Privacy Impact Assessment
RDForce (RDForce)

Policy and Directives

- Version: 2.0
- Date: February 10, 2021
- Prepared for: USDA Rural Development (RD)

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	10/23/2019	AC	PIA Created
2.0	2/10/2021	CC	Updates and revisions.

Abstract

Rural Development's RDForce Information System currently has 3 Salesforce Orgs. Org 1 consists of Resource 1, ReConnect and Higher Blends Infrastructure Incentive Program (HBIIP). Org 2 consists of OneRD Portal, RD CIO Budget Tracker (BTS), CFO Budget Request, Employee Engagement, RD HR Recruiting Tracker Application, and Civil Rights Automated Management System (CRAMS). Org 3 consists of Guaranteed Underwriting System 2 (GUS2). RDForce applications meet RD mission and business needs by providing internal processes and servicing RD customers with loans and grants. This PIA is required as the PTA determined that PII is being processed by RDForce. Only those components that collect, process or store PII will be evaluated in this PIA. BTS and Employee Engagement will not be evaluated in this PIA.

Overview

RDForce is built on the Salesforce platform and Mule Cloud platform; the Lender Intake modules will integrate with MuleSoft to leverage internal and external services.

Rural Development's RDForce Information System currently has 3 Salesforce Orgs. Org 1 consists of Resource 1, ReConnect and Higher Blends Infrastructure Incentive Program (HBIIP). Org 2 consists of OneRD Portal, RD CIO Budget Tracker (BTS), CFO Budget Request, Employee Engagement, and Civil Rights Automated Management System (CRAMS). Org 3 consists of Guaranteed Underwriting System 2 (GUS2).

ORG 1

Resource 1 is the United States Department of Agriculture (USDA) Rural Development's official customer relationship management (CRM) system. R1 was developed by the Office of the Chief Information Officer (OCIO) in conjunction with subject matter experts from across USDA Rural Development and a sub-sect of Rural Development employees who use the system day-to-day work to ensure that the system captures all the fields and functionality. Resource 1 is used by USDA RD employees to enter basic contact information to share with fellow employees facilitating effective communication and correspondence with new and existing employees. Resource 1 is also used by RD employees to track outreach efforts by local staff on various Administration initiatives and any outreach campaigns to increase program funding traffic.

ReConnect is a public facing website/portal to display Rural Utilities Services (RUS) telecom program information. The portal leverages the Salesforce Communities product and has two different ESRI ArcGIS web maps for rendering publicly available mapping data in Salesforce. It will also give a user the ability to submit questions.

ReConnect Application is comprised of a publicly facing web portal leveraging the Salesforce Customer Community Cloud that will be accessed by eAuthenticated RD approved applicants, authorized representatives and borrowers and a web based administrative application leveraging the Salesforce Service Cloud accessed by RD Broadband program staff and application System Administrators. All administrative users authenticate using eAuthentication. The application leverages the following third-

party AppExchange products: Vlocity, Lightning, and Gridbuddy components. The applications are included in the ReConnect system via managed packages or additional API integrations.

The Higher Blends Infrastructure Incentive Program (**HBIIP**) expands the availability of domestic ethanol and bio-diesel by incentivizing the expansion of sales of renewable fuels. It requires an automated grant application and grant tracking tool to evaluate and make award determination to fuel operators. Grants will be available to help transportation fueling and bio-diesel distribution facilities convert to higher-ethanol and biodiesel blends by sharing the costs related to installing, retrofitting and/or upgrading fuel storage, dispenser pumps, related equipment and infrastructure.

The purpose of the HBIIP System is to provide:

- External public users to complete and submit a HBIIP grant application and to submit periodic project performance data for awarded grants.

- External Partner Agency users from National Renewable Energy Lab (NREL), a division of the Department of Energy (DOE), with signed and approved Memorandum of Agreement (MOA) and Non-Disclosure Agreements (NDAs) to review applications and provide recommendations for grant awards.

Internal RBCS users will review, complete and track the award and offering of grants and to monitor project performance for awarded grants. The HBIIP System will also include a one-directional integration with the Commercial Loan Servicing System (CLSS) to push grant requests for subsequent obligation and execution of funding in CLSS, using MuleSoft.

ORG 2

OneRD Portal is an employee-based portal for centralizing USDA RD various Business Center administrative service offerings and service requests. The Business Center, which works with employees throughout the country, performs various workflow that can accommodate selected RD administrative functions and be used by a virtual workforce. The intent is to automate majority of administrative tasks, and provide a paperless, fast, and efficient service to our virtual workforce. The OneRD Portal is a central resource for Rural Development employees. It is implemented on the internal Rural Development Salesforce organization.

OneRD Portal is a central resource for RD employees. It is used internally by RD employees and RD contractors. OneRD Portal will:

- provide links to common employee resources (AgLearn, WebTA, and EmpowHR)
- serve as a communication hub between management and employees by featuring articles and content (Newsbox, IPI in Action, and Newscan)
- automate RD Business Center workflows, some of which are currently automated on SharePoint

RDForce will support the RD Business Center's re-organization by serving as a central point for RD employees to interact with the various business center divisions (HR, Management Services Division, Enterprise Services Division, Finance, Procurement Management Division, Architect and Appraiser Division and Engineer and Environmental Division).

OneRD Portal will provide is a searchable employee directory, which will contain:

- Employee Name
- Email
- Phone Number
- Position
- Supervisor
- Location (state)

Additionally, employee information (for HR requests), and financial information for Budget and Procurement Management requests, FOIA requests, and hardware and software provisioning information may be included in the RDForce workflows.

RD HR Recruiting Tracker Application will be a workflow in OneRD Portal that will create a National web-based data tracking system for all hiring actions identifying HR hiring tasks and actions, timelines for such actions, responsible staff and customer service feedback. This initiative will include goals for creating and implementing employee recognition and awards program. The application will be a future replacement for manual processes into a customer-facing, automated application for tracking and reporting on RD HR Recruitment Services. This application is inactive at this time.

Some of the workflows in OneRD Portal, especially those related to Human Resources, could involve additional employee PII.

Some of the workflows, especially those related to Human Resources, could involve additional employee PII. This PTA, the PIA and related security documentation will be updated with any major technical changes as RDForce continues to evolve with the system development lifecycle.

RD CIO Budget Tracker (**BTS**) is an end-to-end Cloud-based application that provides a secure, scalable, enterprise-level, web-based application for efficiently tracking RD CIO's Budget. It provides the complete capability to create, manage, track, and report on all Budget topics. The application is configured to provide an environment that offers maximum ease of use to the RD management and the users by using presentation techniques that are familiar to users of Internet Explorer or other internet browsers. Being a cloud-based solution, it enables RD management to free up IT resources from day-to-day administration of servers, operating systems and databases. BTS does not collect, process or store PII.

RD CFO Budget Request is an end-to-end Cloud-based application that provides a secure, scalable, enterprise-level, web-based application for efficiently tracking budget requests. It provides the complete capability to create, manage, track, and report on all Budget requests by fiscal year. The application is configured to provide an environment that offers maximum ease of use to the RD management and the users by using presentation techniques that are familiar to users of standard internet browsers. Being a cloud-based solution, it enables RD management to free up IT resources from day-to-day administration of servers, operating systems and databases. Being a cloud-based solution, it enables RD management to free up IT resources from day-to-day administration of servers, operating systems and databases.

Employee Engagement is a simple event tracking application that documents the objectives of the event, key outcome and some basic participant information like number of people etc. The reports from the region are compiled and presented to the Secretary as part of Cultural transformation reporting. Employee Engagement is defined as the employee's sense of purpose that is evident in their display of dedication, persistence, and effort in their work or overall attachment to their organization and its mission. A successful organization fosters an engaged working environment to ensure that each employee reaches their full potential and contributes to the success of their agency and the Federal Government. No PII regarding any individuals is collected, used or processed.

Civil Rights Automated Management System (**CRAMS**) automates the functionality for the RD Civil Rights staff to track complaints and compliance issues involving RD program borrowers regarding federal civil rights statutes and program issues and civil rights violations. CRAMS enables the Program Compliance Branch to enter program complaint and data information and run queries and reports on various Matters relative to program Civil Rights laws, including Equal Credit Opportunity Act, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Title IX of the Education Amendments Act of 1972, Limited English Proficiency (LEP), and Section 504 of the Rehabilitation Act of 1973. Additionally, the system will capture data required by Executive Orders 11063, 11246, 12250, 12892, and 12898, as well as alleged program discrimination complaint activity. Future enhancements will allow CRAMS to track, Civil Rights and other training, public notification and outreach activities, compliance reviews, pre- and post-awards, Affirmative Fair Housing Marketing Plans, Age reports, Civil Rights Impact Analyses, and associated expenses.

Civil Rights tracking application to track correspondence from Office of the Assistant Secretary for Civil Rights (OASCR), U.S. Department of Housing and Urban Development (HUD), and external customers for discriminatory complaints against RD programs and affiliates.

ORG 3

Guaranteed Underwriting System2 (**GUS 2**) application is a web-based portal accessed by mortgage lenders/agents to complete and submit loan applications and accessed by RD employees to review submitted loan applications. GUS 2 is designed to transition the GUS (Legacy) intake process to a Salesforce platform that is compliant with new regulatory requirements, mortgage industry standards, and the Fannie Mae and Freddie

Mac redesigned URLA. The system also includes import and processing capabilities for MISMO 3.4 XML so that the new platform can process formatted loan application exports from customers.

Typical Transaction in System: A loan application will be initiated either directly in the application or will be imported from a Loan Origination System (LOS) by a Lender or Lender Agent. The application information, whether input into the UI or imported, is stored in Salesforce and supplemented by internal (USDA) and external (non-USDA) services used to validate, assess, or retrieve application data. Once submitted, a USDA RD employee will review the loan application and may approve, reject or withdraw the application. If approved, the loan application will be sent to the Guaranteed Loan System (GLS) via MuleSoft (2-way SSL/Restful Services JSONHTTPS 443).

GUS2 – PII will be shared with MuleSoft to pass to internal USDA services, including Application Authorization Security Management (AASM), Guaranteed Loan System (GLS), Electronic Customer File (ECF), Account Cross Reference (ACR), Address Verification, Adobe Lifecycle (AEM), Annual Fee Amortization Schedule Service, Eligibility Service, FICO Blaze Service and MISMO File Upload. In addition, information will be shared with Tabular Data Warehouse (TDW), via the Informatica plug-in with loan application data; this connection is directly with TDW and does not go through MuleSoft.

GUS2 - PII will be shared with MuleSoft to pass to external services, including CAIVRS (HUD), Total Scorecard (HUD), SAVE (USCIS) and Fannie Mae (Credit Report).

This PIA will not provide analysis for the following systems that do not collect PII: CIO Budget Tracker (BTS) and Employee Engagement.

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?

Resource 1:
PII collected, processed or stored on

- USDA Employees
- Contractor

Data elements:

- Names, including Business Names
- Address information

ReConnect:
ReConnect accepts applications for business entities. To apply, businesses must provide the company name, Tax ID number (TIN) and other details about the company and the proposed

project. Users acting on behalf of the business provide their names, phone, and email information.
Business/proprietary information is provided as part of the application process, including the business' financial statements. ReConnect produces completed grant and loan applications, which include the financial data, proposed service area information, and geospatial (map) representation of the service areas. This information is accepted in the application forms and by uploading documents. The review process is documented in the application. This includes communication between RUS staff and the applicants, internal RUS staff documentation, and various scoring metrics.
The entity applying for the ReConnect Award must be one of the following:

- o A state, local government, or any agency, subdivision, instrumentality, or political subdivision;
- o A territory or possession of the United States;
- o An Indian tribe (as defined in section 4 of the Indian Self-Determination and Education Assistance Act);
- o A non-profit entity;
- o A for-profit corporation;
- o A limited liability company; or
- o A cooperative or mutual organization

PII collected, processed or stored on:

- USDA Employees
- Contractor
- USDA Partner

Data elements:

- Name
- Address information
- Personal Identification Number – TIN for Business

HBIIP:
PII collected, processed or stored on:

- USDA Employees
- Contractors
- Non-USDA Federal Government employees
- USDA Partner

Data Elements:

- Name
- Miscellaneous Identification Numbers

OneRD Portal:
OneRD Portal will have searchable employee directory, which will contain:
PII collected, processed or stored on:

- USDA Employees

- Contractors

Data elements:

- Employee Name
- Date of Birth
- Address Information
- Personal Identification number
- Financial Data
- Health Data
- Employment History
- Miscellaneous Identification numbers

RD CFO Budget Request:

PII collected, processed or stored on:

- USDA employees
- Contractors

Data Elements:

- Name
- Personal Identification Number
- Financial Data
- Miscellaneous Identification Numbers

CRAMS:

PII collected, processed or stored on:

- USDA Employees
- Non-USDA Federal Government employees
- USDA Partner
- General Public
- Other – Program Participants

Data Elements:

- Name
- Date of Birth
- Address Information
- Personal identification number
- Financial data
- Health data
- Employment History
- Miscellaneous identification numbers (Loan Account number)
- Photographic Image
- Handwriting or image of the signature
- Other information (Military and demographic information)

GUS2:
PII collected, processed or stored on:

- USDA Employees
- Contractors
- USDA Partner
- General Public
- Loan lenders/loan agents/loan originators

Data Elements:

- Name
- Date of Birth
- Address Information
- Personal Identification Number
- Financial Data
- Employment History
- Miscellaneous Identification Numbers
- SSN/TIN
- Military and Demographic Information

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

Resource 1 – information is provided by USDA RD staff, who enter basic contact information to share with fellow employees facilitating effective communication and correspondence with new and existing employees.

ReConnect – sources of information are largely from business applications and USDA RD users, who are involved in the workflow process of the application for grant and loan applications. ReConnect accepts applications from business entities. To apply, businesses must provide the company name, Tax ID number (TIN) and other details about the company and the proposed project. Users acting on behalf of the business provide their names, phone, and email information.

ReConnect has business/proprietary information provided as part of the application process, including the business' financial statements. ReConnect produces completed grant and loan applications, which include the financial data, proposed service area information, and geospatial (map) representation of the service areas. This information is accepted in the application forms and by uploading documents. The review process is documented in the application. This includes communication between RUS staff and the applicants, internal RUS staff documentation, and various scoring metrics.

HBIIP – Source of the information is the grant applicants/awardees, which are typically organizational borrowers.

OneRD Portal - Employee Directory information will be managed through the Sailpoint integration. SailPoint is a part of the USDA's identity management system managed through ICAM. Other data will be generated through the daily employee requests as recorded and tracked in the workflows.

RD CFO Budget Request – sources of information are largely from business applications and USDA RD users, or budget analysts from the administrative budget branch.

CRAMS – Complaints, letters, correspondence may be received from applicants/ tenants/ borrowers/ customers of RD; or from OASCR, HUD, DOJ or other USDA agencies; and CRAMS staff may verify complaint information from MFH Rental Site.

GUS2 – Information in the system is sourced from:

- User data entry by trusted lenders, lender agents and RD employees
- Lender Loan Origination Systems (LOS)
- Internal USDA services: AASM, GLS, Property Eligibility, Income Eligibility, Annual Fee Amortization Schedule, FICO Blaze, ECF Document Management, Adobe Lifecycle (AEM), Account Cross Reference (ACR)
- External services: Microsoft Bing, CAIVRS (HUD), SAVE (USCIS), HUD Scorecard (HUD), Fannie Mae Credit Bureau

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

Resource 1 – information is collected, maintained and used to facilitate communication and correspondence with new and existing RD employees.

ReConnect – business application information is collected, maintained and used to meet RD mission and business needs of providing loans and grants to qualified broadband business entities in rural communities.

HBIIP – to determine the eligibility of the organizational borrower for a grant or award and the feasibility of their application.

OneRD Portal – the Employee directory in OneRD Portal is intended as a reference for RD employees. The Portal is an employee-based portal for centralizing USDA RD various Business Center administrative service offerings and service requests. The intent is to automate majority of administrative tasks, and provide a paperless, fast, and efficient service to the RD virtual workforce. The OneRD Portal is a central resource for Rural Development employees.

RD CFO Budget Request – information is provided in support of approved base budget requests and additional funds requests.

CRAMS –The system is used to track day-to-day activities and ensuring the capture all the fields and functionality needed for compliance and complaint monitoring. CRAMS is designed to make it easier for the user to input, track, and report civil rights inquiries, complaints and etc., and to connect with internal and external customers. CRAMS tracks information and allows for reporting on work that has previously been untrackable. CRAMS allows the user to generate letters and documents based on information in the case, reducing administrative time spent searching for template letters and manually entering information.

GUS2 – The application collects, maintains and uses the information to facilitate the loan application intake process. Specifically, loan application information is used to determine

eligibility for loans, support RD in loan approval decisions, determine underwriting recommendations, and for consolidated reporting of loan information.

1.4 How is the information collected?

Resource 1 – information is collected from USDA RD users, who enter the information into the application.

ReConnect - information is collected from business applicant users, who input the business application data to apply for a loan or grant from RD. RD users, who are involved with the workflow process for business applicants, facilitate the information flow that is involved with the loan and grant processing.

HBIIP – Borrowers (typically consisting of entity borrowers) will use the HBIIP system to input data and upload supporting documentation. Also, information collected from NREL reviewers who provide a technical opinion regarding the award of the grant.

OneRD Portal – Information will be collected through the regular case management workflows and could also be provided by the individual directly. When an employee submits a request to the Business Center, they need to provide the necessary information for a Business Center resource to work and resolve the request. Additionally, the Business Center resource will update the case with additional information as necessary. For example, a request by an employee to change their Dental Benefits would require the employee to provide their name, contact information, current benefit selection as well as desired benefit selection.

Additionally, the Sailpoint integration performs a nightly update to the Employee Directory in OneRD portal.

RD CFO Budget Request – budget analysts submit either approved base budget request or supplemental budget request and any supporting documentation by logging into the system.

CRAMS – The information may be in the form of an email (electronic collection), letter (electronic or paper collection), data compilation reports (electronic or paper collection), phone calls, and notes (electronic or paper collection) from the Inquirer, Complainant, HUD, DOJ, OASCR, and/or RD National, State, and Field Offices and Program Recipients (Respondents, also known as applicants/ tenants/ borrowers/ customers of RD); also CRAMS staff may verify complaint information using the MFH Rental Site.

GUS2 – Loan application information, which includes PII, is entered directly into the Salesforce User Interface (UI), or it originates in external Lender Loan Originating Systems (LOS) which then flows into Salesforce. As this loan application data flows into Salesforce or is input directly into the UI by lenders, MuleSoft services are leveraged to supplement the information with additional data from USDA- and non-USDA-owned systems (see System Description for a comprehensive list) to support the loan intake and review processes. RD loan officers and trusted lenders provide input for guaranteed loan application data. Once loan applications are approved, the loan application data is sent from Salesforce to the RD FORCE GUS2 database; borrower information stored in RD FORCE GUS2 is then sent to GLS and TDW. Loan information also flows from GLS to Salesforce.

The information is collected via:

- User input, directly into the Salesforce UI, by trusted lenders and lender agents
- Integration with MuleSoft to supplement application data with additional information via internal USDA and external non-USDA services.

1.5 How will the information be checked for accuracy?

Resource 1 – information will be checked for accuracy by RD users, who have authorized access and can provide any data corrections, if necessary.

ReConnect – Business applicants work with RD staff to correct any errors in their loan or grant applications for ReConnect. RD staff can make any corrections that are necessary in the ReConnect application and related documentation.

HBIIP – Organizational borrowers upload the data into HBIIP, and they will attest to the accuracy of the data. RD reviews the data for completeness.

OneRD Portal – Employee Directory information is provided by the SailPoint integration, which aggregates employee information from EmpowHR and Active Directory. Any inaccuracies in the data will need to be addressed in these source system(s).

RD CFO Budget Request – budget analysts will submit either approved base budget request or supplemental budget request and any supporting documentation, then the budget oversight branch budget analysts will confirm the information submitted by the budget analyst.

CRAMS – The information will be verified against the case file, if applicable, Federal Laws and Executive Orders, agency regulations, and automated public data sources. Interviews with knowledgeable parties and stake holders may be utilized to obtain additional information. For complaints involving a Single Family Housing (SFH) borrower, may request information from Customer Service Center (CSC) to verify that the individual has a loan; for complaints involving an individual tenant, may check the Multi-Family Housing (MFH) Rental Site to verify that it involves a MFH property, or reach out to management agent or property owner to verify that individual is tenant of that MFH property; for complaints involving the RUS or RBS program, may verify that individual is in the program and may need to request RUS or RBS employee to verify individual information using GLS. In addition, CRAMS employees are in direct contact with individuals reporting the complaint and can make any updates or changes to the complaint, as necessary, if reported by the individuals.

GUS2 – Data input into Salesforce by a lender/lender agent and data received by Salesforce to supplement any manual data entry will be verified through screen edits and field-level validations. Additionally, RD employees will review data in each loan application.

Salesforce maintains audit information for field changes by User ID; these system logs may be monitored by system administrators.

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

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

- Privacy Act of 1974, as Amended (5 U.S.C. § 552a)
- OMB Circular A-130, Managing Information as a Strategic Resource, July 2016
- Freedom of Information Act, as amended (5 U.S.C. § 552)
- Federal Information Security Modernization Act of 2014 (also known as FISMA), (44 U.S.C. §3551), December 2014
- 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 U.S.C. §1681f
- Consumer Credit Protection Act, 15 U.S.C. §1601*, et. seq.*
- Equal Credit Opportunity Act, 15 U.S.C. §1691, *et. seq*.
- The Fair Debt Collection Practices Act, 15 U.S.C. §162, *et. seq*.
- 7 CFR Part 3550, Direct Single Family Housing Loans and Grants
- 7 CFR Part 3555, Guaranteed Rural Housing Program
- 7 CFR Part 3560, Direct Multi-Family Housing Loans and Grants
- USDA RD Instruction 2033-A – Records, Management of RD Records (updated as of 8-2020)
- NARA General Records Schedules (provides mandatory disposition instructions for records common to several or all Federal agencies)

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

RISK: Data collected facilitates the processing by USDA personnel of applications, obligations, loans, and grants, on behalf of Rural Development customers. Collected data is used to monitor USDA-guaranteed private sector lender's loan portfolios, process loan origination activities, including prequalification, application processing, underwriting, loan closing and borrower's corporate standing. 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 customer.

MITIGATION: RDForce system owners define access roles to ensure separation of duties, account management and authorized access to data and information to mitigate the risks to privacy data in the RDForce applications.

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.

Resource 1 – used internally by USDA RD staff to enter basic contact information to share with fellow employees facilitating effective communication and correspondence with new and

existing employees. Also used by RD employees to track outreach efforts on program activity and Administration initiatives.

ReConnect – information is used to process business applications for loans and grants.

HBIIP – Users/applicants will submit an application to determine the eligibility of the organizational borrower for a grant or award and the feasibility of their application. Grants will be available to help transportation fueling and biodiesel distribution facilities convert to higher-ethanol and biodiesel blends by sharing the costs related to installing, retrofitting and/or upgrading fuel storage, dispenser pumps, related equipment and infrastructure. NREL reviewers will review the application data and will provide a technical opinion regarding the award of the grant.

OneRD Portal - OneRD Portal is a central resource for RD employees and is a searchable employee directory. It is used internally by RD employees and RD contractors. OneRD Portal will:

- provide links to common employee resources (AgLearn, WebTA, and EmpowHR)
- serve as a communication hub between management and employees by featuring articles and content (Newsbox, IPI in Action, and Newscan)
- automate RD Business Center workflows, some of which are currently automated on SharePoint

RD CFO Budget Request – budget oversight branch uses the information submitted by the budget analysts in support of the budget request to provide to senior leadership for final approval.

CRAMS – The information will be used to provide a response to Inquiries; answer Programmatic Complaints, and to address formal civil rights complaints and non-compliance civil rights matters. The application tracks correspondence from OASCR, HUD and external customers for discriminatory complaints against RD programs and affiliates.

GUS2 – The application collects, maintains and uses the information to facilitate the loan application intake process. Specifically, loan application information is used to determine eligibility for loans, support RD in loan approval decisions, determine underwriting recommendations, and for consolidated reporting of loan information.

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

Resource 1 – does not currently use tools to analyze data. RD staff uses the data in this application for internal use and to track outreach efforts on program activity and Administration initiatives.

ReConnect - does not currently use tools to analyze data. RD staff uses the data in this application to process loan and grant applications servicing rural areas.

HBIIP – does not currently use tools to analyze data. RD staff uses the data in this application to process grant applications.

OneRD Portal – RDForce reporting will be used to analyze the data in OneRD Portal to ensure separation of duties, account management and authorized access to data and information.

RD CFO Budget Request – does not currently use tools to analyze data. RD staff uses the data in this application for internal use.

CRAMS – RD staff uses the data in this application to process complaints involving RD program borrowers. RD staff exports data to Excel to create charts, graphs, etc.

GUS2 – Salesforce calls both internal and external services via MuleSoft to supplement the loan application with additional data. The services which are used to analyze data and support the RD employee in reviewing the loan application are as follows:

- Salesforce sends application and borrower data through the FICO Blaze rules engine; the rule engine evaluates the data based on the rules, renders an underwriting recommendation and findings, and sends both back to Salesforce
- Salesforce sends application data through the HUD Scorecard service; HUD runs the data through the Scorecard, evaluates the data and returns a response to Salesforce with a recommendation for the application
- Salesforce receives credit data through CAIVRS that determines if a loan applicant has any Federal debt or is in default or foreclosure.
- Salesforce retrieves the borrower's credit report via the Fannie Mae Credit Bureau service.

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

Resource 1 – does not currently use commercial or publicly available data.

ReConnect – uses internal verification tools, such as map verification, at this point in the system development lifecycle.

HBIIP – does not currently use commercial or publicly available data.

OneRD Portal – does not currently use commercial or publicly available data.

RD CFO Budget Request – does not currently use commercial or publicly available data.

CRAMS – Publicly available data from certified sources may be used when providing a response to specific allegations. CRAMS may use Google maps to verify the property address and may use public data sources, such as, Census data, HUD Funding Report and MFH Rental Housing Listing for comparative purposes to assist with the assessment of the complaint.

GUS2 – The application will use Address Verification service to check and validate the property address prior to checking the property's loan eligibility.

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.

All applications for RD Force use eAuthentication and the UAM ticketing process for RD employees. The controls used to detect unauthorized access are Salesforce security logs/audit trails.

ReConnect – public, non-authenticated, users may access the system, however authorized users that will provide information for the entity applicants, will be required to obtain an eAuth Level 2 account to access the system.

HBIIP – Most users are required to have an eAuth Level 2 account, however, some users with preauthorization will be able to access HBIIP with eAuth Level 1 and role based access controls.

OneRD Portal is accessible only by RD Employees and RD contractors via eAuthentication with role-based access, including privileged users who have access to sensitive data. Privileged users include managers and directors, who can see the records of employees that they supervise for escalation and assignment purposes. Privileged users for budget data, include those with elevated privileges based upon role-based access, such as Branch Chiefs.

CRAMS – system is accessible only RD employees via eAuthentication with role-based access. The system tracks the history of changes (i.e. case owner and edits by the user).

GUS2 - Approved lenders will access the Salesforce Partner Portal, an authenticated web page (HTTPS), to complete the mortgage application intake process. This authentication will require lenders to obtain a Level 2 USDA e-Authentication account and AASM user account (created by the Lender/Branch Security Administrators in AASM). Salesforce will receive AASM account information as part of login process and provision the lenders with a Salesforce community user license/role. These users will be activated as a partner contact for their Lender account in the Salesforce Partner Portal. The application uses Adobe Livecycle (AEM) for forms and ECF for document management. There will be an exemption in place through March 2021 allowing lenders to access the application with a Level 1 e-Authentication account in addition to Level 2.

RD Rural Housing Employees will access the Salesforce GUS2 application to administer guaranteed loans using an e-Authentication Level 2 account and following the UAM ticketing process.

The National Institute of Standards and Technology (NIST) 800-53 rev 4 controls are discussed in detail in the System Security Plan and Access , and Identification and Authentication 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 compensating controls give explanation of why PII is allowed on the system. Systems and Communication Protection 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?

All information will be retained in compliance with NARA Guidelines, according to the NARA General Records Schedules (GRS), as well as the RD Records Management policy and financial compliance regulations.

The Employee data is maintained for the duration of the employment of the individuals. After separation, all the data must be removed from the employee profile in accordance with RD Records Management.

Budget information is retained in accordance with the RD Records Management, which complies with NARA.

The SORN RD-1 specifies policies and practices for retention and disposal of Rural Development's records.

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

Yes. RDForce applications follows data retention as provided by the RD Records Management policy, which is in accordance with NARA and financial compliance regulations.

The Employee data will be maintained for the duration of employment of the individual with USDA. After separation all the data associated with the individual must be removed from the system in accordance with RD Records Management, which complies with NARA.

Budget information is retained in accordance with the RD Records Management, which complies with NARA.

The SORN RD-1 specifies policies and practices for retention and disposal of Rural Development's records.

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: RDForce data retention has the potential risks of unauthorized access, unauthorized disclosure or illegal use of the customer PII data.

MITIGATION: The RD data is protected by the Salesforce hosting environment for RDForce applications, which follows USDA federal agency requirements for data protection and is

accredited by FedRAMP. RDForce applications follow the RD Records Management data retention requirements to manage risk associated with data retention, which complies with NARA.

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?

Resource 1 – shares information internally for communication and collaboration with new and existing employees, and information used for reporting purposes.

ReConnect – connects with CLSS/BDMS and LGMS, using MuleSoft, to access existing customer data if customer has prior applications/loans with RD, and to obligate the funds for award portion; connects with TDW to transfer data for consolidated telecom reporting; and connects with RD Apply to receive data for new Farm Bill and Infrastructure loan applications.

HBIIP – Information will be shared with MuleSoft to pass to internal system, CLSS.

OneRD Portal – OneRD Portal will provide links to common employee resources: AgLearn, WebTA, and EmpowHR, OneRD Portal does not share data elements of the users to other systems.

RD CFO Budget Request – N/A. RD staff uses the data in this application for internal use.

CRAMS – summary of the complaint information may need to be shared with internal RD agencies (specific to the complaint: RUS, RBS, SFH, MFH) to obtain further details or verify information regarding the complaint. Information is shared with the USDA Office of Assistant Secretary for Civil Rights (OASCR) as it relates to civil rights compliance and complaint information.

GUS2 – Information will be shared with MuleSoft to pass to internal USDA services, including **API References listed below**:

Service Name	Description	Purpose
AccountCrossReference API	Retrieves a unique borrower Id for a SSN	mask/scramble Tax ID Numbers
Imaging API	A synchronous call used to add or retrieve documents to/from the ECF Imaging repository.	to initiate workflow on a new/existing application

Guaranteed Loan Workflow API	Create and Complete Loan Application Request	Create and complete loan application request
MISMO File Upload API	Create a Loan Application	Create a loan application
GLS API	Adds/updates borrower information in GLS. Adds applications to GLS. Retrieves information from GLS	for user validation, maintenance of borrower data, and storage of application data
FICO Blaze Rules	Execute the SFHG Rules that reside inside the SFHG Rule Repository. It calls the rules engine and returns a response to the calling application	to retrieve a loan underwriting recommendation
Adobe/AEM API	Experience Adobe Livecycle API to get the PDF form based on the form name and input data passed.	to generate a PDF of the loan application
Eligibility API	Accepts a single-string formatted address for Address Validation and Eligibility Verification	to determine the eligibility of the property and to determine the income eligibility of the borrower
Financial Calculations API	Accepts loan information and provides the corresponding Amortization Schedule	to display the amortization schedule of the approved loan
Address Verification API	Accepts a single-string formatted address for Address Validation	to determine the eligibility of the property
AASM API	Retrieve AASM Customer information by Login Id	for user validation

Additionally, information will be shared with TDW via the Informatica plug-in with loan application data; this connection is directly with TDW and does not go through MuleSoft.

Of the above services, shared information includes PII and sensitive data for AASM, GLS, TDW, FICO Blaze, Adobe Lifecycle (AEM), and ACR.

4.2 How is the information transmitted or disclosed?

Resource 1 – information remains in the system and is shared when RD employees access the system.

ReConnect – ReConnect will include an integration with the Commercial Loan Servicing System (CLSS) using MuleSoft; and an integration with RDApply through Informatica.

HBIIP – The HBIIP System will include a one-directional integration with the Commercial Loan Servicing System (CLSS) to push grant requests for subsequent obligation and execution of funding in CLSS, using MuleSoft.

OneRD Portal – OneRD Portal will provide links to common employee resources: AgLearn, WebTA, and EmpowHR, OneRD Portal does not share data elements of the users to other systems.

RD CFO Budget Request – N/A. RD staff uses the data in this application for internal use.

CRAMS – the complaints may be transmitted or disclosed by electronic format (email), or by telephone. The electronic documents are maintained in CRAMS. The case record and information are updated daily. Information is shared as requested and as part of case processing and closure procedures with Office of Assistant Secretary for Civil Rights (OASCR). All complaint files and any PII information is encrypted and password protected prior to sharing with any internal or external agencies.

GUS2 – The application has a SAML connection with USDA eAuthentication and uses SSL v3.0 and TLS v1.2 (REST API) with all services called in MuleSoft (see Section 4.1 for list of services). The application sends data to TDW via Informatica using token-based authentication (username and password) for ETL; the connection uses TLS 1.2 and 256-bit encryption.

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.

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 the implementation of RD policies, standards and procedures.

MITIGATION:

RDForce leverages Salesforce Shield to mitigate privacy risks and encrypt the data at rest for the RDForce applications hosted on the Salesforce platform. Platform Encryption allows RD to retain critical application functionality, like search, workflow, and validation rules to maintain full control over encryption keys and set encrypted data permissions to protect sensitive data from unauthorized users. Platform Encryption will natively encrypt sensitive data at rest across all RDES applications. The platform encryption process uses symmetric key encryption and a 256-bit Advanced Encryption Standard (AES) algorithm using CBC mode, and a randomized, 128-bit initialization vector (IV) to encrypt field-level data and files stored on the Salesforce Platform.

Encryption will be enabled in the Salesforce application prior to deployment to Production and prior to writing any data to the Production database. Therefore, the relevant data that must be encrypted per configuration workbook will not need to be encrypted after it's written to the database, mitigating risk that encryption only works after a field is touched.

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?

Resource 1 – RD employees use the information internally but may occasionally use the system to send an email to an external contact.

ReConnect – integrates with Google Analytics API: Integrating with the GSA approved Digital Analytics Platform (DAP). Google Analytics with Inform Portal (Salesforce) Customer Community to track search activity such as article views, page views, and object views. This feature transfers customer data to a third party, Google Analytics.

HBIIP – RD will provide shared data and system access to the Department of Energy's (DOE) National Renewable Energy Laboratory (NREL) for NREL reviewers to provide analysis of grant applications.

OneRD Portal – N/A. RD staff uses the data in this application for internal use.

RD CFO Budget Request – N/A. RD staff uses the data in this application for internal use.

CRAMS – Inquiry and/or Complaint information is shared with HUD (under the MOU between USDA and HUD), DOJ (information related to civil rights complaint and compliance matters), Federal Mediation and Conciliation Service (FMCS) (age related Inquiries and/or Complaints), if applicable, to provide assistance in the resolution of said matters. In addition, Complaint files are transferred to the Federal Records Center (FRC) at the end of the specified cut-off period, in accordance with RD 2033-A, Records Management, Exhibit U, Civil Rights Record Retention Procedure.

GUS2 – Information will be shared with MuleSoft to pass to external non-USDA services, including API References listed below:

Service Name	Description	Purpose
Total Scorecard API	A service that uses a statistically derived algorithm developed by HUD to evaluate borrower credit history and application information.	evaluate borrower credit history and application information
SAVE API	Interacts with all endpoints used for DHS SAVE	SSN will be used for the purpose of verifying citizenship and immigration status of non-citizen, naturalized or derived U.S. citizen applicants applying for USDA Housing Assistance, Housing Grants, Housing Loans, Loan Guarantees and Rent Assistance
FNMA API	Accepts a GUS credit report Request for Fannie Mae	data is used by the decision engine to assist in the final rating of a borrower application
CAIVRS API	Retrieves CAIVRS authorization numbers for the given borrower's data	Social Security Number (SSN) will be used to retrieve CAIVRS number and Borrower ID (the SSN is obfuscated)

Of the above services, shared information includes PII for CAIVRS (HUD), SAVE (USCIS), Total Scorecard (HUD), and Fannie Mae (Credit Report).

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, any sharing of PII by any components of RDForce with external entities is consistent with routine uses of sharing of PII data under USDA/RD-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?

Resource 1 – RD employees use the information internally but may occasionally use the system to send an email to an external contact.

ReConnect – Integrates with the GSA approved Digital Analytics Platform (DAP).

HBIIP – Memorandum of Agreement (MOA) with NREL permits NREL users to access the HBIIP system to log in and provide an analysis of the grant application.

OneRD Portal – N/A. RD staff uses the data in this application for internal use.

RD CFO Budget Request – N/A. RD staff uses the data in this application for internal use.

CRAMS – Complaint files are sent electronically, by email, to HUD, DOJ or FMCS. In addition, Complaint files may be sent electronically, by email, to OASCR. PII information is only provided in instances when the information is vital to the processing of an Inquiry or a Complaint. All complaint files and any PII information is encrypted and password protected prior to sharing with any internal or external agencies.

GUS2 – All transmissions with external services flow through MuleSoft via SSL v3.0 and TLS v1.2 (REST APIs); a list of external services is in Section 5.1. The Interconnection Security Agreements (ISAs) or Memorandum of Understanding (MOU) for the GUS2 RDForce components are in CSAM and maintained by RD Cybersecurity.

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 PII information.

MITIGATION:

The risk is mitigated by the connection types, field encryption/masking and Salesforce Shield for RDForce components hosted on the Salesforce platform at USDA.

RDForce leverages Salesforce Shield to mitigate privacy risks and encrypts the data at rest. Platform encryption allows RDES to retain critical application functionality, like search workflow and validation rules, maintain full control over encryption keys and set encrypted data permissions to protect sensitive data from unauthorized access. Platform encryption will natively encrypt sensitive data at rest across all RDES applications. The platform encryption process uses symmetric key encryption and a 256-bit Advanced Encryption Standard (AES) algorithm using CBC mode, and a randomized, 128-bit initialization vector (IV) to encrypt field-level data and files stored on the Salesforce Platform. SSL and TLS provide endpoint security.

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, under USDA/RD-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs. https://www.govinfo.gov/content/pkg/FR-2019-05-14/pdf/2019-09874.pdf

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

Resource 1 – RD employees will log into Resource 1 to provide information and are provided with a privacy notice prior to the collection of their information. In addition, RD employees may be notified by their Supervisor when system information is being collected.

ReConnect – Users/applicants will log into the ReConnect system and are provided with a privacy notice prior to collection of the application data.

HBIIP – Users/applicants will log into the HBIIP system and are provided with a privacy notice prior to collection of the application data. In addition, external partner agency users from NREL will sign Non-Disclosure Agreements (NDAs), prior to being granted access to the system.

OneRD Portal – Employees/Contractors will log into OneRD Portal and are provided with a privacy notice prior to collection of their information. In addition, RD employees and RD contractors are provided with notice of the use of their information at the time of their initial employment with RD.

RD CFO Budget Request – N/A. Budget request and any supplemental or supporting information will not contain information regarding an individual that is not an RD employee or RD contractor.

CRAMS – AD-3027, USDA Program Discrimination Complaint Form contains a privacy notice regarding information collected in connection with the complaint. Said information is

covered under Privacy Act of 1974, 5 U.S.C. §552a. In addition, the USDA Privacy Policy is posted on the Program Complaint Processing and Resolution Branch webpage that provides instructions on how to file a Program Discrimination complaint.

GUS2 – Notice was provided to individuals by the initial source systems prior to collection or processing of the information. RDForce was 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?

Resource 1 – The users can voluntarily add personal information in Resource 1.

ReConnect – The users will voluntarily enter the business information in ReConnect.

HBIIP – A user doesn't have to enter information and submit an application, but a complete application must be submitted to be eligible to receive an HBIIP Grant. If a customer accepts an HBIIP grant, they then agree to provide information about the execution of the project and use of the grant funds as well as information about additional Higher Blended fuel sold due to the grant.

OneRD Portal – The users can voluntarily add personal information in OneRD Portal. There are no mandatory required fields within the employee profile.

RD CFO Budget Request – N/A. Budget request and any supplemental or supporting information will not contain information regarding an individual that is not an RD employee or RD contractor.

CRAMS – The information provided by Inquirers or Complainants is on a voluntary basis. Failure or refusal to provide required information may impact the decision rendered or action taken by the agency.

GUS2 – 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. RDForce was 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?

Resource 1 – The users can voluntarily add personal information in Resource 1. There are no mandatory required fields within the employee profile. The employee can voluntarily provide as much or as little information as they want to share.

ReConnect – The users can voluntarily add business information in ReConnect. To be considered for a loan or grant, there may be some required fields to complete.

HBIIP – In order to apply for an HBIIP Grant, customers must provide data on a proposed project, including its proposed cost and impact. If selected for a Grant, customers must provide information on when the funds were spent, and the additional Higher Blended fuel sold.

Customers can choose whether to provide the information and be eligible for a grant and if selected must chose to accept the terms of the grant obligation.

OneRD Portal – The users can voluntarily add personal information in OneRD Portal. There are no mandatory required fields within the employee profile. The employee can voluntarily provide as much or as little information as they want to share.

RD CFO Budget Request – N/A. Budget request and any supplemental or supporting information will not contain information regarding an individual that is not an RD employee or RD contractor.

CRAMS – The information provided by Inquirers or Complainants is on a voluntary basis. The information provided by the Inquirer, Complainant or Respondent will only be shared with persons who have an official need to know and will be protected from public disclosure pursuant to the provisions of the Privacy Act, 5 U.S.C. § 552a(b). Failure or refusal to provide required information may impact the decision rendered or action taken by the agency.

GUS2 – 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. RDForce was 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.

Resource 1 – Users enter their own profile information and are provided training upon granted access.

ReConnect – Users/applicants will log into the ReConnect system and are provided with a privacy notice prior to collection of the application data.

HBIIP – Users/applicants will log into the HBIIP system and are provided with a privacy notice prior to collection of the application data. In addition, external partner agency users from NREL will sign Non-Disclosure Agreements (NDAs) prior to being granted access to the system.

OneRD Portal - RD employee data is provided as part of employment with USDA. When an RD employee is onboarding with USDA, they are consenting to the use of employment data with USDA, including being added to Active Directory and vetted as a federal employee with USDA. RD employee data in OneRD Portal is protected in accordance with USDA security requirements, which follow OMB and federal agency requirements. In addition, RD employees and RD contractors who log into OneRD Portal are provided with a privacy notice prior to collection of their information.

RD CFO Budget Request – N/A. Budget request and any supplemental or supporting information will not contain information regarding an individual that is not an RD employee or RD contractor.

CRAMS – Notice is provided to individuals by the initial source systems or during the collection or processing of the information that is not collected during the submission of the

Complaint by the individual, using the AD-3027 Complaint Form. AD-3027, USDA Program Discrimination Complaint Form contains a privacy notice regarding information collected in connection with the complaint. Said information is covered under Privacy Act of 1974, 5 U.S.C. §552a. In addition, the USDA Privacy Policy is posted on the Program Complaint Processing and Resolution Branch webpage that provides instructions on how to file a Program Discrimination complaint.

GUS2 – 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?

Resource 1 – RD employees have access to the information they added in Resource 1. They will follow the appropriate process to correct the information, including notifying RD admins to correct inaccurate information, if necessary.

ReConnect – business application information is provided by the business point of contact. Although the user's name and business address are collected, additional PII information is not collected, maintained and used to meet RD mission and business needs of providing loans and grants to qualified broadband business entities in rural communities.

HBIIP – business application information is provided by the business point of contact. PII information is not collected, maintained, and used to meet RD mission and business needs of providing grants to qualified business entities in rural communities.

OneRD Portal – RD employees and RD contractors will have access to OneRD Portal by default. When a RD employee logs in with eAuthentication, they will have access to their profile page and any requests they have made through OneRD Portal. They will follow the appropriate process to correct the information, including notifying any RD staff (RDForce admins) to correct inaccurate information.

RD CFO Budget Request – The public does not have direct access to RD CFO Budget Request. RD employees or RD contractors would notify RD staff to correct inaccurate information, if necessary.

CRAMS – The individual may file a Freedom of Information Act (FOIA) request. The requester must provide specific information regarding their request and they will be provided a copy of the agency records that are subject to disclosure.

GUS2 – The public does not have direct access to GUS2. USDA RD employees, system administrators, and trusted lenders/lender agents have access to the information in GUS2. Data inaccuracies within the GU2 may be corrected by lenders with authorization or USDA staff, who have authorized access to correct any data inaccuracies brought to their attention by RD borrowers or applicants.

In addition, 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, and 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?

Resource 1 – RD employees and system administrators would be able to correct most inaccurate or erroneous information that was input into the system.

ReConnect – Individual users providing business applicant information have access to the application and can correct inaccurate or erroneous information. In addition, RD employees managing ReConnect provide workflow management and support to ReConnect customers and will work with the business applicant users to correct any data inaccuracies.

HBIIP – Data fields submitted by the customer are only editable by the customer up until the point of submission. After submission, fields are not editable unless the application is reverted to an unsubmitted status by an RDForce administrator, during an application window.

OneRD Portal – Specific fields in the employee profile page are editable by the employee for OneRD Portal. Other fields are not, because the data is brought in from an authoritative system (Active Directory) and is managed by authorized privileged users. Errors in these fields will follow the process for correcting the data in Active Directory, which follows RD account management processes and has audit trails in Salesforce of the OneRD Portal information that is updated.

RD CFO Budget Request – The public does not have direct access to RD CFO Budget Request. RD employees or RD contractors would notify RD staff to correct inaccurate information, if necessary.

CRAMS – Inaccurate or erroneous information can be corrected by the RD User. CRAMS does not allow deletion of information unless a request is made by the System Manager to the System Administrator.

GUS2 – The public does not have direct access to RDForce; trusted lenders/lender agents have access to the information in GUS2. Data inaccuracies within the GU2 may be corrected by

lenders with authorization or USDA staff, who have authorized access to correct any data inaccuracies brought to their attention by RD borrowers or applicants.

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.

Customers and employees may also contact:

USDA Rural Development Primary FOIA Contact Information:

Lolita Barnes
FOIA Liaison
1400 Independence Ave., SW
Washington, DC 20250
Tel. 202-692-0004
Email: lolita.barnes@usda.gov

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

Resource 1 – RD employees would have access to the information that they added to the system and can correct their information accordingly or can notify Resource 1 admins to assist them with any corrections.

ReConnect – Individual users providing business applicant information have access to the application and can correct their information. In addition, 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.

HBIIP – 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.

OneRD Portal – Users have access to the system and can correct their information accordingly or can notify RDForce admins to assist them with any corrections.

RD CFO Budget Request – RD employees or RD contractors would notify RD staff to correct inaccurate information, if necessary.

CRAMS – RD System Users (CR Office Staff) have received training and the CRAMS SOP provides additional guidance. The public does not have direct access to CRAMS. 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.

GUS2 – The public does not have direct access to RDForce. For data originating in source systems, source system owners must define the notification procedures to the Individuals. Individuals are also 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?

Resource 1 – RD employees have access, redress, and amendment rights under the Privacy Act and USDA employment processes for correcting information that is inaccurate.

ReConnect – Individual users providing business applicant information have access, redress and amendment rights to the application. In addition, users 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.

HBIIP – 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.

OneRD Portal – Individuals have access, redress, and amendment rights under the Privacy Act and USDA employment processes for correcting OneRD Portal data that is inaccurate.

RD CFO Budget Request – Individuals do not have access to the system and no redress is provided. RD CFO Budget Request is an internal tracking system used by the RD Budget team.

CRAMS – Individuals do not have access to the system and no redress is provided. CRAMS is an internal tracking system used by the CR Staff. 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.

GUS2 - The public does not have direct access to RDForce. Individuals are also 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.

In addition, individuals have access, redress and amendment rights under the Privacy Act, the Freedom of Information Act and the Fair Credit Reporting Act.

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

Residual privacy risks associated with the redress process for individuals are mitigated, since individuals can use the relevant procedures discussed in paragraph 7.3. No additional risks are associated with the redress process. The requestor may also refer to the RD-1 SORN 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?

Resource 1 – RD Employees access the application after being provisioned in eAuthentication by a User Access Management (UAM) ticket, created by the System POC and completed by the UAM Team (UAMT). Each state has their own system of documenting such requests.

ReConnect – public, non-authenticated, users may access the system, however authorized users that will provide information for the entity applicants, will be required to obtain an eAuth Level 2 account to access the system; RD Active Directory users will be granted the "RD Employee" Salesforce profile, which will provide read access to the system. Privileged access will be set by Salesforce Groups, which will be maintained through the User Access Management System.

RD Employees access the application after being provisioned in eAuthentication by a User Access Management (UAM) ticket, created by the System POC and completed by the UAM Team (UAMT).

The System Point of Contact (POC) assigns group membership and individual permissions and access; the POC is responsible for verifying user verification.

HBIIP – An eAuth Level 2 account is required to gain access to HBIIP.

RD CFO Budget Request – RD employees and RD contractors access the application after being provisioned in eAuthentication by a User Access Management (UAM) ticket, created by the System POC and completed by the UAM Team (UAMT).

The System Point of Contact (POC) assigns group membership and individual permissions and access for RDForce applications; the POC is responsible for verifying user identification.

OneRD Portal – An eAuth Level 2 account is required to gain access to OneRD Portal.

CRAMS - RD Active Directory users will be granted the "RD Employee" Salesforce profile, which will provide read access to the system. Privileged access will be set by Salesforce Groups, which will be maintained through the User Access Management System.

RD Employees access the application after being provisioned in eAuthentication by a User Access Management (UAM) ticket, created by the System POC and completed by the UAM Team (UAMT).

The System Point of Contact (POC) assigns group membership and individual permissions and access; the POC is responsible for verifying user verification.

GUS2 – RD Active Directory users will be granted the "RD Employee" Salesforce profile, which will provide read access to the system. Privileged access will be set by Salesforce Groups, which will be maintained through the User Access Management System.

RD Employees access the application after being provisioned in eAuth by a User Access Management (UAM) ticket, created by the System POC and completed by the UAM Team (UAMT).

The System Point of Contact (POC) assigns group membership and individual permissions and access; the POC is responsible for verifying user verification.

Lender users would be first provisioned in AASM, then in Salesforce by just-in-time provisioning. Approved lenders will access the Salesforce Partner Portal, an authenticated

web page (HTTPS), to complete the mortgage application intake process. This authentication will require lenders to obtain a Level 2 USDA e-Authentication account and AASM user account (created by the Lender/Branch Security Administrators in AASM). Salesforce will receive AASM account information as part of login process and provision the lenders with a Salesforce community user license/role. These users will be activated as a partner contact for their Lender account in the Salesforce Partner Portal. The application uses Adobe Livecycle (AEM) for forms and ECF for document management. There will be an exemption in place through July 2020 allowing lenders to access the application with a Level 1 e-Authentication account in addition to Level 2.

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?

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-ICS. Training must be completed with a passing score prior to access to a USDA RD system. All RD employees/contractors are required to complete ISAT, which includes privacy training on an annual basis.

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

Yes, RDForce has an ATO, which is valid until 4/6/2023.

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

The NIST 800-53 rev 4 controls for the RDForce system are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls 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: A privacy risk associated with RDForce could be extracting and using the information erroneously. Since RDForce is used by authorizing RD personnel and other authorized users using eAuthentication and there are group access management controls, the privacy risks are minimal.

MITIGATION: 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 DISC 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.

Risk is mitigated by enabling Salesforce system event monitoring. The application collects auditable events and makes these events available to system administrators in event log files. Auditable events may include logins, logouts, web clicks, page loads, API calls, Apex executions, and report exports. Salesforce field audit history tracking may also be enabled based on system owner requirements.

Salesforce Security Incident Event Management process is detailed at this link:
https://help.salesforce.com/articleView?id=000313354&language=en_US&type=1&mode=1

RD Security runs code scans prior to releases to Production. Salesforce also has security audits they perform on a periodic basis; additional information on security and privacy architecture can be found at this link:
https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf

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?

Resource 1 – information is collected, maintained and used to facilitate communication and correspondence with new and existing RD employees. Resource 1 information includes accounts, contracts and associated programs, RD events and outreach organizations.

ReConnect – is a public facing website/portal that leverages the Salesforce Customer Community Cloud for qualified broadband business entities to provide business information to apply for loans and grants in rural communities.

HBIIP – HBIIP is an automated grant application and grant tracking tool to evaluate and make award determination to fuel operators.

OneRD Portal – used for internal workflow management for RD employees.

RD CFO Budget Request – is an end-to-end Cloud-based application that provides a secure, scalable, enterprise-level, web-based application for efficiently tracking budget requests. It provides the complete capability to create, manage, track, and report on all Budget requests by fiscal year.

CRAMS – CRAMS is the Civil Rights Complaint tracking system used by the Civil Rights Team to track all the fields and functionality of day-to-day action. CRAMS is designed to make it easier to input, track, and report civil rights inquiries and complaints, and to connect with internal and external customers.

GUS2 – GUS2 is a web application that provides a streamlined and automated loan application intake process, automated credit decision-making, and automated eligibility determination for the SFH guaranteed rural housing loan program.

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

No, Salesforce uses the following methods to keep data private and prevent data loss:

- SSL v3.0 and TLS v1.2 to establish secure connections and encrypt data
- Hosting in a secure server environment utilizing firewall to prevent unauthorized access
- Customer data backups
- Advanced security methods and encoded session IDs to store confidential user and session information
- DNS and IDS
- Others, including DNSSec services used with USDA

The full Salesforce privacy policy can be found here:
https://www.salesforce.com/company/privacy/full_privacy/

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?

RDForce is built on the Salesforce platform and the Mule Cloud platform; the Lender Intake modules will integrate with MuleSoft to leverage internal and external services.

RDForce is using the SalesForce platform as a service (PaaS) and software as a service (SaaS) package which provides customers with a platform to develop applications on-demand. The SaaS offerings are applications built by SalesForce and available for tailoring to meet specific business needs.

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

GUS2 – PII will be available through Salesforce's interconnection with MuleSoft to support the loan application review and underwriting. PII and sensitive data are transmitted through MuleSoft for the following services:

- CAIVRS (HUD): Request and Response include SSN
- SAVE (USCIS): Request includes Alien Number, I-94 Number, Visa Number, Card Number, Borrower Name, Birthdate, Phone; Response includes Citizen Name, Birthdate, Citizenship Information
- HUD Total Scorecard: Request includes Borrower SSN and demographics, Credit Report and loan application financial calculations; Response includes Borrower SSN
- Fannie Mae Credit Report: Request includes Borrower SSN, Name, Address; Response includes Fannie Mae Credit Report, including Borrower info and borrower's financial and credit information

- Account Cross Reference: Request includes SSN; Response includes USDA Borrower ID
- FICO Blaze: Request includes Borrower ID, loan and financial information; Response includes Borrower ID
- Adobe LiveCycle: Request incudes all loan information; Response is comprised of a populated pdf form including all loan information.
- AASM: Request includes Login ID, eAuth ID, Username, Email Address; Response includes USDA Org information (e.g. Lender bank, branch, role), TIN
- GLS: Request includes all Borrower loan application information.

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

GUS2 – PII and sensitive data made available through MuleSoft will be used to assess the loan application and borrower's credit worthiness and risk, and support RD's underwriting decision-making process. Further, PII made available by specific integrations may be used in other integrations.

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?

RDForce leverages Salesforce Shield to encrypt the data at rest. Platform Encryption allows RD to retain critical app functionality, like search, workflow, and validation rules maintain full control over encryption keys and can set encrypted data permissions to protect sensitive data from unauthorized users. Platform Encryption will natively encrypt sensitive data at rest across all RD applications.

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

Salesforce is FedRAMP certified, as such, it complies with security requirements for data protection for federal agencies.

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

Other than the sources identified in 10.3, above, there are no other authorized users who will have access to RD PII through third party 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?

Other than the sources identified in 10.3, above, the PII information will not be shared internally or externally.

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)?

No, the purposes and uses of RDForce are identified in RD-1.

10.10 Does the system use web measurement and customization technology?

Salesforce utilizes cookies to perform web measurement and customization. Specifically, session-based cookies (within a single internet browser session) and persistent cookies (cross-browser sessions) are used to compile information on the user to track usage, determine system preferences and customize pages as set by the user.

The eAuthentication system uses cookies for Single Sign-On. When a user logs into an application, eAuthentication issues a token to the user in the form of cookies to be able to authenticate the user to that application.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Yes.

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?

Salesforce functional cookies enhance functions, performance, and services in the Salesforce system; users may opt out of functional cookies. Required cookies are necessary for basic website functionality (e.g. authentication cookies, security cookies, etc.); users may not opt out of required cookies.

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.

Salesforce Shield is used to encrypt data at rest (see Section 10.5 for additional details). Interconnections with MuleSoft use two-way SSL v3.0 and TLS v1.2 (REST API) and HTTPS to protect data in transit.

There is minimal risk because data is protected by Salesforce encryption. Salesforce follows USDA security and privacy requirements and is FedRAMP certified.

Responsible Officials

ANGELA COLE

Digitally signed by ANGELA COLE
Date: 2021.02.10 16:00:30 -05'00'

Angela Cole

Information Security Systems Program Manager (ISSPM)

USDA Rural Development

Approval Signature

KELLI PETRIE

Digitally signed by KELLI PETRIE
Date: 2021.02.10 16:19:52 -05'00'

Kelli Petrie

Information System Owner

USDA Rural Development