Date of Approval: **July 19, 2022**

PIA ID Number: **7136**

SYSTEM DESCRIPTION

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

Office 365 Multi-Tenant & Supporting Services, M365

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, Most recent PCLIA: 6584

What is the approval date of the most recent PCLIA?

12/29/2021

Changes that occurred to require this update:

Significant System Management Changes

Were there other system changes not listed above?

Yes

What were those changes?

A decision was made to merge the One Drive PCLIA 5586, SharePoint PCLIA 5579, and Teams PCLIA 5489 with the new Microsoft 365 PCLIA. The PCLIA will include Exchange Online (EXO) Teams SharePoint Online (SPO) One Drive for Business (ODB)* Project Online (PJO) Power Platform & PowerApps * ODB is part of the license for SharePoint Online which is part of the IRS' G5 license

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

Cloud Governance Board (CGB) and the Enterprise Operations Governance Board (EOPs GB).

Current ELC (Enterprise Life Cycle) Milestones:

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.

M365 Program will migrate on-premises solutions for Microsoft applications of Exchange, SharePoint, Teams, OneDrive, Project Online, and on-premises storage of user files (home drive servers) to the cloud-based Microsoft 365 Software-as-a-Service (SaaS) environment. IRS CI currently maintains a cloud-based Microsoft Pro Plus subscription model which authenticates users to receive The M365 Program will take the next steps to move the Microsoft 365 Server products/workload to the Cloud, including: Exchange Online (EXO) Teams SharePoint Online (SPO) One Drive for Business (ODB)* Project Online (PJO) * ODB is part of the license for SharePoint Online which is part of the IRS' G5 license.

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)
Criminal History
Financial Account Numbers
Photographic Identifiers
Employment Information
Tax Account Information

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.

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

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

Information by CI for certain money laundering cases may be 18 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, criminal history; financial account numbers; tax account information; and photographic identifiers 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?

Network communications in Teams are encrypted by default. Teams' data is protected on the network by requiring all servers to use certificates for traffic taking place over Transport Layer Security (TLS)/Hypertext Transfer Protocol Secure (HTTPS)-encrypted channels. 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?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Criminal Investigations General Support System (CI-1 GSS)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 5/4/2022

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

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

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?

IRS

What is the background check level required for CSP?

High

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 Only

Contractor Managers: Read Only

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 a Business Entitlement Access Request System (BEARS) 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.

One Drive for Business is the online storage space in the cloud that's provided for individual licensed users in an organization. This application will help protect work files and allow access across multiple devices. OneDrive lets you share files and collaborate on documents, and sync files to end user computer.

SA&A OR ASCA

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

In-process

When is the anticipated date of the SA&A or ACS completion?

9/26/2022

Describe the system's audit trail.

This interface enables the M365 Security Information and Event Management (SIEM) to send audit data and logs to the on-premise Splunk server. The Azure SIEM gathers logs and audit data and transfers the files to Splunk on a set frequency. The files are securely transmitted to the IRS on-premise environment utilizing M365 Splunk application programming interface (API). The Splunk Add-on for M365 is used to collect log data from Azure Active Directory (AD) and M365. The log data includes Azure AD Audit and Login activity of Exchange Online, SharePoint, Teams, OneDrive and Project Online are transferred to the IRS on-premise Splunk server.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

M365 will have a new environment in the cloud in addition to maintaining the existing on-prem environment. Microsoft support team provided the M365 data network Test Architecture for Exchange Online, SPO, ODB, PJO and Teams.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Responsible Testing Organization: IRS Enterprise Operations, Criminal Investigations Technology Operations. Testing and validation activities: cyber checks, network security validations, default Sharing link types, privacy, data loss prevention, AdHoc conferencing, express route, and Proxy Auto Configuration (PAC) file testing, external sharing permissions, device access, blocked file types, auditing, file retention, alerts, monitoring, notifications, transfer ownership for separated employees.

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: More than 100,000

Contractors: More than 10,000

Members of the Public: 100,000 to 1,000,000

Other: No

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