Privacy Impact Assessment
RDForce

- Version: 4.0
- Date: 5/11/2023
- Prepared for: USDA Rural Development (RD)

USDA
United States Department
of Agriculture

Privacy Impact Assessment for the RDForce

5/11/2023

Contact Point

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

Abstract

RDForce is a Salesforce platform-based information system used by Rural Development. 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). RDForce contains several modules two of which process PII: CRAMS, GUS2.

Overview

RDForce is a Salesforce platform-based information system used by Rural Development. 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). RDForce contains several modules, three of which process PII: CAMs, CRAMS, GUS2.

Congressional Announcement Management System (CAMS) The Congressional Announcement Modernization (CAM) project has been transferred into a new Salesforce application called Congressional Announcement Management System (CAMS), that will replace the current Congressional Announcement Tracking System (CATS). The solution will enable the standardization and transparency of data throughout the loan origination and obligation process to support communications managed by The Office of External Affairs (OEA). CAMS is implemented on the internal Rural Development (RD) Salesforce platform. It will enable internal users in RD Office of External Affairs (OEA) to perform various actions which include creation, review, and publishing the Congressional Announcements. CAMS will provide the ability for RD OEA users to access information centrally, route information, and maintain data integrity. The platform solution will use the USDA eAuthentication that enables individual employees to obtain an account that allows them access to USDA Web applications via the internet. Users will also be able to use their MobileLinc Credential (PIV-derived) on USDA authorized mobile devices to access CAMS via the internet. Mobile Linc is through ICAM offered by USDA. The application processes PII of borrowers (names, account numbers, signature of release).

Civil Rights Automated Management System (CRAMS) replaced the two applications (MPC and PCRRA) which supported USDA RD Civil Rights staff (National and State offices) activities. The purpose of CRAMS is to automate the functionality for the RD Civil Rights staff to track inquires, complaints and compliance issues involving RD program borrowers regarding federal civil rights statutes and program issues violations both programmatic and of a civil rights nature. 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), Section 504 of the Rehabilitation Act of 1973 and Age reports. 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), external customers for discriminatory complaints against RD programs and affiliates. This system processes PII.

Guaranteed Underwriting System2 (**GUS 2**) is a Salesforce application that captures borrower loan application data for USDA-guaranteed single-family home loans. The purpose of GUS2 is to facilitate a streamlined and automated application process, credit decision-making, and eligibility determination for the SFH guaranteed rural housing loan program. GUS 2 is designed to transition the GUS (Legacy) intake process. GUS2 processes PII.

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?

<u>CAMS:</u>

PII collected from program participants.
Data Elements:
- Names
- Account Number
- Signature

<u>CRAMS:</u>

PII collected, processed or stored on:
- USDA Employees
- Other – Program Participants
Data Elements:
- Name
- Date of Birth
- Address Information
- SSN
- Financial data
- Health data
- Criminal data
- Employment History
- Agency assigned and case numbers.
- Photographic Image
- Handwriting or image of the signature

<u>**GUS2:**</u>

PII collected from program participants.
Data Elements:
- Name
- Date of Birth
- Address Information
- SSN
- Financial data
- Employment History
- Agency assigned and case numbers.
- Other – military, demographic data

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

CAMS – from congressional offices who obtain consent from program participants to inquire about the loan/obligations.

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)
- *Internally*: AASM, GLS, Property Eligibility, Income Eligibility, Annual Fee Amortization Schedule, FICO Blaze, ECF Document Management, Adobe Lifecycle (AEM), Account Cross Reference (ACR)
- *Externally*: CAIVRS (HUD), SAVE (USCIS), HUD Scorecard (HUD), Fannie Mae Credit Bureau

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

CAMS – The information is collected as part of the Congressional Announcement project to showcase the number of loans from USDA/RD have been granted in specific congressional districts.

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, and complaints as well as connect with internal and external customers. CRAMS tracks information and allows for reporting on work that has previously been not trackable. 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?

CAMS – The information is collected from the source systems, Guaranteed Loan System (GLS), Commercial Loan Servicing System (CLSS), Program Loan Accounting System (PLAS), Agricultural Management Assistance (AMA) & the Tabular Data Warehouse (TDW). The data is pushed into CAMS via the Consolidated Data Mark (CDM).

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 – information is collected via user input; directly into the Salesforce UI; trusted lenders and lender agents; and 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?

CAMS – The information will be verified through filed-level validations and the CAMS Process Workflow by the Office of External Affairs (OEA) Public Information Officers (PIA) and the Mission Areas.

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.

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
- 7 CFR Part 15, Nondiscrimination
- Title VI of the Civil Rights Act of 1964 (42 U.S.C. § 2000d)
- Sections 504 and 508 of the Rehabilitation Act of 1973 (29 U.S.C. §§ 790-790f) and any other anti-discrimination statutes, rules and regulations.

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

MODERATE RISK: Current risk are associated with the potential unauthorized disclosure or illegal use of PII, and information contained in civil rights complaints and the potential adverse consequences this disclosure or use would have on the customer and USDA employees.

MODERATION: 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.

CAMS – The data is used to provide timely and accurate announcements to Congressional Offices and Members of Congress.

CRAMS – The information is 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?

CAMS – There are no tools that are used to analyze the data.

CRAMS – Microsoft Excel to create charts, graphs, etc.

GUS2 - FICO Blaze to evaluate the data based on the rules, render an underwriting recommendation and findings.

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

CAMS – N/A

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 for comparative purposes to assist with the assessment of the complaint.

GUS2 – N/A

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

CAMS - System is accessible only by RD employees via eAuthentication with role-based access. The system tracks the history of changes (i.e. edits by the user).

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 Partner Portal 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).

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?

CAMS – The system is currently unscheduled, therefore records in the system must be maintained as if permanent.

CRAMS – The system is currently unscheduled, therefore records in the system must be maintained as if permanent. Additionally, records pertaining to public-facing Civil Rights complaints maintained outside the system are also unscheduled. Disposition is not authorized for those records.

GUS2 – RD GRS 2033a SFH Exhibit O

LOANS: 7 years after Cutoff
Approved:

- Line 6 – Sec 502 (Direct Single Family Housing Loans) DAA-0572-2017-0001-0006
- Line 8 – Sec 502 (Self-Help Housing Loans), DAA-0572-2017-0001-0008
- Line 7 – Sec 504 (Direct Rehabilitation Loans) DAA-0572-2017-0001-0007

Rejected, withdrawn, canceled, or expired: Line 4, DAA-0572-2017-0001-0004

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

CAMS – No

CRAMS – No

GUS2 – Yes

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

MODERATE RISK: The risk is associated with 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: Access controls are in place to reduce unauthorized access.

CAMS - System is accessible only by RD employees via eAuthentication with role-based access.

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 Partner Portal 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).

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?

CAMS – N/A, information is only processed within Rural Development

CRAMS: Information is shared with CRMS (Assistant Secretary database but only cut/paste) to keep the Administration informed the status of RD complaints.

GUS2 – N/A, information is only processed within RD.

4.2 How is the information transmitted or disclosed?

CAMS – N/A, information is kept within Rural Development

CRAMS: Information is shared by cutting and pasting into the CRMS database.

GUS2 – N/A, information is kept within Rural Development.

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.

LOW RISK: The risk is associated with the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the client. The risk is low considering only **CRAMS** authorized users have access to the information that is cut and pasted into the CRMS separate database. Once the information is released to CRMS, RD no longer has control of further exposure.

MITIGATION: Access controls are in place to reduce unauthorized access. **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). The system has implemented the relevant National Institute of Standards and Technology (NIST) 800-53 controls to prevent unauthorized access. Systems and Communication Protection controls are in place to prevent unauthorized access.

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?

CAMS – Produces announcements that are shared with Congressional Offices and Members of Congress.

CRAMS – Inquiry and/or Complaint information is shared via hardcopy 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.

GUS2 – shares information with CAIVRS (HUD), SAVE (USCIS), Total Scorecard (HUD), and Fannie Mae (Credit Report).

- CAIVRS number and Borrower ID (the SSN is obfuscated); SSN are used to prescreen for any debts owed or loans guaranteed by the Federal government to ascertain if the applicant is delinquent in paying a debt owed to or insured by the Federal government.
- SAVE – Request includes alien number, I-94 number, visa number, card number, borrower name, birthdate, phone; response includes citizen name, birthdate, citizenship information. Sharing is done for the purpose of verifying citizenship and immigration status of non-citizen, naturalized.
- Total Scorecard – Request includes borrower SSN and demographics, credit report and loan application financial calculations; Response includes borrower SSN. Sharing is done for the purpose of evaluating borrower credit history and application information.
- 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. Sharing is done for the purpose of enabling the FICO Blaze decision engine to assist in the final rating of a borrower application.

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.

CAMS – Yes, under USDA/RD-1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs, Routine Use No. 2

CRAMS – USDA/OASCR–2, Civil Rights Management System (CRMS); and USDA/RD-1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs

GUS2 – Yes, under USDA/RD-1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs, Routine Use No. 7, 14, 26.

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

CAMS – N/A

CRAMS – N/A

GUS2 – All transmissions with external services flow through MuleSoft via SSL v3.0 and TLS v1.2 (REST APIs).

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

MODERATE RISK: The risk to external information sharing would be the unauthorized disclosure of PII information. **GUS2** moderate risk is associated with the sharing of SSNs, I-94 number, visa number, card number, borrower name, birthdate, phone; response includes citizen name, birthdate, citizenship information, and demographics.

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. 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.

CAMS - Yes, <u>USDA/RD-1</u>.

CRAMS – Yes, <u>USDA/OASCR–2</u>, and <u>USDA/RD-1.</u>

GUS2 – Yes, <u>USDA/RD-1</u>.

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

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

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

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

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

CAMS – 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.

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.

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

CAMS – 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.

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 – Consent of the individuals for particular uses of the information is obtained at the initial source/systems, if required, prior to collection or processing of the information.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

CAMS – 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.

CRAMS – Notice is provided to individuals who file complaints using the AD-3027 Complaint Form. AD-3027, USDA Program Discrimination Complaint Form.

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?

CAMS – The public does not have direct access to GUS2. Individuals gain access from the initial point of collection or via procedures outlined in SORN RD-1.

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. Individuals gain access from the initial point of collection or via procedures outlined in SORN RD-1.

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

CAMS – Inaccurate or erroneous information can be corrected by OEA, PIA and the Mission Areas by Contacting the Source Systems.

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 – 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.

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

CAMS – individuals are notified at the initial point of collection. CAMS is not the initial point of collection.

CRAMS – individuals are notified at the initial point of collection; through USDA/OASCR–2 and USDA/RD-1.

GUS2 – individuals are notified at the initial point of collection. GUS2 is not the initial point of collection.

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

N/A, redress is outlined under Record Access Procedures in both USDA/OASCR–2 and USDA/RD-1.

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

There is no additional risk associated with the redress process available to users.

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?

CAMS – 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.

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.

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. 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).

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?

All RD employees and contractors are required to complete an annual training. In addition, all RD employees and contractors are required to complete annual information security and awareness training, which includes privacy training.

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

Yes, RDForce has an ATO, which is valid until 3/9/2026.

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

The NIST 800-53 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 These controls, including full compliance, inheritance and risk acceptance descriptions, are available in Cyber Security Assessment and Management (CSAM).

8.6   <u>Privacy Impact Analysis</u>: 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?

MODERATE RISK: A privacy risk associated with RDForce is associated with 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 reduced.

MITIGATION: 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.

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?

CAMS – A web application that provides a modernized Congressional Announcement System that tracks and produces announcements to inform Congressional Offices and Members of Congress on the effective use of Appropriated USDA/RD funds to the benefit of their constituents.

CRAMS – 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 – 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.

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.

CAMS – N/A, there are no 3rd party websites or applications.

CRAMS – PII will be available through Salesforce's interconnection with MuleSoft to support civil rights investigations.

GUS2 – PII will be available through Salesforce's interconnection with MuleSoft to support the loan application review and underwriting.

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

CAMS – N/A, there are no 3rd party websites or applications.

CRAMS – N/A

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.

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?

Additional internal applications will have access to PII:

- eServices Area Boundary - Account Cross Reference (ACR): Request includes SSN; Response includes USDA Borrower ID
- Common Call Controls (CCC) Area Boundary – FICO Blaze: Request includes Borrower ID, loan and financial information; Response includes Borrower ID

- eForms Area Boundary – Adobe LiveCycle: Request incudes all loan information; Response is comprised of a populated pdf form including all loan information.
- Guaranteed Loan System (GLS) Area Boundary: Request includes all Borrower loan application information.

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?

No. 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.

MODERATE RISK: The risk associated with the use of 3ʳᵈ party applications and service deals with the amount and quality of PII. **CRAMS** and **GUS2** contain sensitive PII.

MITIGATION: The risk is mitigated using Salesforce Shield. This 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.

Approval Signature

Signed copy kept on record.