USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: USDA Rural Development

System Name: Guaranteed

System Type:
☒ **Major Application**
☐ **General Support System**
☐ **Non-major Application**

System Categorization (per FIPS 199):
☐ **High**
☒ **Moderate**
☐ **Low**

Description of the System:

Guaranteed is one of Rural Development's official accounting and financial management systems and supports Guaranteed and Direct Business & Industry program, Guaranteed and Direct Community Facility program, Guaranteed Rural Rental Housing program, Guaranteed Single Family Housing program - including Guaranteed Single Family Housing Losses, Guaranteed Water & Waste program in Rural Development, and also supports Guaranteed Farm Loan Program in the Farm Service Agency (FSA) and Guaranteed Underwriting System (GUS). Guaranteed is an online transaction entry and inquiry financial and accounting system accessed by over 700 field offices, the National Office, and Finance Office. Updates are done both on-line real-time and through nightly batch processes. The field offices are the primary user of Guaranteed and the Finance Office has overall operational, financial, and accounting responsibility for Rural Development. Our external trusted partners (Lenders) provide loan status data via file uploads from a Lender Interactive Network Connection (LINC) to the mainframe during the monthly reporting periods. These files are verified for data exceptions and updated during monthly and quarterly scheduled processing timeframes. Guaranteed also has an external connection with lenders via Application Authorization Security Management (AASM). This security program resides on the Web Farm and authenticates lenders into Guaranteed via electronic authentication (eAuth). This external connection allows lenders limited capabilities to the Guaranteed Underwriting System (GUS) and the Guaranteed Single Family Housing Losses (SFHLosses) applications. AASM assigns more stringent controls over external users than eAuth alone. Within AASM certain lenders (Branch Representatives) can in turn assign members within their branch access to Guaranteed. Guaranteed functions include: online inquiry and transaction input; pre-application and application processing, loan making and loan servicing transaction updates, portfolio management, lender management, daily register, balancing, and program reporting; and fiscal and financial reporting.

Guaranteed Underwriting System (GUS) is a Java J2EE application that provides a streamlined and automated application process, automated credit decision-making, and automated the eligibility determination for the SFH guaranteed rural housing loan program.

The Guaranteed Underwriting System (GUS) application provides a web user interface used to capture borrower loan application data for single family home loans guaranteed by the USDA. The system utilizes credit agency interfaces in conjunction with a third party underwriting engine to automate the credit decision process. The system is available for Lenders to enter applications seven days a week via an E-authentication protected web site.

Who owns this system?

Greg Eschman
USDA Rural Development
4300 Goodfellow Blvd.
St. Louis, MO 63120
Greg.eschman@stl.usda.gov
(314) 457-5057

Who is the security contact for this system?

Eugene Texter
Information System Security Staff
USDA Rural Development
Building 105, FC-44
4300 Goodfellow Boulevard
St. Louis, MO 63120
eugene.texter@stl.usda.gov
314-457-4778

Brenda Dinges
Information System Security Program Manager
USDA Rural Development
Building 105, FC-44
4300 Goodfellow Boulevard
St. Louis, MO 63120
brenda.dinges@stl.usda.gov
314-457-4772

Who completed this document?

Greg Eschman
USDA Rural Development
4300 Goodfellow Blvd.
St. Louis, MO 63120
Greg.eschman@stl.usda.gov
(314) 457-5057

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	**Yes**	**Yes**
Social Security Number	**Yes**	**No**
Telephone Number	**Yes**	**Yes**
Email address	**Yes**	**Yes**
Street address	**Yes**	**Yes**
Financial data (i.e. account numbers, tax ids, etc)	**Yes**	**Yes**
Health data	**No**	**No**
Biometric data	**No**	**No**
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code[1]	**Yes**	**No**
Are social security numbers embedded in any field?	**Yes**	**No**
Is any portion of a social security numbers used?	**Yes**	**No**
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	**No**	**No**

If all of the answers in Questions 1 and 2 are NO, STOP
You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets,
Part 7, Section E, Question 8c is:
No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

DATA COLLECTION

3. Generally describe the data to be used in the system.

Customer Information: Client names, Social Security Numbers of Borrowers, Co-Borrowers, Key Members addresses, and business financial data, debt payment information. **Lender Information**: Lender Identification Numbers, lender names, addresses and business financial data.

4. Is the collection of the data both relevant and necessary to the purpose for which the system is designed? In other words, the data is absolutely needed and has significant and bearing on the system's purpose.

☒ Yes
□ No. If NO, go to question 5

4.1. Explain.

Yes. The data attributes provide loan processing information.

5. Sources of the data in the system.

5.1. What data is being collected from citizens and/or employees?

Customer Information: Client names, Social Security Numbers of Borrowers, Co-Borrowers, Key Members addresses, and business financial data, debt payment information. **Lender Information**: Lender Identification Numbers, lender names, addresses and business financial data.

5.2. What USDA agencies are providing data for use in the system?

USDA Rural Development provide for inputting application data.

5.3. What government agencies (state, county, city, local, etc.) are providing data for use in the system?

No information is received from State or Local agencies.

5.4. From what other third party sources is data being collected?

FSA loan officers provide for inputting application data. Trusted lenders provide for inputting guaranteed loan application data. We receive a file of banking data form Treasury via NITC monthly.

6. Will data be collected from sources outside your agency? For example, citizens and employees, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

☒ Yes
□ No. If NO, go to question 7

6.1. How will the data collected from citizens and employees be verified for accuracy, relevance, timeliness, and completeness?

The risk of loss, misuse, or unauthorized access to this information is low since the information is transferred to paper forms, which are printed and signed by the customer. Once the data is on hardcopy, the application data store in the system is not involved in the loan process.
There are many balancing processes, which executes with every batch update cycle to validate data. The Deputy Chief Financial Officer (DCFO) reviews these outputs daily. These reports are for both GLS operational tables and data warehouse tables. Balancing is done against general ledger, allotment summary and check disbursement.

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness? See 6.1

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness? See 6.1

DATA USE

7. Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?

Monitor Private Sector Lenders Portfolios for loans guaranteed by USDA and provide financial information on the guaranteed Portfolio

8. Will the data be used for any other purpose?

☒ Yes
□ No. If NO, go to question 9

8.1. What are the other purposes?

Various calculated financial data fields will be derived and stored in GUARANTEED.

9. Is the use of the data both relevant and necessary to the purpose for which the system is being used? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system’s purpose.

☒ Yes
□ No. If NO, go to question 10

9.1. Explain.

Yes. The data attributes provide loan processing information.

10. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

☒ Yes
□ No

10.1. Will the new data be placed in the individual's record (citizen or employee)?

Yes, the data will be stored by borrower record/borrower identification.

10.2. Can the system make determinations about citizens or employees that would not be possible without the new data?

Yes, through GUS, component decisions are made based on the input of data. The government testers and the business users/program sponsors will verify the calculated data during the testing phase of a development project.

10.3. How will the new data be verified for relevance and accuracy?

The government testers and the business users/program sponsors will verify the calculated data during the testing phase of a development project. Once new processes allowing new data are implemented into production, balancing routines would also have been modified, if applicable, so the accuracy of the new data is being verified.

11. Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?

Monitor Private Sector Lenders Portfolios for loans guaranteed by USDA and provide financial information on the guaranteed Portfolio

12. Will the data be used for any other purpose (other than indicated in question 11)?

☒ Yes
□ No. If NO, go to question 13

12.1. What are the other purposes?

Various calculated financial data fields will be derived and stored in GUARANTEED.

13. Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

☒ Yes
□ No. No processes or data is consolidated with Imaging.

13.1. What controls are in place to protect the data and prevent unauthorized access?

Some data is consolidated based on requirements. However, rather consolidated or not the following controls are in place to protect our data.

1. The applications capability to establish access control lists (ACL) or registers is based upon the basic security setup of the operating system.
2. Application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties via access given to User IDs limited to what is needed to perform their job.
3. The controls used to detect unauthorized transaction attempts are security logs/audit trails.
4. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.
5. Warning banners are used to warn and inform users who sign on to the system that this is a secure and private network. Warning banners are in compliance with USDA guidelines.

6. Quarterly verifications reports are produced and required to be reviewed by the responsible Point of Contact (POC) based on the organizational unit.

14. Are processes being consolidated?

☒ Yes
☐ No. If NO, go to question 15

14.1. What controls are in place to protect the data and prevent unauthorized access?

800-53 controls are discussed in detail in the System Security Plan.

DATA RETENTION

15. Is the data periodically purged from the system?

☐ Yes
☒ No

The Guaranteed Loan System has not purged any data from the operational tables nor the data warehouse. A Request for Automation has been written to begin purging data from the operational tables that meets certain criteria. There are no plans to purge any data from the data warehouse.

15.1. How long is the data retained whether it is on paper, electronically, in the system or in a backup?

Indefinitely.

15.2. What are the procedures for purging the data at the end of the retention period?

When we implement a purging process, the operating instructions will be incorporated into the Guaranteed Loan System batch schedule. These operating instructions, along with the user approved project specification documents, will be the documentation for this process.

15.3. Where are these procedures documented?

See 15.2

16. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Reports are produced and reviewed for accuracy. Lenders are required to provide information on a monthly or quarterly basis.

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

☒ Yes
☐ No

DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

☒ Yes

The other agencies that share/have access to GUARANTEED System are Treasury, Fannie Mae, and HUD. Only USDA (currently RD & FSA) authorized system users will have access to the data in this system.

☐ No

18.1. How will the data be used by the other agency?

To create and process loan applications with USDA and trusted Lenders.

18.2. Who is responsible for assuring the other agency properly uses of the data?

The system owner

19. Is the data transmitted to another agency or an independent site?

Yes. GUARANTEED has connections with PLAS, Treasury, Fannie Mae, HUD. Treasury is interfacing with NITC- GLS interfaces with NITC. GLS does not directly interface with Treasury

19.1. Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

Yes. The Information System Security Staff (ISSS) maintain the Interconnection service agreements.

19.2. Where are those documents located?

Located and available upon request from the ISSS department

20. Is the system operated in more than one site?

☒ Yes
□ No

Access is through user terminals, which are on the system.

20.1. How will consistent use of the system and data be maintained in all sites?

Any GLS components/data that are in Web Farm are balanced between the sites.

DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

USDA RD and FSA GUARANTEED system users and managers, GUARANTEED Systems Administrators, and GUARANTEED Trusted Lenders.

22. How will user access to the data be determined?

The ISSS Point of Contact (POC) is responsible for verifying user identification. The User Access Management Team (UAMT) relies on a POC supplying the correct userID and password to Log book to identify them. Log Book tickets are the tool used to track authorized requests by approving POC.

Logbook entries are kept by the POC, Juanita Karels, of the Administrative Support Staff.

The application uses UAMT.

The Security – Greg Eschman reviews User Identification for Production GLS report.

Yes, the GLS Application employs an automated mechanism for account management. It employs Log book entries.

Temporary and emergency accounts are rare but both are terminated based on the expiration date established.

UMAT authorizes the set-up of these accounts.

22.1. Are criteria, procedures, controls, and responsibilities regarding user access documented?

☒ Yes
☐ No. If NO, go to question 23

22.2. Where are criteria, procedures, controls, and responsibilities regarding user access documented?

1. The applications capability to establish access control lists (ACL) or registers is by based upon the basic security setup of the operating system.
2. Application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties via access given to User IDs limited to what is needed to perform their job.
3. Any controls used to detect unauthorized transaction attempts are security logs/audit trails through ACF2 tools.
4. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.
5. Warning banners are used to warn and inform users who sign on to the system that this is a secure and private network. Warning banners are in compliance with USDA guidelines.

23. How will user access to the data be restricted?

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

Are procedures in place to detect or deter browsing??

☒ Yes – See 23
☐ No

23.1. Are procedures in place to detect or deter unauthorized user access?

☒ Yes – See 23
☐ No

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

☒ Yes – The User Access Management Team (UAMT) maintains GLS security and it controls all access to GLS. Only accesses authorized by the responsible POC are granted. Audit trails are conducted after-the-fact to verify if a breach has occurred.

☐ No

CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the citizens and employees affected by the interface (i.e. office, person, departmental position, etc.)?

The System/Application Owner

26. How can citizens and employees contact the office or person responsible for protecting their privacy rights?

Citizens and employees may contact the Freedom of Information Officer:

Dorothy Hinden
Freedom of Information Officer
Rural Development, USDA
7th Floor, Reporter's Bldg.
Washington, DC 20250
Dorothy.Hinden@wdc.usda.gov
(202)692-0031

27. A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

☒ Yes - If YES, where is the breach notification policy located?

- U.S. Department of Agriculture Incident Notification Plan September 2007

- DM3505-001 USDA Computer Incident Response Procedures Manual.

- Computer Incident Response Standard Operating Procedures (CIRT)

28. Consider the following:
    - Consolidation and linkage of files and systems
    - Derivation of data
    - Accelerated information processing and decision making
    - Use of new technologies

Is there a potential to deprive a citizens and employees of fundamental rules of fairness (those protections found in the Bill of Rights)?

□ Yes
☒ No. If NO, go to question 29

28.1. Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of citizens and employees?

DM 3515-002, section e states:

To fulfill the commitment of the USDA to protect customer and employee data, several issues must be addressed with respect to privacy:

1 The use of information must be controlled; and
2 Information may be used only for a necessary and lawful purpose.

Where Public Affairs systems of records are involved:
1 Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them;
2 Information collected for a particular purpose should not be used for another purpose without the subject's consent unless such other uses are specifically authorized or mandated by law; and
3 Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

Also, P.L. 95-454, the Civil Service Reform Act of 1978 which is enforced by The U.S. Equal Employment Opportunity Commission (EEOC) ensures the equitable treatment of the employees.

30. Is there any possibility of treating citizens and employees differently and unfairly based upon their individual or group characteristics?

□ Yes
☒ No. See Above.

SYSTEM OF RECORD

31. Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

☒ Yes
□ No

31.1. How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

Data is retrieved by GUARANTEED authorized users through login IDs using ACF2 IDs which are verified on the NITC Mainframe. The personal identifier, borrower case number, retrieves it. The user inputs borrower case number that is converted to a unique identifier assigned by GLS.

31.2. Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov)

GUARANTEED Operates under SOR Notice USDA/RURAL DEVELOPMENT - 1, System name: Applicant, Borrower, Grantee, or Tenant File.

31.3. If the system is being modified, will the SOR require amendment or revision?

A change control process is in place whereby all changes to application software are tested and user approved prior to being installed into production. Changes to the applications are controlled by specific written requests for automation. Test results are kept until the turnover release warranty is expired and used as reference if necessary. Emergency fixes are handled in the same way as more fixes that are extensive except

that they take priority over all other activity. There are no “hot keys” activated to facilitate the correction of data.
Rural Development’s SDLC and CM process requires the ISSS to review system changes for security documentation updates and re-accreditation decisions impact to ensure that the system SORN is revised as needed.

TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

GUARANTEED is using technologies that are well established within the USDA.

32.1. How does the use of this technology affect citizens and employees privacy?

N/A

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO
THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE/CYBER SECURITY

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Guaranteed System

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

______________________________ 6/26/08
System Manager/Owner Date

Brenda Dinges ______________________________ 6/30/08
Brenda Dinges - Agency's Chief FOIA Officer Date

______________________________ 6/26/08
Agency OCIO Date