Privacy Impact Assessment

Guaranteed Loan System (GLS)

Rural Development (RD)

- August 2017
- Prepared for: RD

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	9/8/2014	SAC	Original under CLP
1.1	7/19/2016	TGW	FY 16 review
1.2	4/20/2017	TGW	Update external connections
1.3	8/22/2017	SAC	FY18 review, updated interconnections removing SEBAS

Abstract

GLS records and manages obligations, servicing, and loss claims for guaranteed programs, as well as managing and monitoring lenders. It is divided into seven modules that include Farm Service Agency Guaranteed (FSAG), Guaranteed Annual Fees (GAF), Guaranteed Loan (GuarLoan), Intermediary Relending Program (IRP), Multi Family Guaranteed Housing (MFGH), and Single Family Housing (SFH Loss).

Overview

As previously mentioned in the abstract, GLS is divided into seven modules that include FSAG, GAF, GuarLoan, IRP, MFGH, and SFH Loss.

FSAG is an application that includes loan origination, loan closing, losses, secondary market transactions, lender portfolio management, servicing actions, re-amortizations, consolidations, transfers, agency loan repurchases, liquidation expenses, interest assistance payments, status reporting.

GAF is an application that provides an automated means to retrieve billing of annual fees against guaranteed loans and submits annual fee payment requests.

GuarLoan is an application that includes common or shared applications used by two or more loan programs within FSA, including loan origination, funds reservation, loan closing, annual fees, late fees, losses, secondary market transactions, lender portfolio management, servicing actions, re-amortizations, consolidations, transfers, agency loan repurchases, liquidation expenses, interest assistance payments, status reporting, and credit bureau reporting.

IRP is an application that provides loans to local organizations (intermediaries) for establishing revolving loan funds. These funds assist with financing business and economic development activity to create/retain jobs in disadvantaged/remote communities.

MFHG applications include loan origination, funds reservation, loan closing, losses, secondary market transactions, lender portfolio management, servicing actions, re-amortizations, consolidations, transfers, agency loan repurchases, liquidation expenses, interest credit payments, and status reporting.

SFH Loss application automates the Guaranteed SFH Loss claims process by allowing lenders to electronically enter and transmit loss data and disburse loss payments to the lender via electronic funds transfer (EFT). It allows for accurate and timely processing of SFH Loss claims data, and the captured data is used for the Debt Collection Improvement Act (DCIA) processing.

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: Client names, borrowers' social security numbers, co- borrowers, key members addresses, business financial data, and debt payment information.

Lender Information: Lender identification numbers, lender names, addresses, and business financial data.

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

Business Programs/Community Facilities/MFHG/FSAG applications, closing documentation, phone personal interviews, and/or correspondence are received via GLS.

SFH applications, closing documentation, phone and personal interviews, and correspondence are received via USDA LINC Guaranteed Underwriting System (GUS).

.

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

Information is collected to monitor USDA-guaranteed private sector lender's loan portfolios and to provide financial information on the Guaranteed portfolio. The data is also used to determine eligibility and for consolidated reporting purposes such as demographic data.

1.4 How is the information collected?

Loan officers and trusted lenders provide input for guaranteed loan application data. RD receives a monthly file of banking data from Treasury, Ginnie Mae, and Dun & Bradstreet.

1.5 How will the information be checked for accuracy?

The information is transferred to paper forms which are printed and signed by the customer. Once the data is on hardcopy, the application data stored in the system is not involved in the loan process.

There are many balancing processes that execute with every batch update cycle to validate the lender's loan portfolios. Balancing is done against general ledger, allotment summary, and check disbursement. NFAOC reviews these outputs daily.

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.

Risks: Risk is low since the customer signs the printed paper documents. Once the data is on hardcopy, the application data stored in the system is not involved in the loan process.

Mitigation: Physical data is stored in a secure environment and the system is behind the USDA secure network 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).

The application is behind eAuthentication (eAuth) with a Level 2 access authority.

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.

Information is collected to monitor USDA-guaranteed private sector lender's loan portfolios and to provide financial information on the GLS portfolio. The data is also used to determine eligibility and for consolidated reporting purposes such as demographic dat.

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

N/A

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 the GLS system are discussed in detail in the System Security Plan and specifically the Access Controls (AC 1-8, 11, 12, 14, 17, 20, and 21). Identification and Authentication (IA 1-7) controls are in place to prevent unauthorized access restricting users from accessing the operating system, other applications or other system resources not needed in the performance of their duties and is restricted by eAuth User Identification (User ID). Authority and Purpose (AP) compensating control gives explanation of why PII is allowed on the system. Systems and Communication Protection (SC 1, 2, 4, 5, 7, 8, 10, 12, 13, 17, 18, 20-23, 28, 39) controls are in place to prevent unauthorized access.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Information is retained indefinitely.

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: Information is retained indefinitely. 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: Data integrity controls (DI 1-2) are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls which refer to tests and evaluations used to determine compliance with security specifications and

requirements are in place and it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements are in place.

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?

GLS applications

- Commercial Loan Servicing System (CLSS) - process lender status reports and loan closings
- Program Funds Control System (PFCS) – Data is forwarded to MQ series messages to PFCS for specific transactions.
- Automated Mail Processing (AMP) - Prints statements and tax forms
- Business Intelligence (BI): Tabular Data Warehouse (TDW) - Receives data for reports
- Common Call Components: Business Rules Engine (BRE) / FICO Blaze – receives information for GLS total scorecard and loan approval recommendations
- eServices: Account Cross Reference (ACR) – request is made to perform TDW lookup
- New Loan Originations: Eligibility, Guaranteed Underwriting System (GUS), Lender Interactive Network Communication (LINC) - process lender status reports and loan closings
- Program Loan Accounting System (PLAS) - Accounting system of record and official reporting mechanism

FSAG

- Farm Services Agency (FSA) – application is shared by both FSAG and FSA

GuarLoan

- Security Management: Authorized Authentication Security Module (AASM) - RD users create a user profile with the AASM system via a hyperlink from GLS applications

IRP

- Business Intelligence (BI): Tabular Data Warehouse (TDW) - Receives data for reports

MFHG

- Program Loan Accounting System (PLAS) - Accounting system of record and official reporting mechanism
- Program Funds Control System (PFCS) – Data is forwarded to MQ series messages to PFCS for specific transactions.
- Business Intelligence (BI): Tabular Data Warehouse (TDW) - Receives data for reports

SFH Loss

- Common Call Component: ECF/Imaging – Loan closing data and workflow; goes through various stages of review, determination of completion, approval, obligation, and closing of the loan.
- eServices: Electronic Funds Transfer (EFT) – Pulls data from EFT tables to send payments
- Program Funds Control System (PFCS) – Data is forwarded to MQ series messages to PFCS for specific transactions.
- Program Loan Accounting System (PLAS) - Accounting system of record and official reporting mechanism

4.2 How is the information transmitted or disclosed?

The information is available within GLS by authorized government employees transmitted using HTTPS.

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, obligation and disbursement data, statement and tax report information, borrower information and accounting information.

MITIGRATION: NIST 800-53 controls are discussed in detail in the System Security Plan (SSP). System and Communication (SC) controls are in place to provide integrity and availability.

The security and control of PII is the responsibility of the System Owner and RD employees. Risk is mitigated with implementation of RD ISSS policies, standards and procedures.

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

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

- **Ginnie Mae**: Loan data information is shared such as sensitive financial and privacy data. Ginnie Mae purchases mortgage back securities.
- **Bulk Data Exchange System (BDES) / Dun & Bradstreet:** FSA-GLS reports Guarantee loan information (Borrower or Co-Borrower name, Lender name, address, date of report, account number, taxpayer identification number, Federal Agency w/program code, lender name, status, amount of outstanding debt, type of debt, date initiated, and maturity date) to Dun & Bradstreet on a monthly basis.
- **Fiscal Service Treasury Web Application Infrastructure (TWAI) Department of Treasury** - U. S. Department of Treasury – Connect:Direct without Secure+ uses a proprietary file transfer protocol
- **Experian Credit Bureau:** Data files transferred from GLS to Experian for credit bureau reporting.

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, 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?

All external connections require an Interconnection Service Agreement (ISA) or Memorandum of Understanding (MOU).

- **Ginnie Mae** – data is sent quarterly via CD (mailed)
- **Bulk Data Exchange System (BDES) / Dun & Bradstreet** – one way transmission via Secure File Transfer Protocol (SFTP)

- **Experian Credit Bureau** – data is transmitted monthly via SFTP connection to Treasury.
- **Fiscal Service Treasury Web Application Infrastructure (TWAI) Department of Treasury** - U. S. Department of Treasury – Connect:Direct without Secure+ uses a proprietary file transfer protocol (TCP ports 1364 and 1372).

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 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 exchange of data will be limited to specific server IP addresses over Secure FTP port 22, enforced by firewall rules. 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.

This information is protected in accordance with Office of Management and Budget (OMB) Circular A-127, Management of Federal Information Resources, Circular A- 130, Financial Management Systems and Privacy Act of 1974 [Public Law (PL) 93- 579].

The security and control of PII is the responsibility of the System Owner and RD employees risk is mitigated with implementation of NIST SP 800-53 Risk Assessment (RA) controls are evaluated as part of the GLS System Security Plan (SSP).

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.

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

Yes.

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. Users consented to the use of their data during application process.

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.

Individuals 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, there is no risk associated. If the user accepts, then 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?

Individuals can go through USDA RD and FSA system users and trusted lenders that have access to their information.

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

For GLS specifically:

For USDA RD employees, FSA users and trusted lenders that have access to their information, access is controlled by User ID and password. Access rights are granted to designated individuals only when their supervisor or the site system manager approves a written request.

Privileges granted are based on job functions and area of authority (e.g. State office user with authority for their state only).

Customers and employees may contact **USDA Rural Development Primary FOIA Contact Information:**

USDA Rural Development
FOIA/Privacy Act/Torts Unit
1400 Independence Avenue, SW, Stop 0742
Washington, DC 20250-0706
Telephone (202) 690-5394
Email: Ssd.foia@wdc.usda.gov

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

Individual borrowers can't update the system. Access is controlled by eAuth User ID and password. Access rights are granted to designated individuals only when their supervisor or the site system manager approves a written request. Data is corrected by authorized users.

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 Freedom of Information Act.

Contact:

Administrator, Rural Housing Service, USDA, 1400 Independence Avenue, SW, Room 5014, South Building, Stop 0701, Washington, DC 20250-0701;

Administrator, Rural Business-Cooperative Service, USDA, 1400 Independence Avenue, SW, Room 5045, South Building, Stop 3201, Washington, DC 20250-3201;

Administrator, Rural Utilities Service, USDA, 1400 Independence Avenue, SW, Room 4501, South Building, Stop 1510, Washington, DC 2050-1510.

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.

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?

USDA RD employee, FSA system users and trusted lenders have access to GLS via eAuth.

National Institute of Standards and Technology (NIST) 800-53 controls for Guaranteed 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 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 HR on a Bi-weekly basis. The organization employs automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are not used or authorized. System Owners 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, Department contractors are required to undergo the same access and authentication procedures that federal employees must adhere to, access procedures are discussed in question 8.1.

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 OCIO-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 23 February 2020.

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 SSP including the Audit and Accountability (AU) controls in place to prevent misuse of data.

RD has a NIST Audit and Accountability Policy, Standards, and Procedure that defines the following auditable events: server startup and shutdown, loading and unloading of services, installation and removal of software, system alerts and error messages, user logon and logoff

attempts (both successful and unsuccessful), granting of elevated privileges (root access success and failure), modifications of privileges and access controls, all root commands (success and failure), and sensitive files accessed, modified and added. These controls, including full compliance, inheritance, and risk acceptance descriptions, are available in CSAM.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

RISK: 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?

This project is part of the Comprehensive Loan Program (CLP) Investment facilitates the processing by USDA personnel of applications, obligations, loans, grants, and collections on behalf of RD Commercial Program customers.

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

GLS does not raise any privacy concerns because of its employed technology.

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?

GLS does not use third 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.

GLS does not use third 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?

GLS does not use third 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?

GLS does not use third 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?

GLS does not use third 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?

GLS does not use third 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?

GLS does not use third 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)?

GLS does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

GLS does 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?

GLS does 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.

GLS does not use third party websites or applications.

Responsible Official

ARCHLOVEDIA STITH

Digitally signed by ARCHLOVEDIA STITH
Date: 2017.10.03 06:40:40 -05'00'

Archlovedia Stith
Chief, Guaranteed Loan Technologies Branch

Approval Signature

Signed For

EUGENE TEXTER

Digitally signed by EUGENE TEXTER
Date: 2017.10.06 07:53:58 -05'00'

Diego Maldonado
Rural Development Privacy Officer