Privacy Impact Assessment
Commercial Loan Servicing System (CLSS)

USDA – Rural Development

- Version: 1.0
- Date: January 13, 2022
- Prepared for: USDA Rural Development (RD)

United States Department of Agriculture

Privacy Impact Assessment for the

Commercial Loan Servicing System (CLSS)

January 13, 2022

Contact Point

RDPrivacy@usda.gov
Rural Development, Cyber Security Division
United States Department of Agriculture

Abstract

CLSS tracks and services the Rural Development's (RD's) Commercial direct loan and grant programs for electric, telephone, distance learning, broadband, cable television, water and environmental, and community facilities to process obligations, loans, grants, and payments for RD customers. CLSS provides program management and financial processing by interfacing to other internal RD applications. This PIA is required for CLSS because CLSS collects, stores, maintains, or disseminates Personally Identifiable Information (PII) and the PTA determined that a PIA is needed.

Overview

CLSS is an internal system used by authorized RD staff. Authorized RD staff access CLSS using eAuthentication (eAUTH). General Field Representatives (GFRs), Field Office Staffs, Program Staff, Servicing Office, Chief Financial Office, and RD Technology Office staffs access CLSS, internally via Hyper Text Transfer Protocol Secure (HTTPS) over the USDA Local Area Network (LAN) on the Digital Infrastructure Service Center (DISC) mainframe. CLSS provides program management and financial processing, utilizing current technology, and stores any generated reports. CLSS is an integrated system with interfaces to other internal RD applications.

CLSS processes approved Rural Electric and Telephone (RET) funds and Federal Finance Bank (FFB) funds to borrowers. Once funds have been advanced, the system bills RD borrowers, processes payment collections from the RD borrower, maintains payments, pre-payments and delinquent payments, manages irregular RD borrower situations, and other loan servicing actions. Additionally, this system handles deferments for Rural Development projects and Energy Resource Conservation loans directed toward electric borrowers.

The current functional components in CLSS are listed below:

Borrower Directory Management System (BDMS) is a web application that collects and maintains RD borrower information to support Rural Development's business processes for the RD commercial loan and grant programs. CLSS users enter borrower information, including full names, addresses, and bank account information, into this component.

Community Programs pulls in application data from Commercial Program Application Processing (CPAP) and transmits the required data to process obligations/de-obligations in the Program Loan Accounting System (PLAS) during the nightly update. PLAS is the financial System of Record for Water and Environmental Program (WEP) and Community Facilities (CF) loans/grants. The obligations/de-obligations results are processed or rejected from the nightly update, then they are sent back to CLSS and CPAP for updating.

Loan and Grant Management System (LGMS) processes web transactions for obligations/rescissions, advances/disbursements, and cancellations that interface with the Program Funds Control System, including notes and designation notices. The advances/disbursements are processed through an interface to the Automated Clearing House via the Digital Infrastructure Services Center (DISC) mainframe. LGMS also interfaces with

CPAP, the Guaranteed Loan System, Reconnect and HBIIP to obtain data to process the obligations in CLSS for selected loan/grant programs. Borrowers would be considered organizational entities.

Cash Application Module (CASH) is used to communicate with eServices Enterprise Cash Management System (ECMS) and allocate the cash receipts for the RUS transactions to the appropriate accounts for reporting to the General Ledger and Cash Tracking on the DISC mainframe. CASH collects the primary borrower ID or RUS ID.

RUS Loan Servicing (RLS) creates and maintains accounts receivable; calculates daily interest accrual and late fees; facilitates capitalization of interest, and usage of Cushion of Credit (CoC) funds; provides consolidated borrower quarterly statements and Rural Telephone Bank's (RTB's) audit confirmations; and performs billing, payment and collections services, and some specific loan servicing transactions.

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?

CLSS tracks RD customer commercial direct loan and grant programs through the borrowers' information in the database, including their Taxpayer Identification Number (TIN), Social Security Numbers (SSNs), address and contact information, full name, financial disposition, and bank and loan account information.

CLSS maintains Congressional Districts and Representative contact information (full name, address, email address, and telephone number); financial institution information, including bank routing, and contact information associated with the borrowers in the system; and Certified Public Accountant (CPA) firms responsible for the auditing of RD borrowers.

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

RD staff manually enter the information contained in an RD potential borrower's application packet into the CLSS application. The application packet, which is managed by RD staff for CLSS includes the application, financials, business plans and a feasibly study. Program Staff, Deputy Chief Financial Officer Staff, General Field Representatives, and Field Office users enter the application and related information directly into CLSS. Data is also provided and uploaded to CLSS via files from other USDA systems and stored procedures, which transfer and update data to and/or from internal RD components listed above.

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

Information is collected to provide automated program management and financial information for Rural Development's commercial direct loan and grant programs. RD collects this information to process applications, obligations, loans, grants, and collections for Rural Utilities customers. This information is also required for reporting purposes to the Internal Revenue Service (IRS) and related federal entities for financial compliance.

1.4 How is the information collected?

Program staff, Chief Financial Office, general field representatives, and field office users enter the application and related information directly into the CLSS system. Data is also collected from the following internal USDA systems: New Loan Originations: Commercial Program Application Processing (CPAP); Guaranteed Loan Servicing (GLS); Multi Family Integrated System (MFIS); Program Funds Control System (PFCS); Automated Mail Processing (AMP); Business Intelligence (BI): Tabular Data Warehouse (TDW); eServices: Enterprise Cash Management System (ECMS) and RD Utilities Program Customer Initiated Payments (RDUPCIP); RD Force: ReConnect and Higher Blends Infrastructure Incentive Program (HBIIP); Admin: Staff Review and Reporting System (SRRS); and Program Loan Accounting System (PLAS).

1.5 How will the information be checked for accuracy?

The data is verified by authorized RD staff with regular review and verification as part of the normal workflow for CLSS. Program Staff, Field Offices, and Finance Office Staff periodically query the data in the system using standard reports, such as Data Warehouse reports, discrepancy reports, and daily obligation reports, to audit the system and verify the data input. Data integrity controls protect the data from accidental or malicious alteration or destruction and provide assurance to the RD user that the data is valid.

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

Information in the CLSS application falls under the following:

- *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.*
- *Federal Information Security Modernization Act of 2014 (Pub. L. 113-283)*
- *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).*
- *Farm Bill 2018 (P.L. 115-334)*
- *Fair Credit Reporting Act, 15 USC 1681 a(f)*
- *Consumer Credit Protection Act, 15 USC 1601*
- *Equal Credit Opportunity Act, 15 USC 1691*
- *The Fair Debt Collection Practices Act, Pub. L 111-203, title X, 124, Stat. 2092 (2010)*
- *7 CFR, section 3560, subsections 55 and 154*
- *USDA Departmental Regulation (DR) 3080-001*
- *RD Records Management Policy – RD Instruction 2033-A*
- *NARA Records Retention – General Records Schedules*

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

The privacy risk is the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the RD customer.

The CLSS system owner defines access roles to ensure separation of duties, account management and authorized access to data and information in CLSS, which is on the intranet and hosted by DISC. Only authorized RD staff can access the CLSS application using eAuthentication via HTTPS over the USDA LAN. These measures mitigate the risks to privacy data in CLSS. Since CLSS is hosted on the DISC platform, it complies with all security and privacy protections required by USDA as a federal agency. See the System Security Plan (SSP) for the security controls.

Section 2.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

CLSS provides for the effective management and maintenance of loans and grants for RD customers, including facilitating the financial and business processes necessary for loan and grant management. CLSS collects this information to process applications, obligations, loans, grants, and collections for Rural Utilities customers, and stores any generated reports. In addition, the system provides financial processing, which includes billing RD borrowers; processing payment collections from the RD borrower; maintaining payments, pre-payments, and delinquent payments; managing irregular RD borrower situations, and other loan servicing actions. Additionally, this system handles deferments for Rural Development projects and Energy Resource Conservation loans directed toward electric borrowers. Data is used to meet federal reporting requirements with the IRS and Federal Funding Accountability and Transparency Act (FFATA).

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

Tools are not used with CLSS. Authorized RD Program Staff, Field Offices, and Finance Office Staff manually review and verify the RD applicant/customer information in the system with data warehouse, discrepancy, and daily obligation reports. CLSS data stored in the system can be queried in a report for authorized RD staff to verify the accuracy of the data.

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

Not applicable, CLSS does not use commercial or publicly available data.

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 controls in place to detect unauthorized access to CLSS information or transactions include DISC audit logs/security logs. There are logs for eAuthentication, which is how the authorized RD staff identify and authenticate to access CLSS on the DISC platform.

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?

All information will be retained in compliance with National Archives and Records Administration (NARA) Guidelines, according to the NARA General Records Schedules (GRS) and RD 2033-A, Management of Rural Development Records.

The SORN RD-1, *Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Program,* specifies policies and practices for retention and disposal of Rural Development's records.

In addition, CLSS information is retained in accordance with financial compliance regulations.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, CLSS follows data retention as provided by the RD Records Management in RD 2033A-Management of Rural Development Records, which is in accordance with NARA.

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

CLSS data retention has the potential risk of unauthorized access, unauthorized disclosure or illegal use of the customer PII data.

CLSS data is protected by the DISC mainframe, which follows USDA federal agency requirements for data protection and is accredited by FedRAMP. CLSS follows the RD Records Management data retention requirements to manage risk associated with data retention. In addition, access to the data is controlled by designated administrators.

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?

CLSS is an integrated system with interfaces to other internal RD applications facilitating RD program management and financial processing of loans and grants. It is on the RD intranet and authorized RD staff use eAuthentication to identify and authenticate before accessing CLSS.

Guaranteed Loan System (GLS) receives the lender account receivables data from CLSS when a disbursement occurs in LGM.

MFIS launches the CLSS application in a separate browser window populated with the tenant pseudo-SSN. MFIS can view specific account data in CLSS vis a secured DB view.

CLSS sends a monthly SFTP file of loan and borrower data to Business Intelligence (BI) Tabular Data Warehouse (TDW) for Federal Assistance Award Data System/Federal Funding Accountability and Transparency Act (FFATA) reporting,

CLSS sends a nightly SFTP file of loan information, including the borrower's full name, to Automated Mail Processing (AMP) for processing and printing by AMP.

CLSS sends a nightly SFTP file of loan advance request data to Program Funds Control System (PFCS) to process and approve automated clearing house (ACH) advances/disbursement requests that are sent to Treasury by PFCS.

CLSS receives a nightly, SFTP file to New Loan Originations (NLO) Commercial Program Application Processing (CPAP) of loan and borrower data to process obligations/de-obligations

CLSS sends a borrower file via SFTP that includes borrower's full name, amount of debt, date of debt, address, Lender's name, and Taxpayer Identification Number (TIN) to CLP Support-Administration (Admin). Data feed between CLSS and Admin occurs with Admin's Staff Review and Reporting System (SRRS) to obtain loan audit information of borrowers by CPA firms. SRRS sends a flat text file back to CLSS with audit and financial review data on borrowers.

CLSS receives nightly cash receipts/collections information from eServices' ECMS for application to loan accounts, which provides the borrower's full name. RUS Borrowers access the RDUPCIP application, which ECMS interfaces. ECMS performs the transfer of funds to CLSS. Borrowers input the borrower's full name, bank account and routing number, and RUS ID into RDUCPCIP and ECMS sends over the borrower's full name only to CLSS.

CLSS receives grant request data for subsequent obligation and execution of funding for business applicant users from RD Force's Higher Blends Infrastructure Incentive Program (HBIIP) using Mulesoft restful services. ReConnect, a component in RD Force, received the borrower Data Universal Numbering System (DUNS) number from CLSS in a nightly SFTP file.

4.2 How is the information transmitted or disclosed?

CLSS receives and send data to the following applications: Admin, NLO, PFCS, AMP, and TDW through SFTP files on a nightly basis. Community Programs pulls in application data from SQL Server DB procedures from CPAP and transmits via flat file the required data to process obligations/de-obligations in the Program Loan Accounting System (PLAS) during the nightly update and online real-time. GLS data is pulled in using DB2 procedures via online real-time processed. Mulesoft Restful services on GOVCLOUD also receive data from HBIIP for processing obligations and sends obligation data to Reconnect for reporting purposes. Data from the RLS, CASH, and LGMS schemas are extracted for use in the Data

Warehouse on a nightly basis. DISC provides the security protections to the data as it flows in CLSS. DISC follows USDA security requirements to protect the data in the CLSS and as it flows internally.

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.

Privacy risks include the potential compromise of PII data with CLSS. The risk associated with the sharing of the data is minimal, as access to the data is controlled by designated administrators, utilizing eAuthentication to identify and authenticate the users, and audit logs of user activity. In addition, the risk is mitigated by DISC security protections in place for CLSS, since it is hosted on the DISC platform.

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?

CLSS is reporting commercial loan information to Dunn & Bradstreet on a quarterly basis. Information is shared with a one-way bulk data exchange via Secure File Transfer Protocol (SFTP). Dunn & Bradstreet employees do not have direct access to CLSS. CLSS sends the borrower or co-borrower's full name, Lender name, address, date of report, account number, Taxpayer Identification Number (TIN), Federal agency with program code, and debt information to Dun & Bradstreet.

Experian Credit Bureau gets data files transferred from CLSS using Linux GPG encryption protocols for credit bureau reporting under the Fair Credit Reporting Act (FCRA). The data files shared with Experian are for reporting commercial loan information. All data files transferred to Experian are via SFTP.

Equifax eReporting Credit Bureau receives information needed for credit reports and scores from CLSS using Linux GPG encryption protocols. CLSS will be reporting commercial loan information to Equifax on a quarterly basis. All data files transferred to Equifax are via SFTP.

National Rural Utilities Cooperative Finance Corporation (NRUCFC) automatically transfers to CLSS files which contain a breakout of borrower and payment amounts from NRUCFC payment processing. RD customers of RUS loans send payments to NRUCFC. NRUCFC sends the bulk payment to Treasury Department, which then passes that data through RDs

Enterprise Cash Management Services (ECMS) system like all other payments. NRUCFC then sends a breakdown by subsidiary/borrower of that bulk payment so CLSS can apply it to Receivable Accounts correctly. The files could contain the following information: Taxpayer Identification Numbers (TIN), debt payment information and mailing addresses. RD maintains an ISA with NRUCFC for the sharing of the data.

Fiscal Service Treasury Web Application Infrastructure (TWAI) provides debtor and debt information for Treasury Offset Program and Cross Servicing, which is done for federal agencies. The interconnection agreement allows for the sharing of federal financial information as well as Privacy Act data between TWAI and USDA agencies, including RD. TWAI is a trusted source for RD and RD maintains an ISA with TWAI for the sharing of the data.

The commercial loan servicing branch in Chief Financial Office and Servicing Offices receives a well-formed XML file daily from Federal Financing Bank (Department of Treasury) via email and CLSS has an upload page. The XML must be well formed in a predetermined format and the data is then staged and matched to LGMS Advances and RLS Accounts. FFB disburses the funds that USDA then services and this File is how we get the payment schedules and verify disbursements. When rejections occur, FFB and the user community manually figure out the differences and we receive a new file.

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.

Yes, System of Record Notice (SORN) USDA/Rural Development 1, *Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs* covers the routine use of this information with the organizations listed in 5.1, Dunn & Bradstreet, Experian Credit Bureau, Equifax Credit Bureau, NRUCFC and Treasury. These external entities are trusted sources for RD. CLSS does not share personally identifiable information outside the Department, other than to the organizations listed in 5.1.

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

Data is sent to the above trusted sources over a Virtual Private Network (VPN) and limited to specific server Internet Protocol (IP) addresses using Secure File Transfer Protocol (FTP) with the security and privacy protections that DISC has in place following USDA requirements.

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

Privacy risks include the potential compromise of PII and sensitive financial information. This is mitigated by the security protections, such as firewalls, Domain Name System Security Extensions (DNSSec), encryption of data in transit, VPN, and audit logs. Authorized RD staff access CLSS using eAuthentication and RD has continuous monitoring from DISC in compliance with Federal Information Security Modernization Act (FISMA) and as required by RD and USDA. CLSS data is stored in a secure environment on the DISC platform. An ISA is in place between USDA RD (CLSS) and each of the organizations listed in 5.1, documenting the connections and sharing of data between the systems and how the security of the two systems will be maintained.

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, it follows Rural Development-1, *Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants and Other Participants in RD Programs*, https://www.govinfo.gov/content/pkg/FR-2016-04-28/pdf/2016-09938.pdf but it is an internal application on the RD intranet, so it is not accessible by the general public.

6.2 Was notice provided to the individual prior to collection of information?

Notice was provided to individuals by the initial source systems prior to collection or processing of the information. CLSS is used internally by authorized RD staff, so it is not available by the public, and it is not involved in the initial collection of information from individuals.

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

Notice of opportunity and/or right to decline to provide information was provided to individuals by the initial source systems prior to collection or processing of the information. CLSS is used internally by authorized RD staff, so it is not accessible by the public, and it is not involved in the initial collection of information from individuals.

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

Consent of the individuals for particular uses of the information would have been obtained by the initial source systems, if required, prior to collection or processing of the information. CLSS is used internally by authorized RD staff, so it is not accessible by the public, and it is not involved in the initial collection of information from individuals.

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.

Notice was provided to individuals by the initial source systems prior to collection or processing of the information. The initial assessment of privacy risk would be performed by the administrators who manage the data at its collection.

Individuals do not have direct access to the system as users. Notice of the purposes and uses for the collection of the information is provided in the SORN RD-1.

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?

The public does not have direct access to CLSS; all data is received by USDA personnel from the original source components.

Individuals are notified of the procedure to gain access to their information in the Record Access Procedures section as outlined in the SORN RD-1. Record Access Procedures: Any individual may request information regarding this system of records or determine whether the system contains records pertaining to him/her, from the appropriate System Manager. If the specific location of the record is not known, the individual should address his or her request to:

Rural Development, Freedom of information Officer, United States Department of Agriculture, 1400 Independence Avenue SW, Stop 0742, Washington, DC 20250–0742. A request for information pertaining to an individual must include a name; an address; the RD office where the loan or grant was applied for, approved, and/ or denied; the type of RD program; and the date of the request or approval.

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

The public does not have direct access to CLSS; all data is received by USDA personnel from the original source components.

Individuals are notified of the procedure to gain access to and contest their information in the Record Access Procedures section as outlined in the SORN RD-1. See Record Access Procedures information in 7.1.

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

The public does not have direct access to CLSS; all data is received by USDA personnel from the original source components.

Individuals are notified of the procedure to gain access to and contest their information in the Record Access Procedures section as outlined in the SORN RD-1. See Record Access Procedures information in 7.1.

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

Individuals are notified of the procedure to gain access to and contest their information in the Record Access Procedures section as outlined in the SORN RD-1. See Record Access Procedures information in 7.1.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

No additional risks are associated with the redress process. The requestor may also refer to the SORN RD-1 for additional information regarding Record Access Procedures.

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 User Access Management (UAM) Team process for establishing, activating, and modifying individual users for CLSS. The group and account types are defined by the System Owner for CLSS. The System Point of Contact (POC) assigns group membership and determines individual RD user access. The UAM Team creates, modifies and deletes user requests approved by the System Point of Contact.

RD employees and RD contractors' access CLSS after being provisioned in eAuthentication by a User Access Management (UAM) ticket, created by the System Point of Contact (POC) and completed by the UAM Team (UAMT).

Steps to provision RD employees and RD contractors follow desk procedures as set by the system owner for CLSS.

8.2 Will Department contractors have access to the system?

Yes, RD contractors are required to undergo the same access and authentication procedures that RD federal employees follow, as 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?

Yes, all RD employees and contractors are required to complete annual information security and awareness training, which includes privacy training for CLSS.

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

Yes, CLSS has an ATO, which is valid until 12/05/2025.

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

CLSS complies with the Federal Information Security Modernization Act of 2014 (FISMA) by documenting the Authorization and Accreditation, annual control self-assessments, and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 4. These controls, including full compliance, inheritance, and risk acceptance descriptions, are available in CSAM . CLSS is hosted on the DISC platform at USDA, which is FedRAMP certified and follows USDA security and privacy requirements.

Access to CLSS is controlled through eAuthentication for authorized CLSS users, and access to sensitive information is controlled through DISC Profiles/Groups on a need-to-know basis with audit logs of user activity for CLSS. Section 5 of this PIA describes security protections in place for CLSS data.

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?

A privacy risk associated with CLSS could be extracting and using the information erroneously. Since CLSS is used by authorized RD staff using eAuthentication and there are group access management controls, the privacy risks are minimal. Potential compromise of privacy data is mitigated by DISC audit event monitoring and USDA network security protections in place to protect RD data for CLSS on the DISC platform.

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?

CLSS, hosted on the DISC platform at USDA, was developed to replace the RUS Legacy System. CLSS tracks and services the Rural Development's commercial direct loan and grant programs for electric, telephone, distance learning, broadband, cable television, water and environmental, and community facilities to process obligations, loans, grants, and payments for RD customers. The system provides program management and financial processing, utilizing current technology, and stores any generated reports. CLSS is an integrated system with interfaces to other internal RD applications. It is on the RD intranet and authorized RD staff use eAuthentication to identify and authenticate before accessing CLSS.

For all technologies chosen by RD, an Analysis of Alternatives (AoA) is completed to determine which technologies will be selected and ultimately purchased or built.

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

No, the project utilizes Agency approved technologies for CLSS, and these technology choices do not raise privacy concerns. CLSS is hosted on the DISC platform at USDA.

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, the system owner and the ISSPM have reviewed the OMB memorandums.

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

Not applicable, CLSS does not use 3rd party websites or applications.

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

Not applicable, CLSS does not use 3rd party websites or applications.

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

Not applicable, CLSS does not use 3rd party websites or applications.

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?

Not applicable, CLSS does not use 3rd party websites or applications.

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

Not applicable, CLSS does not use 3rd party websites or applications.

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

Not applicable, CLSS does not use 3rd party websites or applications.

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?

Not applicable, CLSS does not use 3rd party websites or applications.

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)?

Not applicable, CLSS does not use 3rd party websites or applications.

10.10 Does the system use web measurement and customization technology?

No, CLSS does not use web measurement and customization technology.

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?

Not applicable, CLSS does not use web measurement and customization technology.

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.

Not applicable, CLSS does not use 3rd party websites or applications.

Approval Signature

Signed copy kept on record