Privacy Impact Assessment
Common Call Component (CCC)

- Version: 4.0
- Date: April 25, 2023
- Prepared for: USDA Rural Development (RD)

Privacy Impact Assessment for the Common Call Component

April 25, 2023

Contact Point

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

Abstract

Common Call Component includes BRE (Business Rules Engine)/FICO Blaze and ECF/Imaging. BRE/FICO Blaze Advisor is a business rule management system, which enables business analysts, system analysts, application architects, and developers to create, manage, integrate, test, and deploy business rules. Electronic Customer File (ECF) / Imaging is a project designed to manage the electronic filing and retrieval of loan and grant documents for all Rural Development (RD) programs. This PIA is required because there is PII data in ECF/Imaging and the PTA determined that a PIA is required.

Overview

Common Call Component application, **Q-Action/Electronic Customer File (ECF)/ Imaging** (**ECF/Imaging**), is an internal document repository hosted at USDA. ECF/Imaging manages the electronic filing and retrieval of loan and grant documents for all Rural Development (RD) programs. Currently ECF contains over 40 terabytes of loan documents for the Single-Family Housing Direct and Guaranteed portfolio. The purpose of ECF is to introduce flexibility for RD Program Staff to retrieve loan and grant documents from a borrower level down to documents pertaining to a specific loan or grant. This structure provides the capability for users to view documents for a specific borrower that may span across different program areas in a single search.

ECF/Imaging uses scanning software and equipment to index, store and retrieve electronic images of RD loan and grant application documents and related paper requests sent to Rural Development. ECF/Imaging uses, generates, and stores RD grant and loan documents that contain 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?

ECF/Imaging is an internal electronic document/file repository. ECF/Imaging scans, faxes, and imports document images from internal RD loan and grant systems that contain the following information:

- Name
- Date and/or place of birth
- Address Information
- Personal identification number (SSN/TIN)
- Financial data

- Employment history
- Miscellaneous identification numbers
- Handwriting or an image of the signature
- Photographic image/identifying characteristics

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

ECF/Imaging receives information internally from the following systems: CLP Originations - New Loan Originations (NLO); CLP Servicing; 2 of 7 – Business intelligence; CLP Servicing; 3 of 7 - Guaranteed Loan System (GLS); CLP Servicing; 4 of 7 – LoanServ; CLP Servicing 5 of 7 – Multi-Family Integrated System (MFIS); RDForce.

Additionally, all USDA National, State and Field offices can add documents to the ECF document repository system.

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

ECF/Imaging is an internal electronic document/file repository used by RD for processing loan and grant applications.

1.4 How is the information collected?

ECF/Imaging documentation is collected from RD internal applications or scanned in by authorized RD staff.

1.5 How will the information be checked for accuracy?

Per 1.4, ECF/Imaging collects information from other RD internal applications. Therefore, accuracy checks are not done within ECF/Imaging since itis not the initial point of collection for PII information.

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

Information contained in ECF/Imaging fall under the following:

- Privacy Act of 1974, as Amended (5 USC 552a)
- Computer Security Act of 1987, Public Law 100-235, ss 3 (1) and (2), codified at 15 U.S.C. 272, 278 g–3, 278 g-4 and 278 h which establishes minimum security practices for Federal computer systems
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, which establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links

agency automated information security programs and agency management control systems;

- Freedom of Information Act, as Amended (5 USC 552), which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.
- Federal Information Security Modernization Act of 2014
- Consolidated Farm and Rural Development Act (7 U.S.C. 1921 et seq) and Title V of the Housing Act of 1949 as amended (42 U.S.C. 1471 et seq).
- Farm Bill 2018 (P.L. 115-334)
- Fair Credit Reporting Act, 15 USC 1681 a(f)
- Consumer Credit Protection Act, 15 USC 1601
- Equal Credit Opportunity Act, 15 USC 1691
- 7 CFR, part 1770, subpart A and part 1773
- RD Records Management Policy
- NARA Records Retention

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

ECF/Imaging system owners define access roles to ensure separation of duties, account management and authorized access to data and information ECF/Imaging. These measures help mitigate the risks to privacy data in ECF/Imaging.

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.

ECF/Imaging collects, generates, and stores RD grant and loan images (documents) that contain PII.

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

ECF/Imaging does not currently use tools to analyze data. Authorized RD staff manually review information to ensure that RD applicant/customer information is accurate and meets the RD and USDA requirements.

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

N/A

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

The controls in place to detect unauthorized access to ECF/Imaging information include DISC audit logs/security logs.

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?

Data retention requirements for the ECF/Imaging are in accordance with NARA, RD Records Management policy (Exhibits N, O, P), and financial compliance regulations.

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

Yes.

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

ECF/Imaging data retention has minimal risk. The RD customer data for ECF/Imaging is protected by USDA federal agency requirements for data protection and is accredited by FedRAMP. ECF/Imaging follow the RD Records Management data retention requirements to manage risk associated with data retention.

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?

ECF/Imaging gets internal data feeds from the data warehouse and internal RD applications. Authorized RD staff can also scan or fax information into ECF using USDA scanning and faxing equipment. ECF/Imaging is an internal document repository for RD.

4.2 How is the information transmitted or disclosed?

ECF/Imaging gets internal data feeds from the internal RD applications and TDW. Authorized RD staff can also scan or fax information into ECF/Imaging using USDA scanning and faxing equipment. Only authorized RD users access ECF/Imaging as well as the internal RD applications and data warehouse that send the data feeds.

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.

The RD customer data for ECF/Imaging is protected by USDA which follows federal agency requirements for data protection and is accredited by FedRAMP.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

N/A.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

N/A.

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

N/A.

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

N/A.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

Yes, it follows Rural Development 1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants and Other Participants in RD Programs, https://www.govinfo.gov/content/pkg/FR-2016-04-28/pdf/2016-09938.pdf.

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

N/A. ECF/Imaging is not the initial point of collect where notice is provided.

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

N/A. ECF/Imaging is not the initial point of collect where the opportunity to decline is provided.

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

N/A. ECF/Imaging is not the initial point of collect where consent is granted.

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.

N/A

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?

N/A. ECF/Imaging is not the initial point of collect where access procedures are provided.

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

N/A. ECF/Imaging is not the initial point of collect where correction procedures are provided.

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

N/A. ECF/Imaging is not the initial point of collect where notice is provided.

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

N/A. ECF/Imaging is not the initial point of collect where redress procedures are provided.

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

N/A

Section 8.0 Technical Access and Security

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

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

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

RD employees and RD contractors' access ECF/Imaging after being provisioned in E-Authentication by a UAM ticket, created by the System POC and completed by UAM.

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

8.2 Will Department contractors have access to the system?

Yes, RD contractors are required to undergo the same access and authentication procedures that RD federal employees follow, as discussed in section 8.1.

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

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

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

Yes.

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

Common Call Component complies with the Federal Information Security Modernization Act of 2014 (FISMA) by documenting the Authorization and Accreditation, annual control self-assessments, and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 4. Common Call Component, ECF/Imaging, is hosted on the DISC platform at USDA, which is FedRAMP certified and uses USDA network security protections.

Access to ECF/Imaging is controlled through Level 2 E-Authentication, and access to sensitive information is controlled through DISC Profiles/Groups on a need-to-know basis with audit logs of user activity for Common Call Component. The User Access Management Team has standard desktop procedures and a roles matrix defining the level of access and how to provision this access to the users for ECF/Imaging. They audit the list of users and applications that they have access to. User Access Management verification reports can be used to verify these groups, are assigned appropriately and account management controls are in place.

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?

Common Call Component is used by internal authorized RD staff and there are group access management controls. The privacy risks are minimal. Potential compromise of privacy data is mitigated by USDA audit event monitoring and network security protections in place to protect RD data for Common Call Component (ECF/Imaging). Additionally, ECF/Imaging is accessed using E-Authentication through the USDA network.

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?

ECF/Imaging uses scanning software and equipment to index, store and retrieve of RD loan and grant application documents and related paper requests sent to Rural Development.

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

No, the project utilizes Agency approved technologies for ECF/Imaging, and these technology choices do not raise privacy concerns.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

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

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

N/A

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

N/A

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

N/A

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

N/A

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

N/A

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

N/A

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Does the system use web measurement and customization technology?

No, ECF/Imaging do not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

10.12 <u>Privacy Impact Analysis</u>: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A

Approval Signature

Signed copy kept on record