Privacy Impact Assessment

Commercial Loan Servicing System (CLSS)

Rural Development (RD)

- August 2017
- Prepared for: RD

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	9/8/2014	SAC	Original under CLP
1.1	7/15/2016	TGW	FY 16 review
1.2	11/22/16	TGW	FY17 signature
1.2	8/22/2017	SAC	FY18 review, updated interconnections

Abstract

CLSS tracks and services the Rural Development's (RD) Commercial direct loan and grant programs' (e.g., electric, telephone, distance learning, broadband, cable television, water and environmental community facilities) borrowers, obligations, loans, grants, and payments.

Overview

CLSS tracks and services the RD's Commercial direct loan and grant programs' (e.g., electric, telephone, distance learning, broadband, cable television, water and environmental, community facilities) borrowers, obligations, loans, grants, and payments. The system will provide a complete program management and financial information system, utilizing state-of-the-art technologies. CLSS will be a totally integrated system with seamless interfaces to other agency systems.

CLSS is replacing the RUS Legacy System which maintains accountability and provides authorization for advancing approved funds to borrowers. Once funds have been advanced, the system bills borrowers, processes payment collections from the borrower, maintains payments, prepayments and delinquent payments, and manages irregular borrower situations, and other various 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 that are utilized in CLSS production are listed below:

Borrower Directory Management System (BDMS) component provides a foundation on which to build a web-enabled application that gathers and maintains borrower information and supports Rural Development's loan and grant business processes for the Commercial loan and grant programs.

Community Programs component includes the functionality to pull in application data from CPAP and transmit the data needed to process obligations/deobligations 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/deobligations results; i.e., processed, rejected, from the nightly update are sent back to CLSS and CPAP for updating. This functionality will be used until the PLAS is retired.

Loan and Grant Management System (LGMS) component includes web transactions for obligations/rescissions, advances/disbursements, and cancellations that interface with the Program Funds Control System; notes; and designation notices. The advances/disbursements are processed through an interface to the Automated Clearing House via the National Information Technology Center (NITC) mainframe. Temporary interfaces were implemented to send updates to the legacy system for the notes and advances. LGMS also interfaces with

CPAP, the Guaranteed Loan System, and Broadband Application Information Log to obtain data to process the obligations in CLSS for selected loan/grant programs.

Cash Application Module (CASH) component includes the functionality to reconcile Rural Development cash receipts with vouchers. CASH allocates the cash receipts for the RUS transactions across the appropriate accounts for reporting to the General Ledger and Cash Tracking on the NITC mainframe. Temporary interfaces were implemented to the legacy systems for the payment/bill matching process.

RUS Loan Servicing (RLS) component creates and maintains receivable accounts; calculates daily interest accrual and late fees; allows for CoC deposits, capitalization of interest, and usage of CoC funds; provides consolidated borrower quarterly statements and RTB audit confirmations; and performs billing, payment and collections services, and some unique 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 participants (i.e. customers) for Rural Development's Commercial direct loan and grant programs' as "Borrowers" in a database including their Taxpayer Identification Number, Social Security Numbers, address and contact information, contact personnel, legal name, financial disposition, and bank and loan account information.

CLSS maintains Congressional Districts and representative contact information; Financial Institution information, including bank routing, and contact information associated with the Borrowers in the system; information about CPA firms responsible for the auditing of Borrowers.

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

Data is provided by potential borrowers via application packets (application, financials, business plans and a feasibly study).

Program Staff, Deputy Chief Financial Officer Staff, General Field Representatives, and Field Office users physically *enter* application and other data directly into CLSS. Data is also provided and uploaded to CLSS via files and stored procedures which *transfer/update* data to and/or from interface sources.

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

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 facilitate the processing by USDA personnel of applications, obligations, loans, grants, and collections on behalf of Rural Utilities customers. Data is also used for required reporting purposes to entities such as IRS, U.S. Treasury, etc.

1.4 How is the information collected?

Data is collected via application packets (application, financials, business plans and a feasible study) provided by potential borrowers. Program staff, NFAOC staff, general field representatives, and field office users physically enter application and other data directly into the system. Data is also collected from interface sources uploaded to CLSS via files and stored procedures.

1.5 How will the information be checked for accuracy?

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.

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.

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

Legal Authority: Paperwork Reduction Act and **Section 10708 of the 2002 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.). Additionally, this process is also driven by privacy laws, regulations, and government requirements, including the Privacy Act (5 U.S.C. 552a); the E-Govt. Act, Sec. 208 (44 U.S.C. 3501); the FISMA (44 U.S.C. 3541); OMB Memos M-03-22, M-05-08, M-06-15, M-06-16, M-07-16; OMB Circular A-130, Appendix I.

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

RISK: CLSS tracks participants (i.e. customers) for Rural Development's Commercial direct loan and grant programs' as "Borrowers" in a database including their Taxpayer Identification Number, Social Security Numbers, address and contact information, contact personnel, legal name, financial disposition, and bank and loan account information. CLSS maintains Congressional Districts and representative contact information; Financial Institution information, including bank routing, and contact information associated with the Borrowers in the system; information about CPA firms responsible for the auditing of Borrowers. The risk is in the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the client.

MITIGATION: Data is stored in a secure environment behind the NITC secure mainframe infrastructure. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM).

.

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.

CLSS direct loan and gran programs principal purpose is to provide an automated means to a complete program management and financial information.

Data is used to meet federal reporting requirements. E.g. Internal Revenue Service and Federal Funding Accountability and Transparency Act (FFATA) reporting requirements. Data is used to maintain accountability and provide authorization for advancing approved funds to borrowers (customers).

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

Reports (i.e., Data Warehouse, discrepancy, and daily obligation reports) are utilized by the Program Staff, Field Offices, and Finance Office Staff, who will periodically verify/review the data in the system to audit the system operation and input of data.

Any data entered/stored in the system can be queried for production in a report.

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

CLSS maintains Congressional Districts and representative contact information which is used for tracking and reporting purposes. This is accomplished through a file provided by Program Staff located in Washington, D.C. (WDC) after publishing. The file is uploaded to the CLSS database as a file adjustment/technical change; no external feed is required.

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 CLSS system are discussed in detail in the System Security Plan and specifically the Access Controls (AC 1-6, 11, 12, 14, 17, 20, and 21), Identification and Authentication (IA 1-8) controls are in place to prevent unauthorized access restricting users from accessing the operating system, other applications or other system resources not needed in the performance of their duties and is restricted by eAuthentication (eAuth). The Authority and Purpose (AP 1-2) compensating controls give explanation of why PII is allowed on the system. Systems and Communication Protection (SC 1, 2, 4, 5, 7, 8, 10, 12, 13, 17, 20-23, 28, and 39) controls are in place to prevent unauthorized 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?

Information is retained indefinitely.

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: Information being retained for an indefinite length can potentially be a risk. With data stored for this length of time there is the potential of unauthorized access, unauthorized disclosure or illegal use of the customer PII data.

MITIGATION: Data Integrity controls (DI 1-2) are used to protect data from accidental or malicious alteration and destruction providing assurance to the user the information meets expectations for quality and it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements are in place. 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 CD's, are shredded. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM).

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?

- Guaranteed Loan System (GLS): Process lender status reports and loan closings.
- Multi-Family Integrated System (MFIS): provide a hyperlink connection to CLSS allowing MFIS users to view the MFIS miscellaneous receipts in CLSS from MFIS through a new browser page.
- Program Funds Control System (PFCS): obligation and disbursement data
- RUS Legacy: Sends nightly feeds for notes, and pre-notes data to the mainframe.
- Automated Mail Processing (AMP): Prints statements and tax forms
- Business Intelligence (BI): Tabular Data Warehouse (TDW) receives data for reports
- eServices: Enterprise Cash Management System (ECMS) provides disbursements data and RDUPCIP – customers make payments through online collection system.
- New Loan Originations: Commercial Program Application Processing (CPAP) transmits data needed to process obligations / de-obligations into PLAS during the nightly update.
- CLP Support Applications: Data Collection Service (DCS) User, Borrower User and Partner User information is retrieved from CLSS.
- Admin: Staff Review and Reporting System (SRRS): Provides audit and financial review data
- Program Loan Accounting System (PLAS): Accounting system of record and official reporting mechanism

4.2 How is the information transmitted or disclosed?

Data is transmitted via scheduled job.

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: The risk to internal information sharing would be the unauthorized disclosure of lender status and loan closing reports, obligation and disbursement data, statement and tax report information, borrower information and accounting information.

MITIGATION: The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) 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 the implementation of RD ISSS NIST policies, standards and procedures. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure.

.

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?

- Bulk Data Exchange System Dunn & Bradstreet - Support CLSS reporting commercial loan information to Dun & Bradstreet on a quarterly basis
- Equifax eReporting Credit Bureau – information needed for credit reports and scores
- Experian Credit Bureau - Data files transferred from LoanServ, CLSS and GLS to Experian for credit bureau reporting. Supports reporting commercial loan information on a quarterly basis
- National Rural Utilities COOP Finance Corp (NRUCFC)/ Cooperative Finance Corporation (CFC) - supports data files that are imported via an upload page by the Deputy Chief Financial Officer and applied to CLSS
- Fiscal Service Treasury Web Application Infrastructure (TWAI) Department of Treasury - U. S. Department of Treasury provides debtor and debt information for Treasury Offset Program and Cross Servicing processing

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, USDA/Rural Development-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs.

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

All external connections require an Interconnection Service Agreement (ISA) or Memorandum of Understanding (MOU).

- Dunn & Bradstreet - Bulk Data Exchange System (BDES) - Exchange of data will be limited to specific server IP addresses over Secure FTP port 22, enforced by firewall rules
- Equifax eReporting Credit Bureau – All data files are transferred in a one way connection via Secure File Transfer (SFTP) protocol.
- Experian Credit Bureau - All data files are transferred in a one way connection via Secure File Transfer (SFTP) protocol
- National Rural Utilities COOP Finance Corp (NRUCFC) / Cooperative Finance Corporation (CFC) - processes send files through SCP which encrypts the files
- Fiscal Service Treasury Web Application Infrastructure (TWAI) Department of Treasury - U. S. Department of Treasury – Connect:Direct without Secure+ uses a proprietary file transfer protocol (TCP ports 1364 and 1372).

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

RISK: The risk to external information sharing would be the unauthorized disclosure of statement and tax report information, borrower information and accounting information.

MITIGATION: Data is sent via VPN and a signed Interconnection Service Agreement are in place in CSAM and maintained by the ISSS. The exchange of data will be limited to specific server IP addresses over Secure FTP port 22, enforced by firewall rules. The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to

prevent unauthorized and unintended information transfer. System and Integrity (SI) 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 the implementation of RD ISSS NIST policies, standards and procedures. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure.

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, USDA/Rural Development-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs (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?

Yes, application packet (application, financials, business plans and a feasibly study) data is provided by the potential borrowers for the purposes of obtaining Commercial loans and grants. Therefore, the borrowers are aware of the information as they provide it.

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

Yes, borrowers can decline to provide necessary information at the risk of being declined Commercial loan/grant funding.

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

Yes, borrowers have the right to provide only specific data. The data requested is necessary and is used for determination of funding and to track loans and grants after funding as a complete financial management tool within CLSS. If it is the Borrower's intent not to provide all data requested, they may be declined Commercial loan and grant funding.

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.

CLSS 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.

Individual do not have direct access to the system as users. Individuals have the option to decline to proceed. If the user declines, no data is collected; therefore, no risk is associated. If the user accepts, they provide their own data and are aware of the information being collected.

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?

Individual borrowers do not have direct access to the system as users. Data is provided *by* potential borrowers via application packets (application, financials, business plans and a feasibly study). Program Staff, NFAOC staff, general field representatives, and field office users physically enter application and other data directly into CLSS.

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

If any inaccurate or erroneous information is identified, the program staff, NFAOC staff, general field representatives, or field office users will make the necessary changes manually into CLSS.

Formal requests for correction of USDA information must be submitted by letter, fax, or e-mail to the Information Quality Official(s) of the USDA agency or office that disseminated the information (henceforth in these procedures, the term "USDA agency" shall mean "USDA agency or office"). For requests for correction concerning information on which USDA seeks public comment, submit the correction request during the comment period.

After the responsible USDA agency has made its final determination pertaining to a request for correction of information, that agency will respond to the requestor in writing by letter, e-mail, or fax, normally within 60 calendar days of receipt. The response will explain the findings and the actions the agency will take (if any) in response to the complaint.

If the request requires more than 60 calendar days to resolve, the agency will inform the complainant within that time period that more time is required, reasons for the delay and an estimated decision date.

Customers and employees may contact the Freedom of Information Officer:

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

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

Individual borrowers do not have direct access to the system as users. Data is provided by potential borrowers via application packets (application, financials, business plans and a feasibility study).

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

Individuals have access, redress, and amendment rights under the Privacy Act and the Freedom of Information Act.

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.

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?

For CLSS, eAuth controls all access to the USDA network and information. Access to information is based on the user privilege level. eAuth provides ID by using an infrastructure UserID for a single-sign-on (SSO) solution providing front-end authentication of system users. UserID construction is in conformance to established USDA policy.

8.2 Will Department contractors have access to the system?

Yes.

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 23 February 2020.

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

NIST 800-53 controls are discussed in detail in the SSP including the Audit and Accountability (AU) controls in place to prevent misuse of data.

RD has a Audit and Accountability Policy, Standards, and Procedure 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 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: There is minimal risk given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system.

MITIGATION: However, RD has the following controls in place - 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. Audit logs will be reviewed by the NITC Security Division 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 1C, 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?

This project is part of the Comprehensive Loan Program (CLP) Investment facilitates the processing by USDA personnel of applications, obligations, loans, grants, and collections on behalf of RD Commercial Program customers.

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

CLSS does 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?

CLSS does not use third 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.

CLSS does not use third 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?

CLSS does not use third 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?

CLSS does not use third 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?

CLSS does not use third 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?

CLSS does not use third 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?

CLSS does not use third 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)?

CLSS does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

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?

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.

CLSS does not use third party websites or applications.

Responsible Official

SHANI BURLEY-MOORE

Digitally signed by SHANI BURLEY-MOORE
Date: 2017.09.29 09:33:41 -06'00'

Shani Burley-Moore
Chief, Commercial Loan Technologies Branch

Approval Signature

DIEGO MALDONADO

Digitally signed by DIEGO MALDONADO
Date: 2017.09.29 15:06:57 -05'00'

Diego Maldonado
Rural Development Privacy Officer