



# Rural Development Privacy Impact Assessment

## Single Family Housing (Dedicated Loan Origination and Servicing System)

*July 2004*

*Prepared by:*



©USDA Security Department, December 2003

## Table of Contents

<b>USDA PRIVACY IMPACT ASSESSMENT FORM.....</b>	<b>3</b>
1. DESCRIPTION OF SFH: .....	3
2. DATA IN THE SYSTEM .....	4
3. ACCESS TO THE DATA.....	5
4. ATTRIBUTES OF THE DATA .....	7

# USDA PRIVACY IMPACT ASSESSMENT FORM

Project Name: Single Family Housing (SFH)

## 1. DESCRIPTION OF SFH:

The SFH Systems includes the Dedicated Loan Origination and Servicing System (DLOS), which consists of the Unifi Loan Origination System and the MortgageServ Servicing System, and the National Office Reserve Funds (NORF).

The SFH systems process borrower loan origination and loan servicing data. The UniFi loan origination system supports loan prequalification, loan application tracking, processing and closing activities. These activities are primarily handled by the field office staff. The MortgageServ loan servicing system, also referred to as DLOS, provides standard mortgage servicing processes, such as escrow accounts for taxes and insurance, forced placed insurance, pre-determined amortization schedules, and default management.

Internal users of the SFH Systems are the Centralized Servicing Center; the Office of the Deputy Chief, Financial Officer located in St. Louis, Missouri; National Office; and State and local servicing offices across the nation. External users include the U.S. Department of Treasury, U.S. Internal Revenue Service, Proctor Financial Insurance Company, credit bureaus, and commercial banks providing, tax services, forced place insurance, credit reports and lockbox services.

Borrower loan application data is input into a web-enabled loan origination system at local servicing offices located throughout the United States. The data is uploaded to a mainframe system during the nightly update. Loan servicing data is input into the system from PC's located in the Centralized Servicing Center in St. Louis, Missouri, and at State and local servicing offices across the nation.

The SFH System includes an online transaction entry and inquiry capability accessed by 800 field offices, the Centralized Servicing Center, National Office, and Finance Office. Updates are done both on-line real-time and through nightly batch processes. The Centralized Servicing Center is the primary user and the Finance Office has overall operational, financial, and accounting responsibility for Rural Development. Loan application data is input through the loan origination system at the local servicing offices and uploaded for the nightly batch update on the mainframe system. The loan servicing system maintained on the mainframe includes interfaces with the Digital Imaging System, U.S. Department of Treasury, credit bureaus, insurance vendors, and taxing authorities. SFH System functions include: online inquiry and transaction input, pre-application and application processing, loan making and loan servicing transaction updates, portfolio management, daily register, balancing, program reporting, and fiscal and financial reporting.

## 2. DATA IN THE SYSTEM

<p>1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.</p>	<p><b>Customer Information:</b> Borrower names, Social Security Numbers of Borrowers, Co-Borrowers, Key Members addresses, and business financial data, debt payment information, and tax and hazard insurance information.</p> <p><b>Employee Information:</b> Employee name, work area and teller number.</p> <p><b>Vendor Information:</b> Vendor Identification Numbers, Vendor names, and addresses.</p>
<p>2a. What are the sources of the information in the system?</p>	<p>The loan application information is provided to Rural Development by potential borrowers requesting a direct loan.</p> <p>The UniFi data entry screens are completed by the field office RD employees. The data is uploaded nightly into the MortgageServ system on the mainframe where it is available for loan servicing activities.</p> <p>Insurance vendors and taxing authorities are input by Centralized Servicing Center employees in St. Louis.</p>
<p>2b. What USDA files and databases are used? What is the source agency?</p>	<p>The loan origination system is a web based application developed on a Progress software platform, a proprietary software developed by MortgageServ. The software is maintained on the USDA Web-Farm servers located at St. Louis, Missouri, and is connected to the Agency intranet.</p> <p>The loan servicing system is maintained on an IBM mainframe platform at USDA's National Information Technology Center (NITC) in Kansas City, Missouri, utilizing Z/OS operating system.</p> <p>NORF is maintained on Dell servers within the secured environment of the computer room located at 1520 Market Street, St. Louis, Missouri. The NORF application was developed on a SQL server database and is operating in the Web Farm.</p> <p>Rural Development is the source agency for all data.</p>
<p>2c. What Federal Agencies are providing data for use in the system?</p>	<p>USDA Rural Development loan officers input loan origination and application data.</p>

	<p>Centralized Servicing Center inputs vendor information and loan servicing information.</p> <p>The Federal Bankruptcy Courts provides files with debtor bankruptcy notices via the Defense Automated Addressing System Center (DAASC).</p> <p>U.S. Department of Treasury provides files for certain delinquent management processes such as Treasury Office Program and Cross Servicing.</p>
2d. What State and Local Agencies are providing data for use in the system?	None.
2e. From what other third party sources will data be collected?	Proctor Financial Insurance Company provides forced place insurance information. Mellon Bank and U.S. Bank provide borrower loan payment information through lock box files. Transunion, Equifax and CBC Credit Bureaus provide credit reports and credit scores of potential and current borrowers.
2f. What information will be collected from the customer/employee?	Information included contains Social Security Numbers of Borrowers, Co-Borrowers, credit worthiness information, household information, and employment information.
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	Through daily system update and exception reports and daily audit reports.
3b. How will data be checked for completeness?	Same as 3a.

### 3. ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	USDA RD system users and managers, RD Systems Administrators. Access is given on a 'need-to-know' basis.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	<p>SFH system access is controlled by User ID and password. Access rights are granted to designated individuals only when a written request is approved by their supervisor, the site system manager, and the ISSPM.</p> <p>A behavioral set of rules has been established for this system and is enforced by an intricate network of user ID's and passwords, along with limited access to restricted areas. The rules of behavior have clearly defined the responsibilities and expected behavior of all individuals with access to the system. They include appropriate limits on interconnections to other systems and service provisions, along with restoration priorities.</p>

	<p>The rules are clear about the consequences of behavior not consistent with the rules. They are in writing and form a basis for computer security awareness activities and training.</p> <p>The Security and Employee Handbooks, which are provided to every employee cover those rules. Administrative and technical security controls are also reflected in the rules. Those rules are available to all the users prior to receiving authorization for access to the system.</p> <p>Managers and high-level technical staff are responsible for ensuring individuals comply with published rules of behavior. The roles and responsibilities of Rural Development employees are included in the Security and Employee Handbooks and RD Instruction 2006-Z, Information Systems Security.</p>
<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.</p> <p>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>	<ol style="list-style-type: none"> <li>1. 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.</li> <li>2. The controls used to detect unauthorized transaction attempts are security logs/audit trails.</li> <li>3. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.</li> <li>4. 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.</li> </ol>
<p>5a. Do other systems share data or have access to data in this system? If yes, explain.</p>	<p>The GSS Imaging System and GSS Automated Mail Process systems access the SFH system. These two systems are used to enhance the productivity of the SFH system by providing users the ability to view scanned paper documents and order system generated statements and other automated letters and documents.</p>
<p>5b. Who will be responsible for protecting the privacy rights of the customers and</p>	<p>Janet Havelka Chief, Rural Housing Services Branch (Single Family</p>

employees affected by the interface.	Housing) 314/335-8477
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	General Accounting Office (GAO), Office of Inspector General (OIG), National Finance Center (NFC).
6b. How will the data be used by the agency?	GAO has access only on an occasional, short-term basis for auditing. OIG has access for auditing. NFC has limited access for
6c. Who is responsible for assuring proper use of the data?	Janet Havelka Chief, RHSB(SFH) 314/335-8477

#### 4. 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.
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No.
2b. Will the new data be placed in the individual's record (customer or employee)?	Not applicable as there is no new data (see 2a)
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	Not applicable as there is no new data (see 2a)
2d. How will the new data be verified for relevance and accuracy?	Not applicable as there is no new data (see 2a)
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	<ol style="list-style-type: none"> <li>1. The applications capability to establish access control lists (ACL) or registers is by based upon the basic security setup of the operating system.</li> <li>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.</li> <li>3. The controls used to detect unauthorized transaction attempts are security logs/audit trails.</li> <li>4. Users are required to have password-protected screensavers on their PC's to prevent unauthorized</li> </ol>

	<p>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>
3b. 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 3a still apply.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	<p>Data is retrieved by SFH authorized users through login IDs using ACF2 IDs which are verified on the NITC Mainframe.</p> <p>UniFi users sign on through Windows 2000 Advanced Server Authentication residing on the UniFi Web Servers. Users use acf2 login.</p> <p>Norf users sign on through Windows 2000 Advanced Server Authentication residing on the Norf Server located in the WebFarm. Users use their acf2 login.</p>
4b. What are the potential effects on the due process rights of customers and employees of: consolidation and linkage of files and systems; derivation of data accelerated information processing and decision making; use of new technologies.	<p>The only employee data is the user id for audit trail purposes.</p> <p>There is no new technology impact that will effect due process rights of customers or employees.</p>
4c. How are the effects to be mitigated?	There are no effects to mitigate.

## 5. MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	SFH is used for Loan information processing only. There is no subjectivity or decision making based on an individual customer or employee by the SFH system.
2a. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	The system is hosted on a mainframe computer. Access is through user terminals which are on the system.
2b. Explain any possibility of disparate treatment of individuals or groups.	SFH is used for Loan data storing and processing only. There is no subjectivity or decision making based on an individual customer or employee by the SFH system.
2c. What are the retention periods of data in this system?	Loan history is retained on-line for 48 months. Tape backups of all data are stored for 15 years. Loan origination information is kept on the system for the life

	of the loan.
2d. 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 completely destroyed. Papers and other soft materials, such as microfiche and floppy disks, are shredded.
2e. 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?	Data integrity controls 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 refer to tests and evaluations used to determine compliance with security specifications and requirements.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No.
3b. How does the use of this technology affect customer/employee privacy?	To avoid costly retrofitting of safeguards, sensitivity was afforded importance early in the life cycle. The needs for information protection were established during the initiation, development, and operation phases, and will be afforded appropriate review when termination occurs. To ensure that adequate safeguards, alternatives, and rules are in place and implemented this system is reevaluated periodically.
4a. Will this system provide the capability to identify, locate, and monitor <u>individuals</u> ? If yes, explain.	No.
4b. Will this system provide the capability to identify, locate, and monitor <u>groups of people</u> ? If yes, explain.	No.
4c. What controls will be used to prevent unauthorized monitoring?	Audit trails.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	<b>USDA/RURAL DEVELOPMENT-1</b>
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	No. Modifications to the system will be recorded as part of the Configuration Management process and major revisions will be reflected in updates of the Certification and Accreditation documentation and, if deemed necessary, will trigger re-accreditation of the system.