privacy data and how to protect it.

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

Yes, 04/10/2015.

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

Specific logging of transaction events (including who entered and when the transaction was completed along with type of financial transaction (such as loan activity, program payments, approvals, determinations, general or subsidiary ledger entries, etc.)); and application parameter/table changes (such as loan rates, penalties, etc.) occurs as part of the nightly process.

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?

The main risk associated with privacy is the exposure to unauthorized access to privacy information. This risk is considered moderate. Mitigating controls are in place to ensure privacy risks are minimal. Mitigated controls are mapped back to SSP in CSAM.

Quarterly access reviews are done to ensure controls are mitigated.

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?

Major application

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"?

Yes, no 3rd party website (hosting) or 3rd party application is being used.

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

N/A

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

N/A

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

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

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

N/A

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

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

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

10.10 Does the system use web measurement and customization technology?

N/A

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

10.12 <u>Privacy Impact Analysis</u>: 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

Agency Responsible Officials

NIMAL GUNASINGHE

Digitally signed by NIMAL GUNASINGHE
Date: 2020.09.30 13:25:41 -05'00'

Nimal Gunasinghe
FLAAS Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS

Digitally signed by LANITA THOMAS
Date: 2020.10.23 12:55:56 -04'00'

Lanita Thomas
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2020.10.23 07:54:04 -05'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture