FARM CREDIT ADMINISTRATION PRIVACY IMPACT ASSESSMENT

SYSTEM, PROGRAM, OR PROJECT NAME

Microsoft 365 (M365) Copilot

SYSTEM TYPE

Information Technology System or Capability

PURPOSE

The Farm Credit Administration ("FCA" or "Agency") has enabled Microsoft 365 (M365) Copilot as an AI tool to enhance productivity and efficiency for the agency.

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

Copilot is generative AI chatbot that is based on GPT. M365 Copilot consists of both M365 Copilot Chat and M365 Copilot (collectively, Copilot), which are chat-based generative AI tools from Microsoft.

- M365 Copilot Chat: Chatbot that responds to prompts based on user-uploaded content, and/or, optionally, web grounded prompts.
- M365 Copilot: Integrates with existing Microsoft services in use including Exchange (email), Teams, and office productivity apps (e.g., Word, Excel, PowerPoint). Provides features for writing, editing, data analysis, creating presentations, summarizing meetings, etc.

FCA's implementation of Copilot is the service available within FCA's existing Microsoft GCC tenant and leverages existing accesses to data across the Agency's General Support System (GSS or FCA IT Infrastructure System), or within the agency's Microsoft tenant (Microsoft Cloud). Copilot itself does not collect data, including PII, although it processes prompts and generates responses which include agency data. Agency data is not used to train the underlying foundational model.

Only FCA and FCSIC employees, contractors, and interns may access these systems. In the context of the user, Copilot only accesses the internal data sources which the user can otherwise access. Access and privileges for specific data sources 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 available includes every type of information FCA employees use in support of the agency's mission, including, but not limited to, the following:

- Supervisory, enforcement, borrower complaint, 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. PII is used to generate responses or suggestions which enhance productivity or support tasks related to carrying out the agency's mission, including to overseeing and regulating FCS institutions and carrying out internal administrative functions (e.g., payroll, benefits, system administration, and other similar functions).

Information which may be accessed in using Copilot includes that which 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), and when web content is enabled, information which is publicly available and searchable on the internet. Other information is collected indirectly (e.g., data from FCS institutions, data from other agencies). See the FCA IT Infrastructure System and Microsoft Cloud PIAs for additional details on the types of PII FCA maintains which may be accessed by Copilot, as well as information on sources of information. As noted above, Copilot does not directly collect data, it only accesses existing data.

Copilot is not a Privacy Act system of records although information accessed by it may include information which is part of a system of records or otherwise subject to the Privacy Act.

Data remains within FCA's Microsoft 365 Government Community Cloud (GCC) environment tenant and is not externally shared. Likewise, FCA's deployment of Copilot does not leverage data used in inputs to train Copilot or its underlying models.

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	N/A – Copilot does not constitute a System of Records
Computer Matching and Privacy Protection Act of 1980	
Notice of computer matching agreements	N/A — Copilot is not part of and does not implicate any computer matching agreements
The Paperwork Reduction Act of 1995	
Office of Management and Budget (OMB) control numbers and related forms	N/A – Copilot does not directly collect information or leverage forms to collect information.
The Federal Records Act of 1950 (As Amended)	
Records control schedule names and numbers	In general, data maintained in applications which Copilot may access 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 5 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: N/A. The underlying system(s) which Copilot have been stood up in have received an Authorization to Operate or Authorization to Use. ☐ 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

Microsoft Copilot is deployed within the Microsoft 365 GCC High environment, which meets FedRAMP High standards. FCA's use of Microsoft 365 is at the Moderate level.

Access is restricted to FCA personnel with role-based permissions. Further, as outlined above, Copilot only has access to that internal, Agency data for which the user otherwise has been granted access.

User activity is logged and monitored, including monitoring of prompts to ensure alignment with FCA appropriate use standards and policy. Additionally, FCA has implemented data loss prevention (DLP), encryption, and multifactor authentication (MFA) on its network to reduce risks posed to PII and other sensitive information.

Finally, annual privacy and IT security awareness training is mandatory for all users, and all users must sign and abide by the Agency's General User Rules of Behavior. Additionally, certain users with elevated privileges or responsibilities for PII must also sign the Agency's Privileged Rules of Behavior and complete role-based IT security training. All users also have access to a variety of guidance and training materials produced by the Agency's Office of Information Technology on the use of Copilot, including appropriate use and prohibitions.

PRIVACY RISK ANALYSIS

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

Use limitation: Microsoft Copilot will access 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 technical and administrative 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 and the specific risks posed by use of AI technologies.

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 and Microsoft Cloud 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.

Negative impact(s) due to overreliance on results, inaccurate, or biased results: As a generative AI-based service, Copilot may produce inaccurate or false responses (also called hallucinations). Further, responses may demonstrate bias due to flaws in underlying training data, insufficient data collection, or poor model design. It is important to note that FCA's primary mission does not revolve around the administration of rights, benefits, or privileges of individual members of the public. As a Federal regulator, the Agency's primary focus is on Farm Credit System institutions and not individual borrowers. That said, the Agency does handle a variety of business processes, including internal administrative processes for its employees and contractors, which directly impact individuals, including the processing of criminal referrals and borrower complaints. FCA has reduced the overall risk presented by including in its AI usage policy and in training and guidance provided to employees, requirements for human review in the use of AI outputs, as well as restrictions on specific high-risk use cases which may directly impact administration of an individual's rights, benefits, or privileges.

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, privacy officer	__/s/_____ Wesley Fravel, CISO
__/s/_____ Janice Shelsta, associate director, computing platforms division	__/s/_____ Jerry Versace, CIO and senior agency official for privacy

Change Control and Approval History

Version	Date	Change Summary
V 1.0	3/27/2026	Initial Version