FARM CREDIT ADMINISTRATION PRIVACY IMPACT ASSESSMENT

SYSTEM, PROGRAM, OR PROJECT NAME

FCA IT Infrastructure System

SYSTEM TYPE

Information Technology System or Capability

PURPOSE

The Farm Credit Administration (FCA) Information Technology (IT) Infrastructure System is a general support system that provides the information and technology resources that support FCA users in carrying out the agency's mission.

AUTHORITY

12 U.S.C. 2243, 2252

INFORMATION OVERVIEW

Covered Persons	Included
Employees of Farm Credit System (FCS) institutions	☒
Farm Credit institution customers	☒
FCA employees, contractors, interns	☒
Employees of other federal agencies	☒
Members of the public	☒

Personally Identifiable Information (PII)	Included
Full name	☒
Date of birth	☒
Place of birth	☒
Social Security number (SSN)	☒
Employment status, history, or information	☒
Mother's maiden name	☒
Certificates (e.g., birth, death, naturalization, marriage)	☐
Medical information (medical record numbers, medical notes, or X-rays)	☒
Home address	☒
Phone number(s) (nonwork)	☒
Email address (nonwork)	☒
Employee identification number (EIN)	☒
Financial information	☒
Driver's license/State identification number	☒
Vehicle identifiers (e.g., license plates)	☐
Legal documents, records, or notes (e.g., divorce decree, criminal records)	☐
Education records	☒
Criminal information	☒

Military status or records	☒
Investigative report or database	☐
Biometric identifiers (e.g., fingerprint, voiceprint)	☒
Photographic identifiers (e.g., image, X-ray, video)	☒
Other: System-generated administrative data (audit and use information for FCS, FCA, and Farm Credit System Insurance Corporation (FCSIC) users; personal identity verification (PIV) card numbers, certificates, and associated attributes.	☒

LIFE CYCLE NARRATIVE

The FCA IT Infrastructure System is a general support system that provides the information and technology resources that support FCA users in carrying out the agency's mission. The IT Infrastructure System includes hardware, software, information, data, applications, communications, and facilities that handle the following:

- The agency's network, including incoming and outgoing connections
- Boundary protection
- Identity and access management
- Communications management
- Data storage, processing, and management
- Software applications
- Mobile devices

The IT Infrastructure System provides an agencywide platform for hosting and supporting components used both inside the agency and by non-FCA employees, contractors, and interns. The system also serves as the platform for software applications and subsystems. The system secures the FCA network boundaries, authenticates users, provides data management services, secures internal and external data transmissions, manages mobile devices, and provides technical support for all users.

The IT Infrastructure System connects a variety of cloud environments and applications to support the data processing, computing, and networking needs of FCA for daily operations. Components include the following:

- **Laptops:** The primary computing device for FCA and Farm Credit System Insurance Corporation (FCSIC) employees, contractors, and interns. All laptops are encrypted to protect any sensitive information that is stored or processed.
- **Mobile devices:** Mobile devices issued by FCA to FCA and FCSIC employees, contractors, and interns, as well as mobile device management capabilities for securing and monitoring agency mobile devices.
- **Database systems:** Databases housed on a variety of custom and off-the-shelf applications used agencywide, which are managed by FCA.
- **External data portal:** The system external stakeholders use to submit data to FCA. This portal is supported by SharePoint, the SQL server, and other related services.
- **Secure FTP portal:** The site external stakeholders use to submit a variety of data, from Farm Credit System (FCS or System) institutions, Consolidated Reporting System (CRS) data, including call reports and examination-related data and documentation.
- **Storage and backup systems:** Platforms used to ensure continuity for the agency's mission systems and data.
- **Internal and external custom and commercial applications:** A variety of FCA applications that support the agency's mission and used either solely by FCA employees, contractors, and interns (internal-facing applications) and by external stakeholders and the public (external-facing applications).
- **Networks:** A set of networking components supporting connectivity, including wide area networks, local area networks, virtual networks, and network perimeter and boundary protection devices.

FCA offices use these services to collaborate across the agency. Only FCA and FCSIC employees, contractors, and interns may access these systems, except where noted Access and privileges for specific functions are granted on an as-needed

basis by applying the principle of least privilege (i.e., users have access to and permissions for only the information required to do their jobs).

Information contained on or transported over the IT Infrastructure System includes every type of information FCA employees use in support of the agency's mission, including the following:

- Supervisory, enforcement, and criminal referral data for safety and soundness purposes
- Borrower complaint data
- Human resources data for personnel purposes
- Other administrative data required for meeting operational and mission objectives

These data include personally identifiable information (PII) of the following people: FCA and FCSIC employees, contractors, and interns; FCS institution employees and customers; staff of other federal agencies; and members of the public. PII can be low sensitivity, such as basic business contact information, or high sensitivity, such as Social Security numbers or financial information about customers of FCS institutions. The IT Infrastructure System uses PII for various reasons related to carrying out the agency's mission, including to oversee and regulate FCS institutions and to carry out internal administrative functions (e.g., payroll, benefits, system administration, and other similar functions).

In addition to PII contained in or transported over the IT Infrastructure System, a variety of custom and commercial off-the-shelf applications and other software collect, maintain, and process PII about FCS institution customers and employees and members of the public. Use of some of these applications, such as the Criminal Referral System, presents unique privacy risks. In those instances, the applications have been covered in separate PIAs. The FCA applications and capabilities included in the IT Infrastructure System that process the PII of people who are not FCA and FCSIC employees, contractors, or interns are described in the following sections.

Borrower complaints

The FCA website, www.fca.gov, hosts an electronic form that allows the public to submit complaints about FCS institutions and the System in accordance with the Farm Credit Act and implementing regulations. Once submitted, the information is automatically transferred to a secure, internal repository for tracking and resolution. PII collected and processed by the electronic form varies by complaint type but generally includes the following:

- Name (first and last) of the complainant and the borrower (if different)
- Email address
- Phone number
- Loan number associated with the complaint
- Nature of the complaint, including the name of the institution associated with the complaint and any additional details

Criminal Referral System

The FCA Criminal Referral System allows authorized users at all System institutions to submit reports of known or suspected criminal activity at System institutions in accordance with the agency's published regulations on criminal referrals. See FCA's Privacy Impact Assessment for the Criminal Referral System (PDF).

Correspondence Tracking System (CTS)

The CTS is an application used by FCA's Office of Congressional and Public Affairs and other FCA staff to manage and track communications to and from members of the public, FCS institutions, state and federal agencies, congressional contacts, and others. In general, the system contains the following:

- Name (first and last)
- Title
- Contact information, including home or business mailing address

- General information about the nature of the communication, including the date it was received, the method of communication used (i.e., paper mail, email, fax, telephone), the date FCA responded and the method of communication used, and other pertinent details

EDGe

EDGe is the system FCA uses to manage activities related to the examination of FCS institutions. PII includes the following:

- Names and titles of FCA Office of Examination employees associated with the examination of an FCS institution
- Names, titles, and contact information of FCS institution employees

Web-based collaboration tools

FCA uses commercial off-the-shelf tools that provide for communication and collaboration . FCA uses tools for document sharing and management, collaborative editing, and other functions related to documents, such as document libraries. The agency also uses collaborative workflow systems for a variety of internal, administrative, process-related workflows, such as document routing and approval; functions related to human resources, such as work scheduling and telework approval; requests and approvals for student loan repayments; and processing financial disclosure forms. PII about non-FCA or FCSIC persons that is processed in these tools generally includes the following:

- Name
- Date of birth
- Contact information, including home address, phone number, and personal email address
- Photographic identifiers (i.e., photographs or video)

External data portal and SFTP

FCA uses the external data portal and SFTP to receive data from outside sources, such as CRS data, including call reports, and examination-related data and documentation from staff at System institutions. Information processed includes the following:

- Names, titles, and contact information of users, including FCS institution officials, and other external stakeholders
- Usernames, email addresses, and passwords associated with FCS institution user accounts
- Documents and similar materials related to the agency's mission, which may include PII

In addition to the custom and commercial off-the-shelf tools outlined above, the IT Infrastructure System uses other tools that only process PII about FCA and FCSIC operations and employees, contractors, and interns. This internal, operational PII is unstructured or semistructured content (e.g., documents, list data, and workflows supporting business processes). Supported business processes include administrative functions related to human resources, such as approvals for telework and alternative work schedules, onboarding new employees, and processing student loan repayments, as well as other administrative functions, such as processing financial disclosure forms, routing and approving policies and procedures, management of information technology, and management and formulation of budgets. PII includes the following:

- Names (first, middle, last)
- Information about work schedule, leave requests, and leave balances
- Names (first, middle, last)
- Title, position, grade, salary, and similar employment information, including employment history
- Social Security number
- Date and place of birth
- Age, race, sex
- Contact information, including email address and phone numbers (business and personal)
- Information about property assigned to or returned from employees

- Credit card number(s) and other financial information
- Medical information
- Education information
- Audio and video recordings and photographs

Some information in the IT Infrastructure System is collected directly from individuals (e.g., borrower complaints, requests to be contacted, media inquiries, information requests and similar correspondence, comments on public notices, employment applications, and emergency contact information). Other information is collected indirectly (e.g., data from FCS institutions, data from other agencies).

Where feasible and appropriate, the agency notifies individuals from whom it collects information that the information was collected and how it will be used. In these situations, the person whose information is being collected typically has opportunities to change or update information that is wrong in accordance with the Privacy Act and FCA's Privacy Act regulations, as outlined in 12 CFR Part 603. The agency provides notice through a Privacy Act Statement, a web privacy policy, or some similar means, depending on the nature of the collection and intended use of the information. In addition, FCA has published this PIA to provide notice to individuals whose PII has been collected.

The IT Infrastructure System itself is not a Privacy Act system of records although applications housed on it may be. Information may be retrieved in a variety of ways depending upon the application being used and the user's permissions. Much of the information in the IT Infrastructure System does not constitute a Privacy Act system of records because it is not retrieved by personal identifier, nor does its use require alteration of any existing system of records notices (SORNs). Such information is addressed in one or more of FCA's SORNs. For a complete list of applicable SORNs, go to https://www.fca.gov/required-notices/privacy-program.

Finally, information in the system may be shared with a variety of partners — other federal agencies, external stakeholders, and the public — for a variety of reasons related to ensuring the safety and soundness of the Farm Credit System. Any sharing of information with partners outside the agency must be within the scope of the agency's authorities and regulations and must facilitate a specific FCA business function. Any sharing of Privacy Act data must be in accordance with the routine uses for the specific system from which the data are derived.

COMPLIANCE WITH APPLICABLE STATUTES, REGULATIONS, AND REQUIREMENTS

For each statute or regulatory requirement, indicate applicable sections of statutes, regulations, or requirements and provide links to them, or provide a brief description of compliance. If a requirement is not applicable to the IT Infrastructure System, indicate with N/A.

The Privacy Act of 1974 (As Amended)	
System of records notices	FCA's IT Infrastructure System does not constitute a Privacy Act system of records; however, it does process and store records subject to the Privacy Act from existing Privacy Act systems of records.
Computer Matching and Privacy Protection Act of 1980	
Notice of computer matching agreements	N/A — FCA does not have any computer matching agreements that pertain to this system.
The Paperwork Reduction Act of 1995	
Office of Management and Budget (OMB) control numbers and related forms	Various government standard and optional forms capture information that may be stored in documents and files within the IT Infrastructure System. No FCA-specific forms that require an OMB control number are used to capture information from the public for the IT Infrastructure System.
The Federal Records Act of 1950 (As Amended)	
Records control schedule names and numbers	In general, data maintained in applications housed on the IT Infrastructure System are subject to various records retention policies and schedules in accordance with guidelines outlined by the National Archives and Records Administration.
Other	
N/A	N/A

ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS

☒	All applicable controls for protecting PII as defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Appendix J, and NIST SP 800-122 have been implemented and are functioning as intended, have compensating controls in place to mitigate residual risk, or have an approved plan of action and milestones.
☒	The system has been reviewed for compliance with, and assigned a categorization level in accordance with, NIST Federal Information Processing Standards (FIPS) Publication 199 and NIST SP 800-60, and the senior agency official for privacy has approved the categorization. FIPS 199 Security Impact Category: Moderate
☒	A security assessment has been conducted for the system, and it has been determined that there are no additional privacy risks.
☒	The information system has been secured in accordance with Federal Information Security Modernization Act requirements. Most recent assessment and authorization type: Authorization to Operate (ATO) and date: 8/27/2020 ☐ This is a new system, and the assessment and authorization date is pending.
☒	A comprehensive listing of data elements included in the system has been provided to the privacy officer, reviewed and approved, and included in the agencywide PII inventory.
☒	System users are subject to or have signed confidentiality or nondisclosure agreements, as applicable.
☒	System users are subject to background checks or investigations. FCA employees, contractors, and interns with network access are subject to background checks and investigations before being granted user accounts.
☒	System access is limited to authorized personnel with a bona fide need to know in support of their duties.
☒	Notice is provided in the form of a Privacy Act statement, privacy notice, privacy policy, or similar, as applicable.
☒	Contracts or agreements (e.g., memorandums of understanding, memorandums of agreement, and information security agreements) establish ownership rights over data, including PII.
☐	Acceptance of liability and responsibilities for exposure of PII are clearly defined in agreements or contracts.
☒	Access to and use of PII are monitored, tracked, and recorded.
☒	Training on PII, confidentiality, and information security policies and practices is provided to system users or those with access to information.

ADMINISTRATIVE AND TECHNOLOGICAL CONTROLS NARRATIVE

FCA's IT Infrastructure System is authorized for use at the moderate level, and FCA's chief information officer (CIO) has granted the system an Authorization to Operate.

The agency secures information in the system using a variety of means:

- Physical security controls of FCA facilities and data centers that house the IT Infrastructure System components
- Firewalls, intrusion detection and prevention systems, and antivirus and other software and capabilities for detection of malware and other malicious threats
- Transport layer security connections and multifactor authentication
- Total disk encryption and other encryption methods for securing sensitive data, including PII
- Access controls and the principle of least privilege (i.e., users have access to and permissions for only the information they need to do their jobs)
- Application, network, server, and database activity logs, which are reviewed when abnormalities arise or when requested by the CIO or chief information security officer (CISO)

System owners, in conjunction with information owners and the Office of Information Technology, conduct annual access and permission reviews for specific applications and databases housed on the IT Infrastructure System.

Employees, contractors, and interns are responsible for using the system in accordance with applicable FCA policies and procedures. FCA users must read, sign and acknowledge their understanding of FCA information security and privacy policies, and acceptable use of FCA IT assets and information in the agency's rules of behavior. Additionally, FCA

employees receive annual security and privacy awareness training, as well as training when they join the agency. System administrators use user identification, passwords, and audit logs to ensure that only users with appropriate permissions and access levels are accessing systems.

PRIVACY RISK ANALYSIS

What follows is an overview of the primary risks associated with FCA's use of the IT Infrastructure System and a description of corresponding mitigations the agency has put in place for each.

Use limitation: The FCA IT Infrastructure System processes nearly all the information that is collected and used by the agency in support of its operational and mission objectives. However, there is a risk that information processed by the system could be used for a reason other than the reason provided to the individual from whom the information was collected. The agency mitigates this risk by instituting role-based access controls for applications and capabilities within the IT Infrastructure System that process PII and other sensitive information. The agency also institutes controls to audit access to and use of data processed within the system and requires users to take annual information security and privacy awareness training, which, among other things, focuses on appropriate data handling and use.

Data minimization: FCA reviews data collections to limit the collection and maintenance of PII to the minimum amount necessary to complete the agency's mission. That said, FCA collects and retains significant amounts of PII to fulfill a wide range of mission-related objectives, from supervisory activities to internal, administrative functions (such as personnel management). The agency employs appropriate technical, physical, and administrative controls to ensure that the PII it collects and maintains is appropriately secured relative to the risk presented. These controls include policies and procedures that outline reviews for new collections or uses of PII within the agency.

Data confidentiality, including access or use by unauthorized users: As noted above, the IT Infrastructure System processes a variety of mission and operational data, including PII and other sensitive information. There is a risk that unauthorized users, either within the agency or outside of the agency, could access this information, leak, or lose it either within the agency or outside of the agency.

To reduce the risks of data loss, leaks, and unauthorized access and use, FCA uses a variety of technical and administrative controls to limit access to data it stores and processes in the IT Infrastructure System, including those outlined in the Administrative and Technological Controls Narrative section of this PIA. Through the concept of least privilege, FCA users are granted access to only the information and applications for which they have a valid need to know. Unique usernames, passwords, and two-factor authentication are used to control access to systems and data. FCA users are required to complete annual security and privacy training and must sign and abide by FCA's security policies and rules of behavior.

Overall risk: FCA has implemented and maintains strong administrative, technical, and physical controls to protect the IT Infrastructure System and sensitive information processed on it, including PII. As outlined above, the primary risks to PII include confidentiality, use limitation, and data minimization. The agency has processes in place to evaluate any new intake of PII or new uses of existing PII collections and regularly reviews PII processed by the system. Access to the IT Infrastructure System, applications, and PII is limited to FCA and FCSIC employees, contractors, and interns with a need to know, as well as external parties as outlined in this PIA.

DOCUMENT CONTROL

Approval

/s/ Wesley Fravel, FCA privacy officer	/s/ Jeannie Shaffer, CISO
/s/ Ruth Surface, associate director, infrastructure division	/s/ Jerry Golley, CIO and senior agency official for privacy

Change Control and Approval History

Version	Date	Change Summary
V 1.0	2/24/2021	Initial Version