FARM CREDIT ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

SYSTEM, PROGRAM, OR PROJECT NAME

Microsoft Cloud

SYSTEM TYPE

Information Technology System or Capability

PURPOSE

FCA uses cloud offerings from Microsoft 365 and Microsoft Azure that are authorized by the Federal Risk and Authorization Management Program (FedRAMP). Microsoft 365 provides a collection of software-as-a-service capabilities. Microsoft Azure provides a collection of infrastructure-as-a-service, platform-as-a-service, and other as-a-service capabilities. While each service has separate FedRAMP authorizations, FCA uses these services as a single suite of functions. Therefore, in this PIA we refer to these services collectively as "Microsoft Cloud." FCA has chosen to conduct a single PIA for the combined use of these services to further public understanding of how the services interact in processing personally identifiable information (PII).

Microsoft 365 is rated as a moderate system and Microsoft Azure is rated as a high system under the Federal Information Security Modernization Act of 2014 (FISMA). FCA's authorized use for both services is rated at a FISMA moderate level.

AUTHORITY

12 U.S.C. 2243, 2252

INFORMATION OVERVIEW

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

Personally Identifiable Information (PII) Element(s)	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 and/or records	☒
Investigative report or database	☒
Biometric identifiers (e.g., fingerprint, voiceprint)	☐
Photographic identifiers (e.g., image, X-ray, video)	☒
Other: Information on salary and benefits, performance, clearance and personnel security, and home and emergency contacts	☒

LIFE CYCLE NARRATIVE

Microsoft Cloud provides the FCA IT Infrastructure System[1] — the agency's general support system — with the following services that enable communication; collaboration; administrative work; identity and access management; data storage, processing, and management; mobile device management; and other application support:[2]

- Office applications
- Exchange Online
- Skype for Business Online
- Microsoft Teams
- Microsoft Stream
- OneDrive for Business
- Intune
- Azure Active Directory
- Microsoft 365 and Azure services for security, identity, and information protection
- Microsoft 365 and Azure services for administration

FCA uses these services for agencywide collaboration. Access is limited to FCA and FCSIC[3] employees, contractors, and interns ("FCA users"), with access to and privileges for specific functions granted on an as-needed basis by applying the principle of least privilege (i.e., users have access only to the information required to do their jobs).

Because Microsoft Cloud provides communication and collaboration capabilities, a wide range of data is processed, including sensitive information (necessary for conducting business agencywide) and personally identifiable information (PII). A general discussion of the types of PII follows.

Within Microsoft Cloud, in general, there are two types of information:

- FCA user information, including the user's full name, work email address, and other official contact and profile information (such as photos) as well as use and authentication information

[1] See the FCA IT Infrastructure System Privacy Impact Assessment for more information.
[2] This list includes only the Microsoft services that FCA uses. If Microsoft adds services that involve personally identifiable information, or the agency uses these services or new services in a way which implicates PII, we will update this PIA to reflect those changes.
[3] The Farm Credit System Insurance Corporation or FCSIC leverages information technology resources and services from the FCA including Microsoft Cloud. For the purposes of this PIA, FCA users includes FCSIC employees, contractors, and other authorized FCSIC users of FCA IT resources and services.

- Microsoft Cloud collaboration information (data and documents that users upload, generate, use, or store in the agency's Microsoft Cloud)

PII arising from collaboration

Microsoft Cloud collaboration information may contain PII. Examples of the types of collaboration sites and information maintained in Microsoft Cloud include the following:

- Email, calendar, contacts, and tasks in user mailboxes
- FCA user profiles, including photographs and interests
- Shared calendars and email in shared mailboxes
- Documents and other data in user file storage, including confidential data derived from examinations of institutions
- Chat logs, transcripts of video and audio conferences, and shared documents
- Video images, photographs, transcripts, and similar in internal and publicly available videos

PII in user files concerning non-FCA users

Documents and other data in user files are the source of most of the potentially sensitive PII in the agency. These documents may contain the following PII related to FCS institution employees and customers as well as members of the public:

- Full name (first, last, middle)
- Date and place of birth
- Social Security number
- Employment status or history
- Home address and similar contact information
- Financial information related to borrower complaints or criminal referrals

Types of PII in user files concerning FCA users

The following PII about FCA employees may be included in documents and other data related to human resources and administrative matters:

- Full name (first, last, middle)
- Date and place of birth
- Social Security number[4]
- Employment status or history
- Salary and benefits information
- Performance-related information
- Information related to clearance and personnel security
- Information related to home and emergency contacts

PII contained in FCA's Microsoft Cloud supports the agency in carrying out its mission and includes the following:

- Supervision data used for supervision, regulatory, enforcement, and oversight
- Borrower complaint data used in responding to complainants
- Human resources data used for personnel purposes
- Information used for congressional and public affairs and legal and litigation purposes

Some information in FCA's Microsoft Cloud is collected directly from people (requests to be contacted, media inquiries, comments on public notices, employment applications, Freedom of Information Act requests, emergency contact information, etc.). Some information is not collected directly from people but comes to FCA from other sources, for example, FCS institutions and other agencies.

When information is collected directly from someone, as feasible and appropriate, FCA informs the person what information has been collected and how it will be used. Persons who have their information collected for inclusion in a System of Records are also informed of any available opportunities to change or update any information that is incorrect

[4] Microsoft Cloud does not collect Social Security numbers (SSNs); however, users may store SSNs as part of documents or email in the system. 12 U.S.C. 2243, 2252 provides general authority for the collection of SSNs by FCA.

or no longer relevant (in accordance with the Privacy Act and FCA's Privacy Act regulations, as outlined in 12 CFR Part 603 and the procedures outlined in the applicable SORN). FCA provides notice by a Privacy Act Statement, a web privacy policy, or similar means as appropriate. In addition, FCA has published this PIA to provide notice to anyone whose information has been collected or is processed in FCA's Microsoft Cloud.

FCA users may retrieve information from FCA's Microsoft Cloud either on their own or by asking an administrator to do so, depending on the application and user permissions. Additionally, authorized FCA administrators can search Microsoft Cloud to help users recover lost messages, documents, or files to find messages, documents, or files, for a legal or similar administrative request, or to identify and remediate security threats, such as viruses or malware associated with an infected message or file.

Finally, FCA users can use Microsoft Cloud services search functions to find specific documents or files. FCA's Microsoft Cloud does not constitute a Privacy Act system of records, and its use has not required changes to any existing systems of records notice (SORNs). The system does process and store records, subject to the Privacy Act, from existing Privacy Act systems of records, and is addressed in one or more of FCA's SORNs. A complete list of applicable agency SORNs can be found at https://www.fca.gov/required-notices/privacy-program.

Finally, information in FCA's system may be shared with a variety of partners — other federal agencies, external stakeholders, the public, and others — as part of ensuring the safety and soundness of the Farm Credit System. Any information shared with people outside of the agency must be within the scope of FCA's authorities, regulations, and policies and facilitate a specific FCA business function — for example, sharing employee information with other federal agencies and companies for payroll and benefits purposes or sharing information with the public as required by statute or regulation. Any sharing of Privacy Act data that occurs is in accordance with the routine uses for that particular system of records.

COMPLIANCE WITH APPLICABLE STATUTES, REGULATIONS, AND REQUIREMENTS

For each, indicate as applicable and provide a link, or a brief description of compliance. If not applicable, indicate with N/A.

The Privacy Act of 1974 (As Amended)	
System of records notice(s)	FCA's Microsoft Cloud 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 agreement(s)	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 control number(s) or related form(s)	Government standard forms capture information that may be stored in documents and files within FCA's Microsoft Cloud. However, there are no forms or information collection control numbers specific to FCA's use of Microsoft Cloud.
The Federal Records Act of 1950 (As Amended)	
Record(s) control schedule name(s) and number(s)	Microsoft has a standard policy for data handling for Microsoft Cloud that specifies how long customer data will be retained after deletion. There are generally two scenarios in which customer data are deleted: • Active deletion — FCA has an active subscription to Microsoft Cloud, and a user or administrator deletes data. • Passive deletion — FCA's subscription to Microsoft Cloud ends. In general, information maintained in Microsoft Cloud is subject to various records retention policies and schedules in accordance with guidelines outlined by the National Archives and Records Administration and is retained in accordance with the active deletion scenario.
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 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 Use (ATU) and date: 8/5/2019 and 12/4/2019 ☐ 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.
☒	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.
☒	Contract(s) or agreement(s) (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 agreement(s) or contract(s).
☒	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

Microsoft 365 and Microsoft Azure are both FedRAMP-approved cloud service providers and are regularly reviewed by the sponsoring agency to ensure that all applicable security controls are in place and that all services are operating correctly. In addition, FCA has conducted a security and privacy review of both providers to determine if controls for which the agency is responsible are implemented and functioning as intended or if compensating controls or mitigations are in place or planned. FCA's authorizing official, who also serves as the agency's chief information officer and senior agency official for privacy, has authorized use of both sets of services.

The associate director of the Office of Information Technology's Infrastructure Division is the system owner, responsible for management and oversight of FCA's Microsoft Cloud, including system administration, security enforcement of privileged users, authentication processes, and monitoring the system.

Employees are responsible for using the system in accordance with applicable FCA policies and procedures. Before being granted access to any FCA system or network, FCA users must read FCA Policy and Procedure Manual 902 and 906 and sign an attestation indicating they understand what acceptable use of FCA IT assets and information is. In addition, FCA employees receive annual security and privacy awareness training. New staff receive security and privacy awareness training during onboarding activities.

Users are granted access to FCA systems and information on a need-to-know basis, by using the concept of least privilege. Administrators ensure appropriate permissions and access levels by checking user identities, passwords, and audit logs.

Microsoft policy prohibits it from reviewing, auditing, or transmitting FCA data maintained in Microsoft Cloud. PII stored on Microsoft servers is encrypted in accordance with Federal Information Processing Standard (FIPS) 140-2 standards both when in transit and when at rest.

FCA uses technical and operational controls, such as firewalls, encryption, audit logs, the concept of least privilege, and malware identification, to reduce risk in Microsoft Cloud. All users must have an FCA network account and a government-issued personal identity verification card, or acceptable alternative, to access FCA's Microsoft Cloud.

PRIVACY RISK ANALYSIS

FCA recognizes the risks of using cloud-based solutions for storing and processing PII and other sensitive data. The risks — data confidentiality, data minimization (limiting data collected to the least amount necessary to fulfill a specific purpose), and transparency (providing impacted persons with notice of the agency's collection and use of their PII)— among others, are not unique to cloud-based technologies; they result from inadequate application of the security and data protections that are necessary when such data are processed. To this end, the agency has (1) designed its use of Microsoft Cloud to account for the processing of sensitive information, including PII, and (2) implemented administrative controls to reduce overall risk, including policies and procedures for appropriate access to and collection and use of sensitive information; training and awareness efforts; and other physical and administrative controls to ensure PII is appropriately secured.

DOCUMENT CONTROL

Approval

/s/_____ Wesley Fravel, FCA privacy officer	/s/_____ Jeannie Shaffer, chief information security officer
/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	3/29/2021	Initial Version