Date of Approval: 12/12/2025
Questionnaire Number: 2700

Basic Information/Executive Summary

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

Criminal Investigation CI-M365

Business Unit

Criminal Investigation

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.

Microsoft M365 is a Software-as-a-Service (SaaS) platform that enhances administration, functionality, and collaboration for IRS Criminal Investigation (IRS-CI). It integrates productivity tools with communication and storage solutions, allowing IRS-CI users to efficiently manage documents, share information, and engage in secure team collaboration. Permissions are tightly controlled, ensuring cybersecurity protections across various content storage locations. Select IRS-CI users also have guest accounts in an approved agency's tenant for collaboration. Users in the IRS-CI environment include Administrators, Developers, Managers, and Standard Users, each with specific roles and access levels. Additionally, other IRS personnel, federal employees from other agencies that are permitted access through approved collaboration methods, state and local government agencies, and approved external agencies are granted access within clearly defined security parameters. Any data-sharing with outside entities is conducted under formal Memoranda of Understanding (MOUs) and other agreements to ensure compliance and oversight. MOUs are maintained by the

M365 Project Manager and saved in a centralized M365 Project Management site. The platform consists of key components like Exchange Online, OneDrive for Business, SharePoint Online, Teams, Project Online, and Power Platform. It supports real-time messaging, document management, and structured collaboration while maintaining strict security protocols for handling sensitive data, including Personally Identifiable Information (PII) and Federal Tax Information (FTI). The IRS-CI Cybersecurity team oversees controls to safeguard content storage locations. M365 operates under the Microsoft 365 Government G5 licensing scheme, the highest-tier plan designed for U.S. government agencies. This scheme includes advanced security, compliance, and analytics features to meet strict federal regulatory requirements. The enhanced features ensure that IRS-CI can securely manage and store information while remaining compliant with government 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).

The lifecycle of data in M365 starts when a file is created or uploaded, either directly in the cloud or synced from CI-1 GSS. Files remain accessible and editable, with version history tracking changes. Strict security policies ensure that only authorized users can access sensitive data, enforced through Microsoft Entra ID security groups and Microsoft 365 groups. Other M365 apps, such as SharePoint, Teams, and Outlook, can interact with OneDrive data, enabling collaboration while adhering to the same permission sets. Access restrictions prevent unauthorized users from viewing or modifying files, ensuring compliance with organizational policies. Retention policies dictate storage duration based on sensitivity, and deleted files move through the Recycle Bin stages before permanent removal unless retained by policy.

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

Address
Adoption Taxpayer Identification Number
Agency Sensitive Information
Alien Registration Number
Bar Codes
Biometric Information
Centralized Authorization File (CAF)

Citizenship or Migration Status
Comments (Social Media)
Credit Card Number
Criminal Investigation Information
Criminal Record
Document Locator Number (DLN)
Driver's License Number
Education Information
Email Address
Employer Identification Number
Employment Information
Family Members
Federal Tax Information (FTI)
Financial Account Number
Geographical Indicators
Global Intermediary Identification Number (GIIN)
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Language
Medical History/Information
Name
Non-Tax Proprietary data
Official Use Only (OUO) or Limited Office Use (LOU)
Online Identifiers
Other
Passport Number
Patient Number
Personal Characteristics
Photograph
Physical Security Information
Preparer Taxpayer Identification Number (PTIN)
Procurement Sensitive Data
Professional License Number
Protected Information
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number
Telephone Numbers
Universal Unique Identifier (UUID)
Vehicle Identification Number (VIN)

Please explain the other type(s) of PII that this project uses.
Other: Date of Birth (DOB)

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

Information by CI for certain money laundering cases - 18 USC
PII about individuals for Bank Secrecy Act compliance - 31 USC
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?

No

2 Is this a new M365 project?

No

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

Yes

2.11 What is the PCLIA number of the last approved PCLIA for this project?

1634

2.12 What was the name on the last approved PCLIA for this project?

Criminal Investigation CI-M365

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

Changes to PII use to specifically identify Date of Birth (DOB) that wasn't included in the original.

3 Describe your business process and purpose for use of M365; identify what system(s) or business process(es) the M365 supports.

M365 serves as the organization's primary platform for investigations and interagency communications.

4 Do you use Power Automate?

Yes

4.1 Have you documented this in the Data Locations section?

Yes

5 Do you use Visualization Tools (Power BI or Tableau) for reporting from multiple sources?

No

6 Is the data being accessed coming from OneDrive?

Ys

7 Do you have a data dictionary?

No

Interfaces

Interface Type

Other Federal Agencies

Agency Name

Department of Justice - United States Attorney's Office

Incoming/Outgoing

Both

Transfer Method

Secure email/Zixmail

Interface Type

Other Federal Agencies

Agency Name

Federal Bureau of Investigation

Incoming/Outgoing

Both

Transfer Method

Other

Other Transfer Method

A Microsoft 365 tenant setup where IRS-CI guest accounts are created in the FBI tenant granted access to the FBI tenant. The guest accounts are limited by access packages for applications, Teams and SharePoint sites within the FBI boundaries. IRS-CI users must go through an approval process to acquire a guest account.

Interface Type

Other Federal Agencies

Agency Name

Department of Homeland Security

Incoming/Outgoing

Both

Transfer Method

Other

Other Transfer Method

A Microsoft 365 tenant setup where IRS-CI guest accounts are created in the DHS tenant granted access to the DHS tenant. The guest accounts are limited by access packages for applications, Teams and SharePoint sites within the DHS boundaries. IRS-CI users must go through an approval process to acquire a guest account.

Interface Type

Other Federal Agencies

Agency Name

Department of Justice - Tax Division

Incoming/Outgoing

Both

Transfer Method

Secure email/Zixmail

Interface Type

Forms

Agency Name

Multiple tax forms, Form 9131 Request for Grand Jury Investigation

Incoming/Outgoing

Both

Transfer Method

Secure email/Zixmail

Interface Type

IRS Systems, file, or database

Agency Name

Office 365 Multi-Tenant & Supporting Services, M365

Incoming/Outgoing

Both

Transfer Method

Other

Other Transfer Method

CI-1 to M365 data sync for all CI users utilizing a OneDrive for Business Known Folder Move configuration. Local user profiles on laptops have their data synced to their M365 cloud profile through the OneDrive application. This includes any files shared internally through Teams conversations or Teams meetings.

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 46.050 - Automated Information Analysis System

Describe the IRS use and relevance of this SORN.

Results from the analysis of data collected from internal CI systems are processed and synthesized into M365-generated reports.

SORN Number & Name

IRS 46.002 - Criminal Investigation Management Information System and Case Files

Describe the IRS use and relevance of this SORN.

M365 serves as the organization's primary platform for investigations and interagency communications.

SORN Number & Name

IRS 46.005 - Electronic Surveillance and Monitoring Records

Describe the IRS use and relevance of this SORN.

CI uses these records to support ongoing investigations, uphold legal compliance, and preserve the integrity of investigative processes.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

Audit logs are generated within the M365 environment and offloaded into a secure storage solution for long-term data retention and compliance.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GENERAL RECORDS SCHEDULE 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.

This schedule covers records created and maintained by Federal agencies related to the general management of technology. It includes records related to developing, operating, and maintaining computer software, systems, and infrastructure improvements; complying with information technology policies and plans; and maintaining data standards.

What is the disposition schedule?

Destroy when 5 years old, but longer retention is authorized if needed for business use.

Data Locations

What type of site is this?

System

What is the name of the System?

Splunk Security

What is the sensitivity of the System?

Sensitive But Unclassified (SBU)

Please provide a brief description of the System.

Splunk Security is a suite of products that helps organizations identify, investigate, and respond to security threats by analyzing data from various sources, including IT infrastructure.

What are the incoming connections to this System?

Splunk collects logs from M365 using the Splunk Add-on for Microsoft Office 365, which connects to the Office 365 Management API to pull audit logs from Azure Active Directory, SharePoint Online, and Exchange Online. It also gathers service status updates and security-related events. Once ingested, logs are indexed for analysis, helping track security incidents, login anomalies, and service health. These logs are stored as indexed events in a proprietary database in custom on-prem locations (CI-1) configured by the administrators.

What are the outgoing connections from this System?

Splunk collects logs from M365 using the Splunk Add-on for Microsoft Office 365, which connects to the Office 365 Management API to pull audit logs from Azure Active Directory, SharePoint Online, and Exchange Online. It also gathers service status updates and security-related events. Once ingested, logs are indexed for analysis, helping track security incidents, login anomalies, and service health. These logs are stored as indexed events in a proprietary database in custom on-prem locations (CI-1) configured by the administrators.

What type of site is this?

System

What is the name of the System?

Criminal Investigation General Support System, CI-1 GSS.

What is the sensitivity of the System?

Sensitive But Unclassified (SBU)

Please provide a brief description of the System.

Criminal Investigation (CI) serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law. The CI-1 GSS is integral in supporting the mission of CI as the GSS provides network connectivity to internal CI applications. The CI network provides users with the necessary infrastructure to access email services, file services, print services, and access to management and inventory database systems. The network operates on top of the IRS wide area network (WAN) with CI local area network (LAN) segments isolated behind CI routers for additional layer of security. Due process is provided outside of the system pursuant to 26 USC and 18 USC.

What are the incoming connections to this System?

M365 primarily syncs from Active Directory as the authoritative source using Microsoft Entra Connect for user authentication. OneDrive syncs files bidirectionally. When a file is uploaded to OneDrive from another device or the web, it will appear in the synced OneDrive folder on your system. Any changes made to the file in the cloud will also reflect on your local device once synchronization occurs.

What are the outgoing connections from this System?

CI-1 GSS syncs Active Directory objects to M365, ensuring user accounts, groups, and contacts remain up to date. The initial sync transfers all selected objects, followed by periodic updates that reflect changes in the directory. Authentication methods, including Password Hash Sync and Pass-through Authentication, help manage user access. OneDrive Known Folder Sync backs up Desktop, Documents, and Pictures to M365, ensuring files stay accessible. Though separate from the Active Directory sync cycle, it integrates with Microsoft Entra ID for seamless identity management. When files are stored in the user's local profile folders that are configured in the OneDrive sync, they will sync to the M365 environment.