Privacy Impact Assessment

CLP Support Applications: Support (CLP Support)

Rural Development (RD)

- Date: Dec. 2016
- Prepared for: RD

United States Department of Agriculture

Version: 1.4

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	9/8/2014	SAC	Original under CLP
1.1	7/19/2016	TGW	FY 16 review
1.1A	12/16/2016	TGW	Finalized PM review

Abstract

The USDA relies on its information technology systems, including the Support Applications (Support Apps), to accomplish its mission of providing cost-effective and reliable services to the USDA, other Federal agencies, and the public at large. It is made up of ten modules that include **Additional Project Reporting (APR), Broadband Collection Application System (BCAS), Civil Rights Applications (CRA), Data Collection System (DCS), FoxPro Loan Statistics (FoxPro), Lead Based Paint (LBP), Electric and Telecommunications Loan Statistics (LoanStats), Renewable Energy – Energy Efficiency (REEE), Socio-Economic Benefits Assessment System (SEBAS), and Self Help Automated Reporting and Evaluation System (SHARES).**

Overview

As previously mentioned in the abstract, CLP Support is divided into ten modules that include APR, BCAS, CRA, DCS, FoxPro, LBP, LoanStats, REEE, SEBAS, and SHARES.

NOTE: Only APR, CRA, DCS, REEE, SEBAS, and SHARES require a PIA and will be mentioned from this point forward.

APR: APR is a web based application that is used to collect data not available in source systems for reporting purposes. APR data collected is transferred to tabular data warehouse (TDW) and reports are hosted via Hyperion server and accessed via APR. Hyperion server, system generated emailed reports, etc.

CRA: Civil Rights Applications is a grouping of applications used by Rural Development to manage program discrimination complaints under the Monitoring Program Compliance application (MPC) and to manage Civil Rights complaints and compliance under the Civil Rights Reporting Application (PCRRA).

DCS: Automates financial and statistical report submissions by their borrowers, fulfilling the regulatory reporting requirement. These reports make the information available to the Utilities programs for analysis in connection with Government loan funds' security.

REEE: Application that helps RD–Business Cooperative Programs (RD/BCP) staff automate the collection, reporting, and distribution of Renewable Energy (RE) reports.

SEBAS: Program automates the collection, generation, analysis, and reporting of performance measurement data formulated by the economic model predicting the effectiveness of RD Business & Cooperative Programs' (BCPs') loan and grant programs in rural areas.

SHARES: A web-based database application designed to manage, track, evaluate and report on the status of the Self-Help Housing, Section 523 grant program as well as share this information with all parties that provide assistance to the program.

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?

APR: Borrower Name, Address and Case Number

CRA: Name, address, complainant contact information, complaint basis and issues, compliant status history; employee job title, contact information.

DCS: Customer Name and address

REEE: Customer Name.

SEBAS: Customer name and financial data (credit card numbers, bank account numbers, etc.).

SHARES: Borrower 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.

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

APR, CRA, DCS, REEE: USDA employees, contractors and the public.

SEBAS, SHARES: Data is retrieved by the entity id (non-profit organization id).

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

APR, DCS: Reporting purposes.

CRA: Information is used to investigate the complaint filed against RD.

REEE: Information is collected to help RD–Business Cooperative Programs (RD/BCP) staff automate the collection, reporting, and distribution of Renewable Energy (RE) reports.

SEBAS: Automates the collection, generation, analysis, and reporting of performance measurement data formulated by the economic model predicting the effectiveness of RD Business & Cooperative Program's loan and grant programs in rural areas.

SHARES: A system is designed to manage, track, evaluate and report on the status of the Self-Help Housing, Section 523 Grant program as well as share this information with all parties that provide assistance to this program.

1.4 How is the information collected?

APR: Information is entered in by customer.

CRA: Employees enter Complainant information and update complaint status.

DCS: DCS User, Borrower User and Partner User information is retrieved from CLSS.

REEE: A file is sent from the Guaranteed Loan System (GLS) nightly and updates the REEE system, there is no direct interface between the two applications.

SEBAS, SHARES:
1. The GRANTEE Module: Grantees enter date to help them manage and track the grant information
2. The Contractor Module: enables the Technical and Management Assistance contractors to enter and track information on their monthly activities and expenses
3. County/District Office module allows the RD local and area offices to view and comment on the grantee information
4. The State Office Module allows RD State Offices to view and comment on the grantee information
5. A National Office Module allows the National Office to review and analyze all data, reports, and comments submitted by the grantees, contractors, and the RD Field Office Staff.

1.5 How will the information be checked for accuracy?

CRA: Contact information is verified when Civil Rights staff contacts the party to verify their data; data validation, required fields, reports.

REEE: Information is checked through REEE which is protected by USDA eAuth.

APR, DCS, SEBAS, SHARES: Application software contains internal edits to ensure data integrity.

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

Consolidated Farm and Rural Development Act (7 U.S.C. 1921 et. seq.) and Title V of the Housing Act of 1949 as amended (42 U.S.C. 1471 et. seq.).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Overall risk is minimal; The NIST 800-53 controls for the Shared Services system are discussed in detail in the System Security Plan.

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. .

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.

CRA: Information is used to investigate the complaint filed against RD.

REEE: Information is collected to help RD–Business Cooperative Programs (RD/BCP) staff automate the collection, reporting, and distribution of Renewable Energy (RE) reports.

APR, DCS, SEBAS, SHARES: Reporting purposes only.

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

CRA, REEE, SEBAS:

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

APR, DCS, SHARES: Reports only

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

CRA, REEE: N/A.

APR, DCS, SEBAS, SHARES: Reporting purposes only.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The National Institute of Standards and Technology (NIST) 800-53 controls for the CLP Support Applications: Support 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. The Authority and Purpose (AP-1 and 2), Accountability, Audit, and Risk Management (AR-1, 2, 3, 4, 5, 6, 7, and 8), Data Quality and Integrity (DI-1 and 2), Data Minimization and Retention (DM-1, 2, and 3), Individual Participation and Redress (IP-1, 2, 3, and 4), Security (SE-1 and 2), Transparency (TR-1, 2, and 3), and User Limitation (UL-1 and 2) controls are in place to protect privacy.

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.

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

Safeguards are in place in the system to protect lenders personal information from unauthorized use and/or access.

Section 3.0 Retention

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

3.1 How long is information retained?

APR, CRA, DCS, REEE, SEBAS: Information is retained indefinitely.
SHARES: Data is retained on the system for the length of the loan. The NITC 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.

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

Risk:

SHARES: Data is retained for the length of the loan, however, there is minimal risk to the SHARES 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.

APR, CRA, DCS, REEE, SEBAS: Data is retained indefinitely, however, there is minimal risk to the APR, CRA, DCS, REEE, and SEBAS systems. 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.

Mitigation:

APR, CRA, DCS, REEE, SEBAS, SHARES: Data is stored in a secure environment and the system is behind the USDA secure network infrastructure. The application is behind eAuthentication (eAuth) with a Level 2 access authority. Users of the system are required to complete security awareness training prior to accessing the system and annually thereafter.

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?

APR: TDW, Hyperion (APR data collection is transferred to TDW/Hyperion for reporting purposes)

CRA, SHARES: N/A.

DCS: CLSS (DCS User, Borrower User and Partner User information is retrieved from CLSS for reporting purposes)

REEE, SEBAS: Loan and grant funding data is imported from GLS; REEE receives data files from Guaranteed and provides reports for senior managers, executives, and the RD Under Secretary, SEBAS is for reporting purposes only.

4.2 How is the information transmitted or disclosed?

CRA, SHARES: N/A.

APR, DCS, REEE, SEBAS: Information is transmitted to other internal system 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.

CRA, SHARES: N/A.

APR, DCS, REEE, SEBAS:

Risk: Minimal risk since the data is securely 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.

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?

N/A – Data is not shared with external organizations.

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.

N/A

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

N/A

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

N/A, data is not shared with external organizations, therefore no risk for external sharing.

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?

CRA, REEE: N/A.

APR, DCS, SEBAS, SHARES: Yes

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

CRA, REEE: N/A.

APR, DCS, SEBAS, SHARES: Yes

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

APR, CRA, DCS, REEE: N/A.

SEBAS: Yes, users can opt out of bulk email; no sharing of information outside of application exists.
SHARES: Yes, data is received from Guaranteed, and those users have agreements to consent to the use of his/her data.

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.

APR, CRA, DCS, REEE: N/A.

SEBAS, SHARES: Yes, data is received from Guaranteed, and those users have agreements to consent to the use of his/her data.

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?

APR, CRA, DCS: N/A.

REEE: 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.

SEBAS, SHARES: 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).

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

APR, CRA, DCS: N/A

REEE: REEE utilizes data from the Guaranteed Loan System (GLS), there is no direct interface between the two applications.

SEBAS, SHARES: Access is controlled by User ID and password. Access rights are granted to designated individuals only when their supervisor or the site system manager approves a written request. Privileges granted are based on job functions and area of authority (e.g. State office user with authority for their state only).

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

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

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

APR, CRA, DCS, REEE: N/A.

SEBAS, SHARES: Information is disseminated through annual POC training.

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

APR, CRA, DCS, REEE: N/A.

SEBAS, SHARES: 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.

APR, CRA, DCS, REEE: N/A.

SEBAS, SHARES: No additional risks are associated with the redress process.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

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).

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.

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 – see paragraph 8.1.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

USDA RD requires annual Information Security Awareness Training (ISAT) for all employees and contractors. RD is responsible for ensuring all new employees and contractors have taken the Department Security Awareness Training developed by OCIO-CS. Training must be completed with a passing score prior to access to a USDA RD system.

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

Yes, the current ATO is valid until 17 December 2017.

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?

APR is a web based application that is used to collect data not available in source systems for reporting purposes.
CRA consists of two applications to support USDA RD Civil Rights staff (National and State offices) activities.
DCS automates financial and statistical report submissions by their borrowers, fulfilling the regulatory reporting requirement.
REEE is a web application that helps RD/BCP staff automate the collection, reporting, and distribution of RE reports.
SEBAS automates the collection, generation, analysis, and reporting of performance measurement data formulated by the economic model predicting the effectiveness of RD Business & Cooperative Program's loan and grant programs in rural areas.
SHARES security environment is a fully functional, operational, and effective system. Agency testing and acceptance processes include validating the application security. This systems' platform is a HP-UX servers located within NITC Tier IV EDC in Kansas City, MO.

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

No, there are no privacy concerns related to the technologies used with **APR, CRA, DCS, REEE, SEBAS, or SHARES.**

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"?

System does not use 3rd party websites and/or applications.

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

System does not use 3rd party websites and/or applications.

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

N/A.

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

N/A.

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?

N/A.

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

N/A.

If so, is it done automatically?

If so, is it done on a recurring basis?

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

N/A.

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?

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)?

N/A

10.10 Does the system use web measurement and customization technology?

N/A

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?

N/A

10.12 <u>Privacy Impact Analysis</u>: 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.

N/A.

Responsible Official

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: 2017.02.15 14:55:32 -06'00'

Michael Sutton
Chief, Enterprise 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: 2017.02.17 12:07:04 -06'00'

Diego Maldonado
Information Systems Security Program Manager