Date of Approval: 10/28/2025
Questionnaire Number: 2487

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Microsoft 365 (M365)

Acronym:

M365

Business Unit

Information Technology

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

The Chief Technical Officer (CTO) is piloting Microsoft 365 (M365) Copilot to assess feasibility, functionality, and productivity gains through AI Integration.
Microsoft 365 (M365) is a Software-as-a-Service (SaaS) platform designed to enhance the Internal Revenue Service's (IRS) digital productivity and collaboration capabilities. It integrates Microsoft's Office Productivity Suite with advanced cloud-based communication, collaboration, and data management tools.
The IRS utilizes the M365 GCC G5 subscription tier-the most comprehensive government-level service-enabling centralized management, enhanced functionality, and strict compliance with federal security and privacy requirements.
The M365 GCC G5 suite includes, but is not limited to, Exchange Online, OneDrive for Business, SharePoint Online, Teams/Teams Premium, Project

Online, Microsoft Intune, Power Platform, Microsoft Purview, Defender for Office 365, Microsoft Audit, Unified Audit Stream, and Copilot. IRS access includes all IRS, IRS-CI, and TIGTA users through B2B connections managed via Microsoft Entra ID (formerly Azure AD) with MFA and zero trust. Access to Microsoft 365 Copilot and Teams Premium remains limited to pilot participants with BEARS entitlements.

For government customers, M365 offers multiple subscription levels (e.g., G1, G3, G5). The IRS employs the fully featured M365 GCC G5 subscription, which simplifies administration, provides improved functionality, and enforces required security and compliance controls within the M365 environment.

Components of M365 GCC G5

Exchange Online (EXO): Messaging service delivering email, calendar, and contacts with 100GB mailboxes.

OneDrive for Business (ODB): Secure 1TB cloud storage for personal work files, replacing local drives and network shares.

SharePoint Online (SPO): Shared document storage, collaboration, and intranet website hosting.

Teams: Centralized hub for chat, voice, video, and file-sharing collaboration.

Project Online (PIO): Cloud-hosted version of Microsoft Project Server used for portfolio and project management.

Intune Logging Solutions: Supports IRS mobile device and application management (MDAM).

Microsoft Power Platform (MPP): Data visualization and automation tools (Power BI, Power Automate, Power Apps).

Microsoft Purview: Unified solutions for data governance, security, and compliance.

Microsoft Audit: Centralized collection of user and administrative audit records.

Microsoft Defender for Office 365: Cloud-based threat protection against phishing, malware, and other advanced threats.

Calendar: Enterprise scheduling and time management.

Copilot: Embedded AI assistant that enhances productivity and creativity by summarizing information, automating tasks, and generating content.

Delve: Provides personal insights based on work activity and collaboration.

Excel: Tool for creating and managing worksheets for budgeting, planning, and calculations.

Forms: Used for surveys and quizzes.

Lists: Enables creation and tracking of structured data sets.

OneNote: Digital notebook for organized notetaking.

Outlook: Unified interface for email, calendar, and task management.

People: Directory for managing and sharing contact information.

Planner: Organizes, assigns, and tracks tasks and project progress.

PowerPoint: Creates visual slide presentations.

Shifts: Teams feature for managing frontline worker schedules and time tracking.

Stream: Platform for sharing training videos, meetings, and presentations.

Teams Premium: Enhances Teams with advanced features for webinars, virtual appointments, and secure meetings.

To Do: Task management and prioritization tool.
Visio: Enables creation of visual diagrams and process charts.
Whiteboard: Facilitates interactive collaboration through a shared digital canvas.
Word: Supports collaborative document creation and real-time editing.
Platform Overview
Microsoft 365 Government G5 serves as the IRS's foundational platform for secure communication, collaboration, and productivity. It integrates essential tools such as email, instant messaging, file sharing, and team sites to support structured management and efficient information exchange aligned with the IRS's operational and strategic goals.
Permission to use M365 is granted to all IRS users, including IRS Criminal Investigation (IRS-CI) and Treasury Inspector General for Tax Administration (TIGTA) personnel, as well as authorized external government partners via Microsoft Business-to-Business (B2B) access. Access to Microsoft 365 Copilot and Teams Premium is currently limited to pilot participants with BEARS entitlements.
Microsoft Intune, a cloud-based endpoint management solution, complements these services by enabling centralized device administration, configuration, and security enforcement across the enterprise. Intune supports mobile device management (MDM) and mobile application management (MAM), ensuring secure access to IRS resources while maintaining compliance with IT governance standards.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

Microsoft 365 (M365) processes personally identifiable information (PII) such as names, email addresses, IP addresses, and SEIDs, collected via user input or system-generated metadata. Data classification and protection are enforced through Microsoft Purview features including Sensitivity Labels, Data Loss Prevention (DLP), and Information Barriers. Data is stored in the Government Community Cloud (GCC) and GCC High environments, encrypted in transit and at rest. Access is controlled through Conditional Access policies, multi-factor authentication (MFA), and zero trust principles via Microsoft Entra ID. All access attempts are logged and ingested into Splunk for monitoring, with Microsoft Defender XDR used to detect anomalous activity. Retention policies define how long data is preserved, ensuring recoverability and compliance, while secure deletion methods enforce federal privacy requirements. Data collection includes

PII processed through user input or system-generated metadata, with classification and protection achieved using Microsoft Purview tools like Sensitivity Labels, DLP, and Information Barriers. Data is stored within tenant boundaries like GCC and GCC High, encrypted in transit and at rest.
Access control and usage involve Conditional Access policies, MFA, and zero trust principles via Microsoft Entra ID, with all access attempts logged and monitored through Splunk. Retention and archiving policies ensure data is kept for the necessary period, with backup and archive solutions guaranteeing recoverability and compliance. Destruction and deletion are automatic upon the expiration of IRS information retention policies, with secure deletion mechanisms in place to ensure compliance with privacy regulations.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address
Email Address
Employer Identification Number
Employment Information
Federal Tax Information (FTI)
Internet Protocol Address (IP Address)
Name
Photograph
Protected Information
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Telephone Numbers

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
PII for personnel administration - 5 USC
SSN for personnel administration IRS employees - 5 USC and Executive Order 9397
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

Yes

1.1 What is the name of the Business Unit (BU) or Agency initiative?

Intune Logging Solutions (ILS)

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

Project

3 What Tier designation has been applied to your system? (Number)

2

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

2358

4.12 What is the previous PCLIA title (system name)?

Microsoft 365 Government 5, M365 G5

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

Alteration in Character of Data -New information in identifiable form added to a collection raises the risks to personal privacy

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

Yes

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Steering committees and governance boards have been placed on indefinite hold by the Chief Information Officer (CIO).

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

ABA ID: 211877, 211196

10 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?

No

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

Yes

11.1 Describe the business process and purpose of your Artificial Intelligence (AI) and identify what system(s) or business process(es) this AI supports.

AI acts as a personal assistant, helping IRS users find information, create content, and streamline workflows across various Microsoft 365 apps. AI's footprint will increase over time.

11.2 What is the algorithm or learning method used and what database is training your AI?

Microsoft 365 Copilot is powered by advanced large language models (LLMs) and Natural Language Processing (NLP) techniques. Specifically: The core model is GPT-4o, optimized for chat-based interactions. It also utilizes OpenAI's GPT-4, GPT-4 Turbo, and DALLÂ·E 3 for various functionalities like summarization, content generation, and image creation12. These models are accessed through the Azure OpenAI Service, not OpenAI's public APIs, ensuring enterprise-grade security and compliance1. The AI system uses machine learning algorithms to deliver personalized, context-aware responses, adapting to user behavior and task patterns within Microsoft 365 apps. Copilot is not trained on IRS data or any user-specific content. Instead, it uses pre-trained models hosted in Azure's secure environment12. The models are not fine-tuned on tenant-specific data. Instead, they process prompts in real time using the context available from the user's Microsoft 365 environment (e.g., emails, documents, chats), but this data is not retained or used to retrain the model1. This design ensures data privacy and compliance with federal standards, including FedRAMP authorization3.

11.3 How is this AI system tested and validated to ensure that the decisions or outputs are reliable (relevant to the input) and performs without biases and drifting? Note: Outputs include, User information, transfer to assistor, reports on dashboard depicting activities.

It will also demonstrate how users employ the tools in both expected and unexpected ways, the extent to which users may attempt to use the tools for inappropriate purposes, and the degree to which AI risks manifest in operations. It will assess how users exercise control over the AI to ensure quality products. To monitor Microsoft 365 (M365) Copilot usage, the pilot team will leverage several reporting and auditing tools, including Microsoft 365 Admin Center Reports, Copilot Dashboard in Viva Insights, and Microsoft Purview Audit Logs. The team will: â€¢Engage with the vendor. â€¢Share findings with the user community. â€¢Perform training and education for awareness and mitigation. â€¢Limit AI access to data. Why: 1. The vendor creates and manages the AI, including internal guardrails. The IRS has no control. 2. The tool reacts to user prompts and consumes user data-this is the only way users exercise control over the AI to ensure quality products. Awareness and education are key.

12 Does this system use cloud computing?

Yes

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

Microsoft Corporation, MSO365MT,08/05/2022

12.2 Does the CSP allow auditing?

Yes

12.21 Who has access to the CSP audit data (IRS or 3rd party)?

IRS Cybersecurity

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

Moderate

13 Does this system/application interact with the public?

No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

Access to M365 G5 and the creation of M365 G5 user records is automatic based on the user's completion of the initial request to access the IRS network and agreement to those terms and conditions. Procurement and security information is only used for high-level executive communication and tracking; it is restricted to only those users. M365 G5 is a document management and collaboration platform. Owners of content containers are required to document how they handle

this provision as part of the request for a container. Content Administrators and Owners are responsible for the data they share through the system and are required to declare intent to introduce, collaborate upon, and store PII or SBU data when requesting a container. Content administrators and owners are also required to verify the correct labels are applied to content containers in accordance with IRS CUI marking policies. All corrections or errors should be handled through the IRS standard process to correct errors with the IRS Active Directory. M365 G5 does not allow access to individuals external to IRS. Due process to address federal tax deficiencies is afforded by the Internal Revenue Code and established IRS tax administration procedures, not directly through M365 G5. Any error would be corrected in upstream GS-17 system.

15 Is this system owned and/or operated by a contractor?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

IRS Users, Managers, and Developers have Read and Write access. IRS and Contractor System Administrators have Administrator access. Contractor Users, Developers, and Managers have Read and Write access.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

Notice comes through such communications as the Privacy Act notification on Human Resource Connect (HR Connect) and e-Performance, Single Entry Time Reports (SETR), and other personnel systems. Employee rights are covered through appropriate legal and National Treasury Employees Union (NTEU) contractually negotiated process for remediation. Owners of content containers (sites, M365 Groups, or other) are required to document how they handle this provision at time of request for a container. M365 G5 is internal (not public facing) set of websites and digital services.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

50,000 to 100,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

More than 10,000

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

Not Applicable

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

Less than 10,000

22 How is access to SBU/PII determined and by whom?

The M365 G5 system utilizes the Business Entitlement Access Request System (BEARS) to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access to their local management for approval. Users are not permitted access without a signed form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. M365 G5 is internal (not public facing) set of websites and digital services.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

24 Explain any privacy and civil liberties risks related to privacy controls.

None

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

No

26 Describe this system's audit trail in detail. Provide supporting documents.

Microsoft 365 read and write activities are captured in the M365 Unified Audit Stream and ingested by the IRS Splunk system. Microsoft Intune audit logs are loaded into the IRS Azure "Intune Logging Solution" and then ingested by IRS Splunk.

27 Does this system use or plan to use SBU data in a non-production environment?

No

Interfaces

Interface Type
IRS Systems, file, or database
Agency Name
Microsoft Office Applications
Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
Data gateway connection to Microsoft cloud government services

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 00.001 - Correspondence Files and Correspondence Control Files
Describe the IRS use and relevance of this SORN.
Documentation of interactions with external stakeholders and internal IRS business units.

SORN Number & Name
IRS 36.003 - General Personnel and Payroll Records
Describe the IRS use and relevance of this SORN.
Microsoft 365 supports IRS workforce operations by storing and managing records associated with employee identity, communication, and collaboration. These may include user contact details, organizational role information, and content generated as part of the personnel management activities. This information issued to authenticate users, facilitate access to authorized resources, and support administrative functions required for managing IRS personnel.

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
Microsoft 365 generates and maintains audit logs that capture user access, authentication events, and security-relevant activities across the platform. These records support continuous monitoring, detection of anomalous behavior, and enforcement of IRS cybersecurity policies. Logs are retained to enable incident

response, accountability, compliance validation, and investigation of unauthorized attempts to access or misuse IRS systems and data.

Records Retention

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
3.1: General Technology Management Records
What is the GRS/RCS Item Number?
011
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
System development records
What is the disposition schedule?
Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.

Data Locations

What type of site is this?
Environment
What is the name of the Environment?
Microsoft Office 365 Multi-Tenant & Supporting Services
What is the sensitivity of the Environment?
Personally Identifiable Information (PII) including Linkable Data
Please provide a brief description of the Environment.
The environment is a FedRAMP approved cloud service. Microsoft Government Cloud Services FedRAMP Package ID MSO365MT.
What are the incoming connections to this Environment?
Inbound data is transmitted through a data gateway connection from Microsoft Government Cloud Services. (FedRAMP Approved)
What are the outgoing connections from this Environment?
Outbound data is transmitted through a data gateway connection to Microsoft Government Cloud Services. (FedRAMP Approved)