



UNITED STATES DEPARTMENT OF
AGRICULTURE

**Guaranteed
Rural Development
Privacy Impact Assessment (PIA)**

FOR OFFICIAL USE ONLY

Privacy Impact Assessment

For

Guaranteed

Guaranteed Loan System (GLS) Lender Interactive Network Connection (LINC)

Version 1.0

April 2007

FOR OFFICIAL USE ONLY

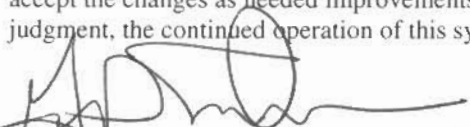
FOR OFFICIAL USE ONLY
Privacy Impact Assessment Authorization
Memorandum

I have carefully assessed the Privacy Impact Assessment for the Guaranteed System. This document has been completed in accordance with the requirements of the E-Government Act of 2002.

MANAGEMENT CERTIFICATION – Please check the appropriate statement.

- The document is accepted.
- The document is accepted pending the changes noted.
- The document is not accepted.

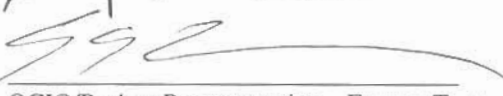
_____ **We fully** accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.



 System Manager – Greg Eschman

5-29-07

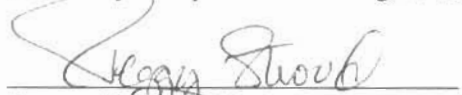
 DATE



 OCIO/Project Representative – Eugene Texter

5-29-07

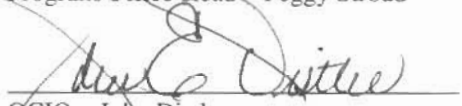
 DATE



 Program/Office Head – Peggy Stroud

6/6/07

 DATE



 OCIO – John Distler

6/6/07

 DATE



 Chief FOI/PA – Brenda Dinges

6/16/07

 DATE



 Senior Official for Privacy – Christopher L. Smith

6/6/07

 DATE

FOR OFFICIAL USE ONLY

Table of contents

A. CONTACT INFORMATION..... 1

B. SYSTEM APPLICATION/GENERAL INFORMATION 2

C. DATA IN THE SYSTEM 3

D. ATTRIBUTES OF THE DATA..... 5

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS 6

F. ACCESS TO THE DATA 8

APPENDIX A 11

APPENDIX B 13

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Name of Project: Guaranteed
Program Office: Rural Development
Project's Unique ID: 005-55-01-01-01-1050-00-402-124

Information System Name/Title	Guaranteed
System Acronym	Guaranteed
System of Records (SOR)	USDA / RD-SOR-1
System Type	<input type="checkbox"/> GSS <input checked="" type="checkbox"/> MA <input type="checkbox"/> GSS sub-system <input type="checkbox"/> MA individual application
Responsible Organization	USDA – Rural Development

A. CONTACT INFORMATION

1. Who is the person completing this document?

Name	Greg Eschman
Title	Chief, Guaranteed Loan Technology Branch
Address	1520 Market Street, Saint Louis, MO 63103
Email address	greg.eschman@stl.usda.gov
Phone Number	(314) 335-8503

2. Who is the system owner?

Name	Peggy Stroud
Title	Director, Enterprise Systems Design and Development Division
Address	1520 Market Street, Saint Louis, MO 63103
Email address	peggy.stroud@stl.usda.gov
Phone Number	314-335-8925

3. Who is the system manager for this system or application?

Name	Greg Eschman
Title	Chief, Guaranteed Loan Technology Branch
Address	1520 Market Street, Saint Louis, MO 63103
Email address	greg.eschman@stl.usda.gov

FOR OFFICIAL USE ONLY

Phone Number	(314) 335-8503
---------------------	----------------

4. Who is the IT Security Manager who reviewed this document?

Name	Gene Texter
Title	Information Systems Security
Address	Information Security Staff 1520 Market Street, FC-44 Saint Louis, MO 63103
Email address	Eugene.texter@stl.usda.gov
Phone Number	314-335-8104

5. Did the Chief FOI/PA review this document?

Name	Brenda Dinges
Title	Information Systems Security Project Mgr
Address	Information Security Staff 1520 Market Street, FC-44 Saint Louis, MO 63103
Email address	brenda.dinges@stl.usda.gov
Phone Number	314-335-8814

6. Did the Agency's Senior Office for Privacy review this document?

Name	Christopher L. Smith
Title	Rural Development DAA
Address	300 7th ST SW Washington DC 20024
Email address	ChristopherL.Smith@wdc.usda.gov
Phone Number	202-692-0212

7. Who is the Reviewing Official? (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).

Name	Christopher L. Smith
Title	Rural Development DAA
Address	300 7th ST SW Washington DC 20024
Email address	ChristopherL.Smith@wdc.usda.gov
Phone Number	202-692-0212

B. SYSTEM APPLICATION/GENERAL INFORMATION

Guaranteed is one of Rural Development's official accounting and financial management systems and supports Guaranteed and Direct Business & Industry program, Guaranteed and

FOR OFFICIAL USE ONLY

**Rural Development
Privacy Impact Assessment (PIA)**

FOR OFFICIAL USE ONLY

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 Under-writing System (GUS). It is a mission-critical system with a FIPS 199 security rating of "moderate."

1. Does this system contain any information about individuals?	Yes
(a) Is this information identifiable to the individual? (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, <u>the remainder of the Privacy Impact Assessment does not have to be completed past this section.</u>)	Yes
(b) Is the information about individual members of the public?	Yes
(c) Is the information about employees?	No
2. What is the purpose of the system/application?	Monitor Private Sector Lenders Portfolios for loans guaranteed by USDA and provide financial information on the guaranteed Portfolio
3. What legal authority authorizes the purchase or development of this system/application?	OMB Exhibit 300 authorizes the purchase or development of this system.

C. DATA in the SYSTEM

1. Generally describe the type of information to be used in the system and what categories of individuals are covered 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.
2. What are the sources of the information in the system?	The Loan application information is provided to Rural Development by Lenders for Guaranteed Loans and

FOR OFFICIAL USE ONLY

**Rural Development
Privacy Impact Assessment (PIA)**

FOR OFFICIAL USE ONLY

	by potential borrowers if requesting a direct loan. A RD Loan Officer or E-authenticated lenders complete the data entry screens.
(a). Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?	The source is from the individual.
(b). What Federal Agencies are providing data for use in the system?	USDA Rural Development and FSA loan officers provide for inputting application data. Trusted lenders provide for inputting guaranteed loan application data. We receive a file of banking data from Treasury via NITC monthly.
(c). What State and Local Agencies are providing data for use in the system?	No information is received from State or Local agencies.
(d). From what other third party sources will data be collected?	No data will be collected from third party sources.
(e). What information will be collected from the customer/employee?	Information included contains Social Security Numbers of Borrowers, Co-Borrowers, Key Members, and Lender Identification Numbers, debt payment information, client names, lender names, addresses, and business financial data.
3. Accuracy, Timeliness, and Reliability	
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	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.
3b. How will data be checked for completeness?	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.
3c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).	Yes, Reports are produced and reviewed for accuracy. Lenders are required to provide information on a monthly or quarterly basis.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

3d. Are the data elements described in detail and documented? If yes, what is the name of the document?	Yes , The Guaranteed Loan System Data Model
---	---

D. ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes. The data attributes provide loan processing information.
2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	Yes, various calculated financial data fields will be derived and stored in GUARANTEED.
3. Will the new data be placed in the individual's record (customer or employee)?	Yes, the data will be stored by borrower record/borrower identification.
4. Can the system make determinations about customers 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.
5. 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.
6. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	<p>Some data is consolidated based on requirements. However, rather consolidated or not the following controls are in place to protect our data.</p> <ol style="list-style-type: none"> 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

FOR OFFICIAL USE ONLY

	<p>transaction attempts are security logs/audit trails.</p> <p>4. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.</p> <p>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.</p> <p>6. Quarterly verifications reports are produced and required to be reviewed by the responsible Point of Contact (POC) based on the organizational unit.</p>
7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	Yes. The controls in 6 still apply.
8. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	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.
9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?	Varies reports are produced on the individuals loan or loan guaranteed which are used and accessed by Rural Development and Farm Service Agency employees.
10. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses and how individuals can grant consent.)	The GLS system contains edits to ensure mandatory data is collected. Some data elements are defined as optional.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1. If the system is operated in more than one site, how will consistent use of the system and data will be maintained in all	The system is hosted on a mainframe computer. Access is through user terminals, which are on the system. Any GLS components/data that are in Web
--	--

FOR OFFICIAL USE ONLY

**Rural Development
Privacy Impact Assessment (PIA)**

FOR OFFICIAL USE ONLY

sites?	Farm are balanced between the sites.
2. What are the retention periods of data in this system?	Indefinitely – repack upon request. However, data would be retrievable, if necessary, after any repack.
3. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	Once data is no longer needed, it is properly destroyed. Methods such as overwriting the entire media, degaussers, and disk formatting are used, but strict attention is paid to whatever process is selected to ensure that all unneeded data is destroyed. Papers and other soft materials, such as microfiche and floppy disks, are shredded.
4. Is the system using technologies in ways that the USDA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?	GUARANTEED is using technologies that are well established within the USDA.
5. How does the use of this technology affect public/employee privacy?	N/A
6. Will this system provide the capability to identify, locate, and monitor <u>individuals</u> ? If yes, explain.	Yes, but only so far as their user ID and passwords are uniquely provided and secured.
7. What kinds of information are collected as a function of the monitoring of individuals?	Basic name and address information, financial data along with data specific to the guaranteed loan.
8. What controls will be used to prevent unauthorized monitoring?	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.
9. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	GUARANTEED Operates under SOR Notice USDA/RURAL DEVELOPMENT - 1, System name: Applicant, Borrower, Grantee, or Tenant File.
10. If the system is being modified, will the SOR require amendment or revision? Explain.	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

FOR OFFICIAL USE ONLY

**Rural Development
Privacy Impact Assessment (PIA)**

FOR OFFICIAL USE ONLY

	<p>activity. There are no “hot keys” activated to facilitate the correction of data.</p> <p>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.</p>
--	--

F. ACCESS TO THE DATA

<p>1. Who will have access to the data in the system (E.g., contractors, users, managers, system administrators, developers, tribes, other)?</p>	<p>USDA RD and FSA GUARANTEED system users and managers, GUARANTEED Systems Administrators, and GUARANTEED Trusted Lenders.</p>
<p>2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?</p>	<p>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.</p> <p>Logbook entries are kept by the POC, Juanita Karels, of the Administrative Support Staff.</p> <p>The application uses UAMT.</p> <p>The Security – Greg Eschman reviews User Identification for Production GLS report.</p> <p>Yes, the GLS Application employs an automated mechanism for account management. It employs Log book entries.</p> <p>Temporary and emergency accounts are rare but both are terminated based on the expiration date established.</p> <p>UMAT authorizes the set-up of these accounts.</p>

**Rural Development
Privacy Impact Assessment (PIA)**

FOR OFFICIAL USE ONLY

<p>3. Will users have access to all data on the system or will the user's access be restricted? Explain.</p>	<p>No, users do not have access to ALL DATA on the system. Privileges granted are based on job functions and area of authority (e.g. State office user with authority for their state only).</p>
<p>4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?</p>	<p>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.</p>
<p>5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, are Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?</p>	<p>Yes, and yes there are privacy clauses included in the contract.</p>
<p>6. Do other systems share data or have access to data in this system? If yes, explain.</p>	<p>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</p> <p>The system utilizes input from the PLAS system and supplies input to the PLAS system through files during certain update cycles of the respective data bases. The system supplies a file to the RD data warehouse.</p>
<p>7. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface?</p>	<p>Greg Eschman 314-335-8503 greg.eschman@stl.usda.gov</p>
<p>8. Will other agencies share data or have</p>	<p>The other agencies that share/have access to</p>

FOR OFFICIAL USE ONLY

**Rural Development
Privacy Impact Assessment (PIA)**

FOR OFFICIAL USE ONLY

<p>access to data in this system (International, Federal, State, Local, And Other)?</p>	<p>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.</p>
<p>9. How will the data be used by the agency?</p>	<p>To create and process loan applications with USDA and trusted Lenders.</p>
<p>10. Who is responsible for assuring proper use of the data?</p>	<p>Greg Eschman 314-335-8503 greg.eschman@stl.usda.gov</p>

FOR OFFICIAL USE ONLY

APPENDIX A

DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the United States Department of Agriculture to the public and are the responsibility of all USDA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the USDA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of USDA data systems, processes and facilities.

All USDA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the USDA, the following Privacy Principles would guide the USDA:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.
Principle 4:	Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.
Principle 5:	Personally, identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 6:	Personally, identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.

FOR OFFICIAL USE ONLY

Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the USDA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any USDA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.
Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the USDA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

FOR OFFICIAL USE ONLY

APPENDIX B

POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The USDA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the USDA recognizes that compliance with legal requirements alone is not enough. The USDA also recognizes its social responsibility, which is implicit in the ethical relationship between the USDA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the USDA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the USDA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The USDA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. USDA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the USDA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the USDA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the USDA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.