Privacy Impact Assessment

Common Call Components

Rural Development (RD)

- July 19, 2016
- Prepared for: RD

United States Department of Agriculture

Abstract

Common Call Components (CCC) is a combination of applications which includes BRE/FICO Blaze and ECF/Imaging.

BRE/FICO Blaze is a business rule management system product suite enabling business analysts, system analysts, application architects, and developers to create, manage, integrate, test, and deploy business rules. BRE/ FICO BLAZE supports loan underwriting and provides business rules throughout the loan and grant lifecycle which contains PII.

ECF/Imaging uses scanning software and equipment providing indexing, storage and retrieval of electronic images of loan application documents and other paper requests sent to the Rural Development. ECF/Imaging uses, generates, and stores grant and loan images (documents) that contain PII.

Overview

Business Rules Engine (BRE) / FICO Blaze
BRE/Fico Blaze is a business rule management system which describes the operations and constraints that that apply to RD achieving its goals, a means to implement strategies, provide tactical details on how the strategy will translate into actions, and designed to manage business actions and decisions for IT systems.

The **Electronic Customer File (ECF)** system consists of two modules which include Retrieval and Indexing.

The **Indexing** module scans, faxes, and imports documents into the image repository are placed in an "Indexing Queue". The users go to a designated website, depending on their business, use the web applications to populate index values for each scanned image. This application then writes these index values to the Electronic Customer File database for future retrieval of the images.

The **Image Retrieval** module scans, faxes, imports and indexes into the image repository and can be viewed in the Web Image Retrieval application. The user searches for documents based on previously entered index values to return the images. No PII data is used for searches, however PII data can be found on the images themselves.

Access to documents is provided through client server and intranet based applications. Electronic Customer File uses an Oracle database for the repository where access is granted only to the QFlow Administrator.

Per the PTA, BRE/FICO Blaze does not require a PIA and will not be discussed in the remainder of the document.

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: Privacy Act protected information to include (but not limited to): Social Security Number (SSN), Taxpayer Identification Number (TIN), debt payment information, addresses, employment history, date and/or place of birth, address information, miscellaneous account numbers, and image of the signature. These modules do not collect PII information. Information stays within the department and is maintained in the systems. ECF/Imaging has scanned, faxed, and imported document images from loan granting systems.

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

ECF/Imaging receives information from GLS, LoanServ and RD Apply. All of the USDA National, State and Field offices have the ability to add documents to the ECF system.

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

ECF/Imaging provides electronic processing of loan applications and other paper requests coming into the RD agency. This system provides an electronic means to access past loan documents and servicing documents to be able affectively service the current loan portfolios. This system essentially serves as an electronic file storage center.

1.4 How is the information collected?

ECF/Imaging – loan documentation is scanned into the system via Kodak scanners or imported from RD internal applications.

1.5 How will the information be checked for accuracy?

N/A

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

Paperwork Reduction Act and Section 10708 of the 2002 Farm Bill.

Consolidated Farm and Rural Development Act (7 U.S.C. 1921 et. seq.); and Title V of the Housing Act of 1949 as amended (42 U.S.C. 1471 et. seq.).

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

Risk: Minimal; information is either scanned or imported into the system.

Mitigation: EFC/Imaging is internal to the USDA RD network. Data is stored in a secure environment behind the NITC secure midrange infrastructure. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM). The application is behind eAuthentication (eAuth) with a Level 2 access authority. Users of the system are required to complete annual privacy act training to ensure the proper handling of privacy data.

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 uses scanning software and equipment providing indexing, storage and retrieval of electronic images of loan application documents and other paper requests sent to RD.

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

N/A, ECF/Imaging documents are either scanned or imported into the application.

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 National Institute of Standards and Technology (NIST) 800-53 controls for the Common Call Components are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1-8, 12, 14, 17, and 19- 22), Identification and

Authentication (IA- 1-7) 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 eAuth User Identification (User ID). Authority and Purpose (AP) compensating control gives explanation of why PII is allowed on the system. Systems and Communication Protection (SC-1-8, 10, 12, 13, 17, 18, 20-23, 28, and 39) controls are in place to prevent unauthorized access.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

ECF/Imaging documents are backed up and are archived indefinitely.

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: The risk is minimal.

Mitigation:

ECF/Imaging application is an internal application with security measures in place protecting stored data with Data Minimization and Retention (DM) and Media Protection (MP) controls. RD employees are trained and instructed on the methods to secure RD data.

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 shares information with Guaranteed Loan System (GLS), LoanServ and RD Apply (New Loan Originations).

4.2 How is the information transmitted or disclosed?

ECF/Imaging: ECF transactions travel over the USDA's internal LAN and via fax servers connected to the agency Fax Over IP (FOIP) networks Web-based ASP or .NET application is needed to access the system and by users with eAuthentication access.

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 security and control of PII is the responsibility of the System Owner and RD employees.

Mitigation:

The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality.

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, information is not shared outside USDA

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, information is not shared outside USDA.

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

N/A, information is not shared outside the department.

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

N/A, information is not shared outside USDA.

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, https://www.federalregister.gov/articles/2016/04/28/2016-09938/privacy-act-of-1974-system-of-records-usdarural-development-1-current-or-prospective-producers-or

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

N/A, notice is the responsibility of the collecting system.

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

N/A

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

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?

ECF/Imaging systems does not allow external users. If data is incorrect for a borrower, it is addressed by the SOR.

The procedures are documented.

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

ECF/Imaging system does not allow external users. If data is incorrect for a borrower, it is addressed by the SOR.

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

ECF/Imaging does not allow external users. If data is incorrect for a borrower, it is addressed by the SOR**7.4**

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

N/A

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

No additional risks are associated with the redress process.

Section 8.0 Technical Access and Security

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

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

Generally, the National Institute of Standards and Technology (NIST) 800-53 controls for Common Call Components are discussed in detail in the System Security Plan and specifically the Access Control (AC), Identification and Authentication (IA) and Systems and Communication Protection (SC) controls are in place to prevent unauthorized access. Access control is also addressed in the individual systems desk procedures.

Desk Procedures document the process for establishing, activating, and modifying IDs. This process is defined by System Owners. System Owners define Groups and account types. System Point of Contact (POC) assigns group membership and determines Need-to-know validation. The POC is responsible for verifying user identification; the User Access Management (UAM) Team relies on a POC supplying the correct UserID and password. UAM tickets are the tool used to track authorized requests by approving Point of Contact (POC).

Currently RD reviews reports from Human Resources (HR) on a Bi-weekly basis. The organization employs automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are not used or authorized. Guest and Anonymous accounts are not managed by ISSS UAM Team. POCs (empowered by RD IT managers) are responsible for notifying UAM Team if access or roles need to be modified and periodically reviewing and certifying established access.

8.2 Will Department contractors have access to the system?

Yes

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

USDA RD requires annual Information Security and 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 Office of Chief Information Officer-Cyber Security. Training must be completed with a passing score prior to access to a USDA RD system. All RD employees/contractors are required to complete Computer Security Awareness Training and USDA Privacy Basics on an annual basis.

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?

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 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 is mitigated by 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 are reviewed by NITC and Client Technology Services (CTS) for all security suspicious activity and conduct an investigation as warranted. Suspicious activity includes, but is 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 UserID, modification or attempted modification of sensitive files without authorization, and within the applications repeated attempts to access data outside a user's privilege.

Per the General Records Schedule 20, Section IC the following items will be deleted/destroyed when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes: electronic files and hard copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system usage.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

Commercial-off-the-Shelf (COTS) products\ supplemented with custom programs

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

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?

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

Responsible Officials

MICHAEL SUTTON

Digitally signed by MICHAEL SUTTON
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=MICHAEL SUTTON, 0.9.2342.19200300.100.1.1=12001000317363
Date: 2016.11.15 15:13:34 -06'00'

Michael Sutton
Chief, Enterprise Technologies Branch

Approval Signature

EUGENE TEXTER

Digitally signed by EUGENE TEXTER
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=EUGENE TEXTER, 0.9.2342.19200300.100.1.1=12001000317346
Date: 2016.11.15 15:27:45 -06'00'

Diego Maldonado
Information Systems Security Program Manager