# Privacy Impact Assessment

## (New Loan Originations)

**Rural Development (RD)**

- Date: August 2016
- Prepared for: RD

United States Department of Agriculture

| Document Revision and History | | | |
|---|---|---|---|
| **Revision** | **Date** | **Author** | **Comments** |
| 1.0 | 8/1/2016 | TGW | FY16 review/rolled up modules into parent PIA |

# Abstract

The USDA relies on its information technology systems, including the CLP Originations - New Loan Originations (New Loan Origination), to accomplish its mission of providing cost-effective and reliable services to the USDA, other Federal agencies, and the public at large. New Loan Origination consists of the following modules: **Broadband Application Information Log (BAIL), Broadband Search Application (BSA), Commercial Program Application Processing (CPAP), Construction Work Plan (CWP), DocFactory, Eligibility/Manager, Electronic Preliminary Engineering Report (ePER), GrantsUSDA (GIM), Guaranteed Underwriting System (GUS), National Office Reserve Funds (NORF), RepRequest (dev), RD Apply, UniFi, and VAPG**.

# Overview

New Loan Originations consists of:

- **Broadband Application Information Log (BAIL)**
- **Broadband Search Application (BSA)**
- **Commercial Program Application Processing (CPAP)**
- **Construction Work Plan (CWP)**
- **DocFactory**
- **Eligibility/Eligibility Manager**
- **Electronic Preliminary Engineering Report (ePER)**
- **GrantsUSDA (GIM)**
- **Guaranteed Underwriting System (GUS)**
- **National Office Reserve Funds (NORF**)
- **RD Apply**
- **RepRequest (dev)**
- **UniFi**
- **Value Added Producer Grants (VAPG)**

**BAIL** allows RD Broadband Division staff members to track loan applications from companies for the construction, improvement, and acquisition of facilities and equipment to provide broadband services to eligible rural communities.

**BSA** helps public users get information on broadband companies serving different rural communities across the nation and provides a snap-shot of broadband loan status across the country to RD executives and Congress.

**CPAP** processes WEP and CF loan and grant applications and sets up/modifies projects. CPAP also provides capabilities for environmental assessments and impact statements as well as underwriting capabilities that include loan determination and project funding breakdowns. CPAP is also used by RUS Electric and Telecommunication personnel to perform their daily tasks and maintains borrower details, associated documents for a borrower's account, tracks borrower loans/grants and funds, and provides relevant reports.

**Construction Work Plan (CWP)** provides applicants interested in receiving financial assistance from Rural Development (RD) the capability to submit a CWP online and receive an approval decision in less time than the processing work plans manually.

**DocFactory** implements an enterprise document assembly for a system and workflow that aids in the selection and assembly of appropriate documents using data from other systems and/or data retrieved via an interview process.

**Eligibility/Eligibility Manager** is an application whereby RD Housing Program staff, potential borrowers, and lenders can determine whether a property or prospective property address is inside or outside boundary of areas ineligibility for the Single Family and Multi-Family Housing Programs. Eligibility also provides employees, partners, and public with the capability to determine income eligibility of a potential SFH applicant via the Web and is based on the income limits for Single Family Guaranteed and Direct Housing Programs by county.

**ePER** provides engineers hired by potential applicants interested in receiving financial assistance from RD the ability to generate a preliminary engineering report to fulfill the federal requirements of the 1780-2 bulletin.

**GIM** provides USDA employees access to information and forms on a 24/7 timeframe to submission of specified Grant forms via the Internet, allowing Grant making agencies to process electronically submitted Grants more efficiently, automating the process of providing interaction through paper format and faxes.

**GUS** provides a streamlined and automated application process, automated credit decision-making, and automated the eligibility determination for the SFH guaranteed rural housing loan program.

**RD Apply** provides applicants interested in receiving financial assistance from RD the capability to submit an application online and receive a lending decision in less time than the processing applications manually.

**RepRequest (dev)** provides applicants interested in receiving financial assistance from RD the capability to submit an Authorized Representative Request (ARR) online and receive approval in less time than the processing of the ARR manually.

**NORF** includes the NORF Web Application which incorporates web pages for the State Offices to input requests for funds reserves from the National Office. The application also includes web pages for the State Offices to view the status of requests for funding, and pages for the National Office staff to view or process these requests.

**UniFi** is a loan origination application used by the USDA Service Centers for all phases of rural housing direct loan and grant origination, from prequalification to loan approval to loan closing.

**VAPG** is a mechanism to allow the Rural Development Business and Cooperative Programs staff to post Value-Added Grant applications to a web site so that both internal and external reviewers of the applications can download them in a secure way.

**Only the following systems require a PIA and will be evaluated in this document: CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), RD Apply, and UniFi.**

# 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?

**CPAP –** Information included contains Taxpayer Identification Numbers, address information, contact personnel, legal name, financial, and loan account information.

Customer data entered in this system includes all data required for completion of forms (pre-application and application) needed to process the obligation of the loan/grant. CPAP also provides capabilities for environmental assessments and impact statements as well as underwriting capabilities including loan determination and project funding breakdowns.

CPAP also maintains borrower details, associated documents for a borrower's account, tracks borrower loans/grants and funds, and provides relevant reports.

The system maintains audit log information by user identifications (IDs). These users are USDA employees and the system logs changes made in the system by the ID. CPAP is also used by personnel to perform their daily tasks, which includes tracking activities performed with and for the borrowers and keeping their itineraries.

**CWP** -

- Name and Address
- Customer ID
- RUS ID
- Construction Project Codes
- Environmental Classifications
- Required Attachments (Construction Work Plan, Approval Letters, Environmental Reports)
- Other information required for Construction Approvals in RD

**DocFactory –** The data to be processed by this application will be loan application documentation, along with all related requirements.

Information included contains Taxpayer Identification Numbers, address information, contact personnel, legal name, financial, and loan account information.

**ePER –**

- Name and Address
- Personal identification number (TIN, DUNS)
- Miscellaneous identification numbers (accounts, permits)

- Photographic image/identifying characteristics (Geographic information, U.S. Census track information)
- Other information that may be seen as personal: (Project Analysis, Alternative Project Proposals, and Service Area Information)

**GIM –**

Customer Information: Organization Name, Data Universal Numbering System (DUNS) ID, Key Contacts.

Employee Information: Name, eAuthID, phone numbers, agency

**GUS –**

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.

**NORF** - The NORF Web Application includes web pages for the State Offices to input requests for funds reserves from the National Office. The application also includes web pages for the State Offices to view the status of requests for funding and pages for the National Office staff to view or process these requests.

**RepRequest (dev) –**

- Legal Name
- TIN
- Program
- DUNS Nbr
- State
- County
- RUS ID
- Name
- Email
- eAuth ID
- Security Role
- POC Name
- ARR Contact Name
- ARR Contact Email
- ARR Contact Phone
- Required Attachments (Construction Work Plan, Approval Letters, Environmental Reports)

**RD Apply –**

- Name and Address
- TIN
- DUNS
- Financials
- Operating Reports
- Service Area Information
- Other information required to apply for credit subsidy in RD.

**UniFi –**

Customer Information: Borrow and co-borrower names, social security numbers, addresses, phone numbers, financial data, debt payment information, employment history, household information, date of birth, age, gender, marital status, credit score and tax and hazard insurance information.
Employee Information: Employee name, work area, and teller number

Vendor Information: Vendor names and addresses

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

**CPAP** - Application packet (application, financials, business plans and a feasibly study) data is *provided* by potential borrowers. Program Staff, Deputy Chief Financial Officer Staff, General Field Representatives, and Field Office users physically *enter* application and other data directly into the CPAP. Data is also provided and uploaded to the CPAP via files and stored procedures which *transfer/update* data to and/or from interface sources. Processing copies of the application packet data are/could be maintained on the USDA-RD intranet SharePoint server in a locked down directory to ensure that no unauthorized use could take place.

**CWP –**

- User supplied information
- BDMS
- CPAP
- ECF
- RD Apply

**DocFactory, ePER, RepRequest (dev)** – User supplied information

**GIM** - Personal Identifiable information is being collected electronically to remove the need for citizens to mail or fax grants information.

**GUS** - USDA RD, FSA loan officers, trusted lenders and monthly banking data files from Treasury via National Information Technology Center (NITC).

**NORF** - National and State Office Personnel input, review and approve Loan and Grant information into the system.

**RD Apply –**

- User supplied information
- BDMS
- CPAP
- BAIL
- ECF

**UniFi –** Applicants/Customers, Credit Reports, Employment Verification Reports, USDA Employees, and Vendors.

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

**CPAP** - Data is being collected to make available an automated means to provide a complete program management and financial information system for Rural Development direct loan and grant programs. Data will facilitate the processing by USDA personnel of applications, obligations, loans, and grants, on behalf of Rural Development customers. Data is also used for required reporting purposes to entities such as, U.S. Treasury, etc.

**CWP, ePER, RepRequest (dev), RD Apply** - The information being collected, used, and disseminated, or maintained is required through existing agency regulation regarding the act of requesting Federal Credit Subsidy and subsequent monitoring and reporting of Credit Subsidy requests.

**DocFactory** - This data is required in most states for filing purposes and is also necessary in order to keep track of the borrower’s corporate standing.

**GIM** - The information is collected to provide an electronic service for the customer.

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

**NORF** - The National Office makes a recommendation on the request, approves the request or denies the request. National Office can also modify, delete or add new fund sources.

**UniFi** - Data is used to process loan origination activities, including prequalification, application processing, underwriting, and loan closing.

## 1.4 How is the information collected?

**CPAP** - Application packet (application, financials, business plans and a feasibly study) data is *provided* by potential borrowers. Program Staff, Deputy Chief Financial Officer Staff, General

Field Representatives, and Field Office users physically *enter* application and other data directly into the system. Processing copies of the application packet data are/ could be maintained on the USDA-RD intranet SharePoint server in a locked down directory to ensure that no unauthorized use could take place. Data is also collected from interface sources which are uploaded to CPAP via files and stored procedures.

**CWP, ePER, RepRequest (dev), RD Apply** - Information is collected through a combination of structured system data loads and user supplied data collected through secure web pages.

**DocFactory –** Entered electronically by loan applicant.

**GIM** - The data represents an electronic service delivery channel that supplements existing business processes employed by USDA Grant making programs. Government staff review data submitted through this delivery channel for accuracy and completeness prior to accepting it for further processing. It removes the need for citizens to mail or fax available electronic interactions to these Grant making programs. Personal Identifiable information is being collected.

**GUS** - RD and FSA loan officers and trusted lenders provide input for guaranteed loan application data. RD receives a monthly file of banking data from Treasury via NITC.

**NORF** - Information is directly input into the system by National and State Officer Personnel.

**UniFi** - Through daily system updates, exception reports, and daily audit reports.

## 1.5 How will the information be checked for accuracy?

**CPAP** - The data will be verified through system screen edits and validations. Program Staff, Field Offices, and Finance Office Staff will periodically query the data in the system through standard reports (i.e., Data Warehouse, discrepancy, and daily obligation reports) to audit the system operation and input of data.

During development and testing phases of system enhancements and new functionality, business users/program staff will verify the newly developed and test results data.

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.

The system maintains audit log information by user identifications (IDs). Users are USDA employees and the system logs changes made in the system by their ID for auditing and control purposes.

**CWP, DocFactory, ePER, RepRequest (dev), RD Apply** - Information will be checked for accuracy through a combination of real time data validation and inspection of operational reports by authorized government personnel.

**GIM** - Manual inspection of Grant Application information by authorized USDA employees is leveraged to verify accuracy of that data set. Other system data sources are viewed as authoritative sources and maintain a separate verification process for the data they provide.

**GUS** - There are many balancing processes that execute with every batch update cycle to validate the data. Reports are for both New Loan Originations operational tables and data warehouse tables. Balancing is done against general ledger, allotment summary, and check disbursement. The Deputy Chief Financial Officer (DCFO) reviews these outputs daily.

**NORF** - Application software contains internal edits to ensure data integrity.

**UniFi** – Data is reviewed by area specialists.

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

Customer and employee information is protected by the following legal authorities:

- Privacy Act of 1974, as Amended (5 USC 552a);
- Computer Security Act of 1987, Public Law 100-235, ss 3 (1) and (2), codified at 15 U.S.C. 272, 278 g–3, 278 g-4 and 278 h which establishes minimum security practices for Federal computer systems;
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, which establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems;
- Freedom of Information Act, as Amended (5 USC 552), which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.
- The E-Government Act of 2002, 44 U.S.C. 3531 et seq.
- House Resolution 6124, also known as the Food, Conservation, and Energy Act of 2008 (Farm Bill).
- 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.

Overall risk is minimal; The NIST 800-53A controls for the Shared Services system are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls and Access Control (AC) controls are in place to limit and prevent misuse of data.
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.
2. Controls used to detect unauthorized transaction attempts are security logs/audit trails.

3. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.
4. Warning banners are used to warn and inform users who signs on to the system that this is a secure and private network. Warning banners are in compliance with USDA guidelines.
5. System Owners define access roles to ensure separation of duties and privileged access. Access to a system is requested and authorized via UAM, a ticket-oriented access tracking system that is utilized to gather the required documentation and authorization for each access assigned to an application. Each system has management units with an assigned POC that has been granted access to UAM. The POC has been delegated the authority to request access changes via UAM for management. Within UAM, the POC must define the type of access requested, completion of security training, Rules of Behavior Certification, Background Investigation completion and authorization. The UAMT processes the UAM access requests and responds directly back to the user. All changes to the access established must be coordinated through management and the POC. The user is required to have an Active Directory account established by ITS (e-mail) prior to submission of individual system access.

# 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.

**CPAP** - The principal purpose of the data being collected is to make available an automated means to provide a complete program management and financial information system for Rural Development's Commercial direct loan and grant programs. Data will also be used to meet Federal reporting requirements; e.g., Federal Funding Accountability and Transparency Act (FFATA) reporting requirements; and data is used to provide supporting documentation for determining level of risk of funds and repayment capability of borrowers (customers).

**CWP, ePER, RepRequest (dev), RD Apply** - Customer information is used in the process of applying for RD credit subsidy to assess initial eligibility and regulatory compliance regarding credit subsidy requests.

**DocFactory –** The data to be processed by this application will be loan application documentation, along with all related legal requirements.

**GIM** - To provide a single point of integration between USDA and Grants.gov for receiving and routing all Grant Applications submitted through the Grants.gov Apply service.

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

**NORF** - National and State Office Personnel input, review and approve information into the system.

**UniFi** - To provide loan servicing and support for all rural housing direct loans and grants, including delinquency servicing and risk management.

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

**CPAP, CWP, DocFactory, ePER, RepRequest (dev), RD Apply** - The data consumed, processed, and provided is analyzed by Subject Matter Experts (SMEs).

**GIM** - Manual inspection by RD government staff is used to analyze the data. No data is produced.

**GUS –** None.

**NORF, UniFi** - Application software contains internal edits to ensure data integrity.

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

**CPAP, CWP, DocFactory, GIM, GUS, NORF, RepRequest (dev) –** N/A.

**ePER, RD Apply** - The system uses Geographic Information System (GIS) base services providing US Census Track information as part of the loan application process.

**UniFi -** collects information from such sources as CBCInnovis, Employers, Taxing Authorities, Insurance Companies, and other vendors in order to make credit underwriting decisions.

## 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.

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.

Users must have a Level II eAuth ID and are uniquely identified with a user ID. The system maintains the identity of the user and links allowable actions to specific users.

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

The applications capability to establish access control lists or registers is based upon the basic security setup of the operating system.

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.

The controls used to detect unauthorized transaction attempts are security logs/audit trails.

Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.

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.

The National Institute of Standards and Technology (NIST) 800-53A controls for the New Loan Originations system are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1, 2, 3, 4, 5, 6, 7, 8, 12, 14, 17, 19, 20, 21, and 22), Identification and Authentication (IA-1, 2, 3, 4, 5, 6, and 7) and Systems and Communication Protection (SC-1, 2, 4, 5, 7, 8, 10, 12, 13, 17, 18, 20, 21, 22, 23, 28, and 39) controls are in place to prevent unauthorized access.

Authority to see any privacy data within the system is restricted to those users with National Office approval. This is a special authority added to a logon ID. Logon ID set up goes through UAMT.

# 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?

**CPAP, CWP, DocFactory, ePER, GUS, RepRequest (dev), RD Apply** – Information is retained indefinitely.

**GIM** - Information is only retained for the length of time to perform a process.

**NORF, UniFi** - Data is retained on the system for the length of the loan. The CTS web farm backs up data daily to tape. Tape backups of all data are stored for 15 years.

## 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.

**GIM** - There is not data retention beyond the time it takes to process the information.

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

**CPAP** – Since data is retained indefinitely there is minimal risk to the CPAP system. 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 which refer to tests and evaluations used to determine compliance with security specifications and requirements are in place.

**CWP, DocFactory, ePER, GUS, RepRequest (dev), RD Apply** - Risks associated with length of time data is retained have been reviewed. The mitigation strategy is to accept the risk.

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.

Copies of the application packet paperwork which includes PII information are maintained either in hard copy at each state’s office or electronically in an encrypted file on a USDA-RD intranet SharePoint server.

**GIM** - Minimal risk associated, since there is not data retention beyond the time it takes to process the information.

**NORF, UniFi** - At the end of the retention period, data is properly destroyed. Methods such as overwriting the entire media, degausses, 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.

## 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?

**CLP Shared Services (BI) –** CPAP and RD Apply send reporting information to TDW.

**Commercial Loan Servicing System (CLSS)** – CPAP transmits data needed to process obligations / de-obligations into PLAS during the nightly update.

**Common Call Component –** RD Apply and ePER provide data to ECF/Imaging for HUD total scorecard and loan approval recommendations.

**eForms –** UniFi provides data to populate forms that forwards data to agencies.

**GLS –** GUS sends data for GLS to process Lender Status Reports and Loan Closings.

**LoanServ -** UniFi data is used to update application information in the LoanServ loan servicing application.

### 4.2 How is the information transmitted or disclosed?

**CPAP -** Data is transmitted via files/automated stored procedures.

**ePER, RD Apply** - Once the information is transmitted using HTTPS to Electronic Customer File (ECF)/Imaging it is processed in association with the application being submitted via RD Apply.

**DocFactory, GIM, NORF –** N/A

**GUS** - The information is transmitted using HTTPS.

**RepRequest (dev) –** Information is transmitted using HTTPS to Informatica, TDW, and GDW.

**UniFi –** Information is transmitted to LoanServ and eForms via Network.

### 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:** Minimal risk since the data is transmitted internally.

**Mitigation:**

The NIST 800-53 controls are discussed in detail in the System Security Plan and specifically the System and Communication (SC) 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 implementation of RD ISSS NIST policies, standards and procedures.

**DocFactory –** Minimal risk, if any, associated; information is not shared

## 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?

**CPAP, CWP, DocFactory, ePER, NORF, RepRequest (dev), RD Apply –** N/A.

**GIM -** Grants.Gov: To deliver grant applicants with a simple, unified system through which applicants can search for funding opportunities, download grant opportunity packages and submit completed applications. Pay.Gov: payment, collection and cash management services to designated financial institutions and Federal Reserve Banks.

**GUS –** HUD, Fannie Mae, Ginnie Mae, SAVE; the data provided: State Code, County Code, I.D. Number, Loan Amount, Borrower Name & Address, City Name, State Abbr., Zip Code, Date of Loan Closing, Interest Rate, Lender ID, USDA Assigned Branch, and Lender Name & Address. The purposes are for the sharing of sensitive financial and privacy data. Ginnie Mae and Fannie Mae purchases mortgage backed securities. The expected benefits of the data sharing are:

- Validate Mortgage Backed Securities (MBS) pool data to include pool, investor, and Issuer furnished data
- Perform risk analysis of MBS Issuers
- Ensure that Ginnie Mae security holders are paid properly monitor the financial health and stability of Issuers

In addition, the data sharing will support HUD's goals of ensuring proper handling of sensitive data and or personally identifiable information (PII) from RD's systems.

**UniFi –** Equifax; The UniFi application is a loan origination system. In order to apply for an RD single family housing direct loan, a tri-merge credit report must be obtained for the applicant(s). An Infile credit report may also be requested for pre-qualifications. A request is sent from the UniFi production server to EMSWS then to the credit bureau server over a secure internet connection using Secure HTTP (HTTPS). Equifax returns a Tri-Merge/Infile credit report via an Internet API call to the secure web portal over HTTPS. The Tri-Merge/Infile credit report format is in the MISMO 2.3.x XML file data format that contains the applicant's credit history and credit scores, if available. This information is used to help determine eligibility for UniFi loan.

## 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.

**CPAP, CWP, DocFactory, ePER, NORF, RepRequest (dev), RD Apply –** N/A.

**GIM, GUS, UniFi** - Yes, under SORN Rural Development – 1 which is a shared artifact in CSAM.

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

**CPAP, CWP, DocFactory, ePER, NORF, RepRequest (dev), RD Apply –** N/A.

**GIM, GUS** – transmissions between the RD systems and the external systems is via SSL. Interconnection Service Agreement and Memorandum of Understanding agreements are in place in CSAM and maintained by the ISSS.

**UniFi** - uses Progress OpenEdge 10.0 database. A file is created and transmitted to the NITC mainframe at regular intervals using WS_FTP Pro v7.5.

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

**CPAP, CWP, DocFactory, ePER, NORF, RepRequest (dev), RD Apply** – N/A.

**GIM, GUS** – No risks to the privacy data; they are sent via SSL and signed Interconnection Service Agreement and Memorandum of Understanding agreements are in place in CSAM and maintained by the ISSS.

**UniFi** - Data files are exchanged for certain transactions associated with a loan via file transfer protocol (FTP). All external connections require an Interconnection Service Agreement (ISA) or Memorandum of Understanding (MOU).

## 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, SORN1 (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?

**CPAP, NORF** – N/A.

**CWP, DocFactory, ePER, GIM, GUS, RepRequest (dev), RD Apply, UniFi** – Yes.

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

**CPAP, NORF** – N/A.

**CWP, DocFactory, ePER, GUS, RepRequest (dev), RD Apply, UniFi** – Yes.

**GIM** - Individuals willingly participate in the application. Review and disposition determination of electronic grants submitted through Grants.gov.

## 6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

**CPAP, NORF –** N/A.

**CWP, ePER, RepRequest (dev), RD Apply** - No. The information required and how it will be used is documented in agency regulations.

**DocFactory** - All information collections require regulatory approval. The program regulations describe allowed usage.

**GIM** - Authorization to collect and use any data begins with the Regulatory authorization to do so. It is reviewed by parts of OMB when agencies are clearing information collections and disseminations.

**GUS –** Yes, Users have agreements to consent to the use of his/her data.

**UniFi** - No, RD410-4 indicates all possible uses of the information.

## 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.

**CPAP, NORF –** N/A.

**CWP, ePER, RepRequest (dev), RD Apply** - Notice is provided to applicants at the time of their application submission. It is during this process that the applicant has the opportunity to cancel the request.

**DocFactory** - it is an automated means to provide a complete program management and financial information system. There is no subjectivity or decision making based on an individual customer or employee by the system.

Notice is provided to the individual through the eAuth warning banner and the individual does have the option to decline to proceed. If the user declines no data is collected so there is no risk associated. If the user accepts, then they enter their own data so they are aware of what is being collected.

**GIM** - Individuals willingly participate in providing information for the completion of loan and grant requirements. Users complete privacy forms when they apply for loans or grants and consent to the use of their data before this information is provided.

**GUS –** Users have agreements to consent to the use of their data.

**UniFi** - RD410-4 is provided at the time of loan/grant application. If an individual doesn't sign the application it will result in the rejection of the loan/grant application. Applicants are aware of the collection of personal information.

# 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?

**CPAP, NORF –** N/A.

**CWP, ePER, RepRequest (dev), RD Apply** - information is open for edit to applicants up and until the point at which they submit the application to Rural Development. After submission, applicants would have to follow exiting agency procedures to request changes.

**DocFactory, GIM** - 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.

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

**GUS** - USDA RD and FSA system users and managers, systems administrators, and trusted lenders have access to the information.

**UniFi** - Individuals should be instructed to call customer service (800-414-1226) to verify information on their account, they can also apply for an eAuth account and Mortgage Account Information Access which will allow them to view their account on the web.

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

**CPAP, NORF –** N/A.

**CWP, ePER, RepRequest (dev), RD Apply** - Information is available for review and change by applicants up and until they submit the application for processing. Current procedures for correcting inaccurate or erroneous information are in place and would be leveraged after application submission. These processes are currently understood and used by applicants.

**DocFactory –** customer will need to manually correct the information.

**GIM, GUS** - 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 the Freedom of Information Officer:

Andrea Jenkins<br>
Freedom of Information Officer<br>
Rural Development, USDA 7th<br>
Floor, Reporter's Bldg.<br>
Washington, DC 20250<br>
Andrea.Jenkins@wdc.usda.gov<br>
(202) 692-0029

**UniFi** - Individuals should be instructed to call customer service (800-414-1226) to have changes made regarding incorrect information.

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

**CPAP, NORF** – N/A.

**CWP, ePER, ReqRequest (dev), RD Apply** - The agency regulations provide applicants notification of procedures to correct information.

**DocFactory** – customer is contacted via phone or e-mail.

**GIM** - Information is disseminated through annual POC training and users of PAD have the ability to update their information which is disseminated when they sign their consent form to use the service.

**GUS** – Information is disseminated through annual POC training.

**UniFi** - Field Office personnel will give the borrower the customer service number to call. The monthly billing statement also provides procedures for correcting their information.

## 7.4 If no formal redress is provided, what alternatives are available to the individual?

**CPAP, DocFactory, ePER, NORF, UniFi** – N/A.

**CWP, RepRequest (dev), RD Apply** - All formal and alternative processes for redress are part of existing agency regulation. The agency regulations provide applicants notification of procedures to correct information.

**GIM, GUS** - 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.

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), and RD Apply** - not affecting existing processes for redress and are not introducing any new risks requiring mitigation.

**UniFi** - Notification to the borrower that a telephone call may be recorded is provided at the onset of the call, notes are entered into the borrower account, and all employees are required to complete annual Information Security and Awareness training. The system uses before and after logging and audit logs to automatically record transactions to borrowers accounts.

## 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?

Generally, the National Institute of Standards and Technology (NIST) 800-53 controls for the CLP Originations, New Loan Originations system 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 Team (UAMT) relies on a POC supplying the correct UserID and password to UAM to identify themselves. 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. Guest and Anonymous accounts are not managed by ISS UAM Team. POCs (empowered by RD IT managers) are responsible for notifying UAMT if access or roles need to be modified and periodically reviewing and certifying established access.

**CWP, RepRequest (dev), RD Apply –**

***Loan Applicants***
requires USDA eAuthentication Level 2 assurance.

***Internal USDA RD Employees or Affiliates***
SAAR requests are submitted by Servicing Offices request access to the application and to establish the User's authority in the system. SAAR requests are entered by UAMT. Appropriate users lists are on file.

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

The applications capability to establish access control lists or registers is based upon the basic security setup of the operating system.

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.

The controls used to detect unauthorized transaction attempts are security logs/audit trails.

Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.

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.

**ePER** -

***Engineers***
ePER requires eAuthentication (eAuth) Level 2 assurance.

***Internal USDA RD Employees or Affiliates***
In future phases of the application, SAAR requests will be submitted by Servicing Offices request access to the application and to establish the User's authority in the system. SAAR requests are entered by UAMT. Appropriate users lists are on file.

## 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 section 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. All RD employees/contractors are required to complete ISAT training  on an annual basis.

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

Yes

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

RD has an Application Auditing and Monitoring Policy in place 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 Cyber Security Assessment and Management (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 is mitigated by 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.

NIST 800-53 controls are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls which are in place to prevent misuse of data. At a minimum the following information will be collected for each of the 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 security personnel 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 I c 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?

**CPAP** - This project is part of the Comprehensive Loan Program Investment which facilitates the processing by USDA personnel of applications, obligations, loans, grants, and collections on behalf of Rural Development Commercial Program customers.

**CWP, ePER, GIM, RepRequest (dev), RD Apply** - A CLP Framework program. The CLP Framework is a collection of open source frameworks and technologies.

**DocFactory** - Exari is a commercial, off-the-shelf (COTS) document assembly tool that will be used to build an enterprise solution (DocFactory) to automate the generation of agency documents.

**GUS –** A web 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.

**NORF** - A web application which includes web pages for the State Offices to input requests for funds reserves from the National Office. The application also includes web pages for the State Offices to view the status of requests for funding, and pages for the National Office staff to view or process these requests.

**UniFi –** The UniFi application is a loan origination system. In order to apply for an RD single family housing direct loan, a tri-merge credit report must be obtained for the applicant(s).

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

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), RD Apply, and UniFi** do 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 has been reviewed by all parties.

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

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), RD Apply** – N/A.

**UniFi** - This information is used to help determine eligibility for UniFi loan. .

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

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), RD Apply** – N/A.

**UniFi** - Borrower and co-borrower names, social security numbers, phone numbers, addresses, financial data, repayment information, and tax and hazard insurance information.

## 10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), RD Apply** – N/A.

**UniFi** - Proctor Financial Insurance Company provides forced place insurance information. U.S. Bank provides borrower's loan payment information through lock box files. Credit Bureaus provide credit reports and credit scores of potential and current borrowers. First American Real Estate Tax Service provides a file containing borrower real estate tax information as a service for some taxing authorities. U. S. Department of Treasury provides debtor and debt information for Treasury Offset Program and Cross Servicing processing.

## 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?

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), RD Apply** – N/A.

**UniFi** - It becomes a part of the borrower loan record, and is maintained/secured the same way as all information on the borrower account.

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

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), RD Apply –** N/A.

**UniFi -** Loan origination information is kept on the system for the life of the loan. Tape backups of all data are stored for 15 years.

***If so, is it done automatically?***

**UniFi** - Yes

***If so, is it done on a recurring basis?***

**UniFi** - Yes

## 10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest (dev), RD Apply –** N/A.

**UniFi** - USDA Rural Development system users and managers, Rural Development Systems Administrators, developers, analysts, and contractors, ITS System Administrators, developers and contractors.

## 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?

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest, RD Apply, UniFi –** N/A.

## 10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest, RD Apply –** N/A.

**UniFi** - No

## 10.10 Does the system use web measurement and customization technology?

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest, RD Apply –** N/A

**UniFi** - No

### 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?

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest, RD Apply, UniFi –** N/A

### 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.

**CPAP, CWP, DocFactory, ePER, GIM, GUS, NORF, RepRequest, RD Apply, UniFi –** N/A.

# Responsible Officials

TAMARA ORLET Digitally signed by TAMARA ORLET
Date: 2016.12.27 14:37:31 -06'00'

**Tamara Orlet**
**Chief, Management Services Technologies Branch**

MICHAEL SUTTON Digitally signed by MICHAEL SUTTON
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=MICHAEL SUTTON, 0.9.2342.19200300.100.1.1=12001000317363
Date: 2017.01.04 12:43:08 -06'00'

**Mike Sutton**
**Chief, Enterprise Technologies Branch**

KIMBERLY FRANKE Digitally signed by KIMBERLY FRANKE
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=KIMBERLY FRANKE, 0.9.2342.19200300.100.1.1=12001000272674
Date: 2016.12.30 07:44:56 -06'00'

**Kim Franke**
**Chief, Guaranteed Loan Technologies Branch**

Janet Havelka Digitally signed by Janet Havelka
DN: cn=Janet Havelka, o=Mortgage Loan Technologies Branch, ou=DCIO/ESDDD/MLTB, email=Janet.Havelka@stl.usda.gov, c=US
Date: 2016.12.29 15:20:42 -06'00'

**Janet Havelka**
**Chief, Mortgage Loan Technologies Branch**

# Approval Signature

EUGENE TEXTER Digitally signed by EUGENE TEXTER
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=EUGENE TEXTER, 0.9.2342.19200300.100.1.1=12001000317346
Date: 2016.12.30 10:53:21 -06'00'

**Diego Maldonado**
**Information Systems Security Program Manager**