Date of Approval: **July 29, 2022**

PIA ID Number: **7064**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Microsoft 365 Government 5, M365 G5

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

Microsoft 365 Government 5, M365 G5

What is the approval date of the most recent PCLIA?

12/29/2021

Changes that occurred to require this update:

Significant System Management Changes

New Access by IRS employees or Members of the Public

Were there other system changes not listed above?

Yes

What were those changes?

Federation within M365 allows users from TIGTA and IRS-CI to access content and collaborate with IRS employees, where need-to-know requirements are met. The second release of Teams will include adding the following features/enhancements for availability within the Teams application. - Microsoft Whiteboard: a free-form, digital canvas where people, content, and ideas come together. Whiteboard integration in Microsoft Teams meetings is powered by the Whiteboard web app, which lets Teams meeting participants draw, sketch, and write together on a shared digital canvas. - OneNote: an online, digital note-taking app that provides a single place for keeping all of your notes, research, plans, and information in an easy to organize interface. OneNote also supports print, and share, and search functionality. - Planner: a light weight, mobile and web-based application that allows you and your team to create plans, assign tasks, chat about tasks, and see charts of your team's progress. - Winnie Chatbot: an online resource that quickly provides customers the answers customer self-service experience that is to be pinned to Teams. - Webinars: allows registration and polling as part of large conference style meetings. This will be open for both internal and external participants. - Private and Shared Channels: Inside of a Team (as a container) these features allow users to create sub-groups for collaboration. Overall, across M365, the following features and services were updated and/or introduced. - Microsoft Visio Web App was added to the list of end user applications. - Microsoft Stream service is no longer a stand-alone service in M365 and is now part of SharePoint Online.

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Both the Cloud Governance Board (CGB), the Enterprise Operations Governance Board (EOPs GB), and the UNS Technical Integration Board (TIB).

Current ELC (Enterprise Life Cycle) Milestones:

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

System Development/Milestone 4B

System Deployment/Milestone 5

Operations & Maintenance (i.e., system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

Microsoft 365, Government Level 5 (M365 G5) is a Software-as-a-Service (SaaS) product that acts as a platform to combine familiar Microsoft Office Productivity suite with online versions of Microsoft's next-generation communications and collaboration services. M365 will allow the Internal Revenue Service (IRS) to simplify administration and improve functionality for end users. The components of M365 G5 include (but are not limited to): Exchange Online (EXO) - Replacing on-premises Exchange One Drive for Business (ODB) - Providing an alternative file sharing service SharePoint Online (SPO) - replacing on-premises SharePoint 2013. Teams - replacing Skype Project Online (PJO) - providing a new service for project management. The overall purpose of M365 G5 is to provide a backbone for team collaboration, with email, instant messaging, and team sites is to store, maintain, and share information as it correlates to the objectives and goals of the IRS Business Units. Information owners are responsible for the data they share through the system. Processes and procedures built into the system will replace Privacy Impact Assessment (PIA) previously required for SharePoint sites. Controls will be configured as needed for any content storage locations (within ODB, SPO, Teams, or PO) storing Sensitive But Unclassified (SBU) or Personally Identifiable Information (PII) data. These content storage locations are referred to as "Content Containers," and include, but not limited to: SPO site collections, ODB libraries, Teams collaboration groups, PJO project sites, and M365 Groups. Federation of the IRS M365 allows users from TIGTA and IRS-CI to access content and collaborate with IRS employees, where need-to-know requirements are met. TEAMS is a multi-function application which will replace components of Microsoft Skype for Business and SharePoint. TEAMS provides collaboration sites and messaging for both one-to-one and one-to-many communication. TEAMS uses SharePoint On-Line (SPO) sites for file/document storage and management. TEAMS also uses SPO sites for user interfaces. TEAMS uses an updated instant messaging component similar to Skype, offering both voice and video capabilities. TEAMS uses both a desktop and mobile client for access to the system. TEAMS offers options for external dial-in. TEAMS also support external collaboration. Enhancements to Teams provides full integration with Whiteboard, OneNote, and Planner from the overall M365 user application suite. The Webinars feature provides registration and polling support inside conference style Teams meetings. In addition, Winnie Chatbot is configured for easy access within the Teams application. Inside of TEAMS private channels provide a sub-container for collaboration within a smaller set of users, as opposed to the entire team collaboration group. Shared channels provide a means add individuals from outside the team (but internal to the IRS or federated partners) for collaboration around specific topics, but not grant those individuals access to other parts of the team's collaboration. For both private and shared channels, TEAMS and SPO create separate and dedicated file storage, content management, and channel messaging spaces as a sub-container. Those sub-containers inherit the sensitivity settings from the parent TEAMS container. The purpose of the SPO software is to provide a backbone for team collaboration sites is to store, maintain, and share information as it correlates to the objectives and goals of the Internal Revenue Service (IRS) Business Units. It provides the tools to maintain and manage the IRS SPO platform, technical documentation, plans, policies, standard operating procedures, and allows users to leverage built-in tools for manipulating data and presentations. It will also house day-to-day materials to assist the teams with tracking progress including meeting minutes, agenda and internal knowledge documentation that assist in storing key internal knowledge for customers looking to create a SPO collection. SharePoint will host functionality such as collaboration on documents, document management, and structured data storage. ODB software provides personal storage within the M365 cloud SaaS environment. This functionality maps to current usage of personal shares on file shares and the My Documents folder of the workstations. ODB uses the same document storage components as SharePoint Online (SPO) and TEAMS. ODB will host functionality such as document storage and management. ODB supports one-on-one document collaboration through the TEAMS service from M365. The individual users have options to share documents from their personal ODB site. But controls limit the user's ability to share documents outside the IRS. As part of the full M365 G5 product, user have access to additional applications. Most of these applications are used within the context of a content container to allow users to create, update, retrieve, and dispose (where permitted by retention rules) of information. The data from these applications remains exclusively inside the M365 storage areas and access is governed by permissions set on the content container. Those applications include Microsoft Calendar, Delve, Excel Web App, Word Web App, Visio Web App, PowerPoint Web App, OneNote Web App, Microsoft Forms, Microsoft Lists, Microsoft Planner, Power Automate, Power Apps, Power BI, Stream (on SharePoint), and Whiteboard. In addition, there is one application which aggregates user activity to provide analytics and suggestions to improve personal productivity, known as Viva Insights (formerly known as MyAnalytics and simply Insights). The IRS is disabling the use of Viva Insights pending full review of the applications capabilities and business need.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e., last 4 digits, etc.)?

No

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing Address
Phone Numbers
E-mail Address
Standard Employee Identifier (SEID)
Internet Protocol Address (IP Address)
Photographic Identifiers

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Procurement sensitive data   Contract proposals, bids, etc.

Protected Information   Information which if modified, destroyed, or disclosed in an unauthorized manner could cause loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Technical documentation, plans, policies, standard operating procedures, and presentations. It will also house day-to-day materials including meeting minutes, agenda and internal knowledge documentation that assist in storing key internal knowledge for customers looking to create a content container. While the M365 G5 core platform uses only limited PII (Name, SEID, work contact information, workstation information), individual content containers may store PII/SBU information. Owners of content containers which will store PII/SBU are responsible for documenting how they will handle PII/SBU as part of the process for requesting a container (site, M365 Group, or other). TEAMS collects call quality data, call history, support data, feedback data, diagnostic data, and service data. These elements can contain PII. The data is collected for use with service quality assessment and troubleshooting system issues. This PII and private data is stored by the system, in aggregate, within M365, and is not exposed to any systems external to M365 or the IRS.

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

PII for personnel administration is 5 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

Standard Employee Identifier (SEID), Login Account, Name, Phone E-mail are used to grant access to content, and may also be used by the M365 G5 Services organization to contact users as part of the oversight and management of the M365 G5 platform. IP Addresses and workstation information is recorded as part of system logging. Procurement and security information is only used for high-level executive communication and tracking; it is restricted to only those users. All other uses of SBU/PII will be documented when requesting a container (site, M365 Group, or other).

How is the SBU/PII verified for accuracy, timeliness, and completion?

M365 G5 user information is obtained via a daily automatic synchronization with the IRS Active Directory (AD). Any corrections to the data should be handled per standard processes for updating the IRS AD. Procedures for verifying the accuracy, timeliness, and completeness of SBU/PII will be documented in content container specific controls.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 36.003	General Personnel and Payroll Records
IRS 00.001	Correspondence Files and Correspondence Control Files
IRS 34.037	Audit Trail and Security Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

11/20/2014

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

3rd Party

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

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.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

M365 G5 is a document management and collaboration platform. At time of request for a container, owners of content containers are required to document how they handle this provision.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

All corrections or errors should be handled through the IRS standard process to correct errors with the IRS Active Directory. M365 G5 is a document management and collaboration platform. Owners of content containers (sites, M365 Groups, or other) are required to document how they handle this provision when requesting a container.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Write

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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

Access to M365 G5 and the creation of M365 G5 user records is automatic based on the user's completion of an Online-5081 request for access to 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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

M365 G5 is a document management and collaboration platform. Since M365 will be used to store a significant array of record types at the IRS, all applicable records schedules must be applied. All applicable retentions related to GRS and RCS items will be built into the Compliance Center over time and available to be applied by users. Users are responsible for applying the appropriate policy to ensure records are retained according to respective schedules. GRS 3.1 Item 011-System development records-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. GRS 5.1 Item 010-Administrative records maintained in any agency office. Destroy when business use ceases. IRS policy will allow storage of records in SPO and Teams. However, ODB is considered a storage location for working documents only. ODB is not authorized for the storage of records at the IRS.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

12/28/2021

Describe the system's audit trail.

The platform records multiple types of audit data within the M365 G5 logs. Document versioning functionality has been enabled to track history of information uploaded and updated. Additional options to audit access to information are available within the M365 G5

Administrative capabilities. These enable auditing of the access, or ability to access (via permissions), sites collections or other containers of potential PII/SBU.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

System is currently in operations and maintenance. However, individual services under M365 G5 may require separate system test plans. Results of those are stored in the M365 G5 Program Office SharePoint site.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: 50,000 to 100,000

Contractors: More than 10,000

Members of the Public: Not Applicable

Other: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

M365 G5 is a document management and collaboration platform. Owners of content containers where records are stored are responsible for documenting the categories of records as part of requesting a container. A Teams Webinar is considered a container. Where a Webinar organizer includes individuals external to the IRS, the organizer creates the event as part of an existing TEAMS container, thus inheriting the categories of records.

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax, or Privacy Act consent?

No