Date of Approval: **July 23, 2021**

PIA ID Number: **6135**

SYSTEM DESCRIPTION

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

O365 Exchange Online Migration, O365 EXO

Is this a new system?

Yes

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

Enterprise Services Cloud Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

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 Exchange Online (EXO) is service within the Microsoft 365 (M365). M365 is a Software-as-a-Service (SaaS) product that hosts cloud-based components of enterprise, Microsoft services. EXO provides an e-mail hosting, e-mail transport services, and messaging compliance and security. EXO allows agencies to integrate on-premise Exchange server infrastructure with a hybrid configuration.

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.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Security Background Investigations

Interfaces with external entities that require the SSN

Legal/statutory basis (e.g., where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Delivery of governmental benefits, privileges, and services

Law enforcement and intelligence purposes

Another compelling reason for collecting the SSN

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

IRS personnel may continue to use SSNs for IRS official business as specified in IRM 10.5.1.6.8.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The EXO system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from IRC 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Other Taxpayer Identification Number

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
Date of Birth
Place of Birth
Standard Employee Identifier (SEID)
Mother's Maiden Name
Protection Personal Identification Numbers (IP PIN)
Internet Protocol Address (IP Address)
Criminal History
Medical Information
Certificate or License Numbers
Vehicle Identifiers
Passport Number
Alien Number
Financial Account Numbers
Photographic Identifiers

Biometric Identifiers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

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:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Procurement sensitive data Contract proposals, bids, etc.

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Proprietary data Business information that does not belong to the IRS.

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.

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.

IRS personnel may use e-mail to share SBU/PII needed to conduct IRS official business as specified in IRM 10.5.1.6.8.

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)

SSN for tax returns and return information is Internal Revenue Code Section 6109

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 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.

Business units within the IRS define the business needs, uses, and policies for e-mail to transmit SBU/PII. Privacy Policy and Compliance (PPC) clarifies the IRS-wide policy for use of SBU/PII in IRM 10.5.1.

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

The sender/recipients of SBU transmitted via e-mail are responsible for verification of accuracy, timeliness, and completeness.

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 34.037 Audit Trail and Security Records

IRS 00.001 Correspondence Files and Correspondence Control Files

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: EMAIL
Current PCLIA: No
SA&A: No

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

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Any Federal Agency
Transmission Method: EMAIL/SMTP
ISA/MOU: No

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

Yes

For each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Any State or Local Agency
Transmission Method: EMAIL/SMTP
ISA/MOU: No

Does the system receive SBU/PII from other sources?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: PUBLIC
Transmission Method: EMAIL/SMTP
ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: Various
Form Name: Tax Administration Forms

Form Number: Various
Form Name: Personnel Administration Forms

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

Yes

Please identify the form number and name:

Form Number: Various
Form Name: Personnel Administration Forms

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: SPLUNK
Current PCLIA: Yes
Approval Date: 1/24/2020
SA&A: Yes
ATO/IATO Date: 6/25/2021

Identify the authority.

IRC Section 26 U.S.C. 6103

For what purpose?

IRS official business

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: Various Federal Agencies
Transmission Method: Email
ISA/MOU: No

Identify the authority.

IRC Section 26 U.S.C. 6103

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

ROUTINE USES OF RECORDS MAINTAINED BY THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSE OF SUCH USES: Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described in SORN IRS 00.001 Correspondence Files and Correspondence Control Files, and IRS 34.037 Audit Trail and Security Records.

For what purpose?

IRS official business

Does this system disseminate SBU/PII to State and local agencies?

Yes

Identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Various State Agencies
Transmission Method: Email
ISA/MOU: No

Identify the authority.

IRC Section 26 U.S.C. 6103

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

ROUTINE USES OF RECORDS MAINTAINED BY THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSE OF SUCH USES: Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described in SORN IRS 00.001 Correspondence Files and Correspondence Control Files, and IRS 34.037 Audit Trail and Security Records.

For what purpose?

IRS official business

Does this system disseminate SBU/PII to IRS or Treasury contractors?

Yes

Identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: IRS Contractors as Appropriate
Transmission Method: Email
ISA/MOU: No

Identify the authority.

IRC Section 26 U.S.C. 6103

For what purpose?

Yes

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

Yes

Does this system disseminate SBU/PII to other Sources?

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.?

Yes

Briefly explain how the system uses the referenced technology.

Approved IRS personnel may enroll to send/receive/view e-mail on government-owned and personal mobile devices via the IRS mobile messaging program.

Does the system use cloud computing?

Yes

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

Yes

Date Certified.

9/24/2020

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?

None

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
Maintenance

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Not Applicable

Please explain.

The Exchange online transaction will be considered out of scope and will not require a DIRA/e-RA.

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?

The IRS provides timely and effective notice to the public and/or to individuals about activities that impact privacy. For information that is collected pursuant to a request from the IRS, notice is provided as part of that request. The IRS Privacy Act statements are included on all forms, websites, and other instruments by which Privacy Act information is collected from individuals, either in written or oral form.

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):

The opportunity or right depends on how the information is collected. The IRS generally does not use O365 to collect information, including PII, directly from the public. Information in O365 pertaining to IRS employees and contractors is collected to authenticate end-users and manage administrative business functions including personnel security, human resources, emergency notifications, etc.

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

Notice, consent, and due process are provided via the IRS systems and their related forms instructions, and pursuant to Title 5 USC.

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?

An IRS user may provide access to SBU/PII by sending a message to a specific recipient, by allowing an individual to have access to the message in his/her/their mailbox folder where SBU/PII is stored, or by using a shared/organizational mailbox where SBU/PII is shared. Administrators may access/view unencrypted SBU/PII messages when performing tasks to support a user. Administrator access is approved via an access request. Individuals performing eDiscovery tasks in support of an official investigation may view SBU/PII messages included in eDiscovery search results. Management determines access to the system.

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.

IRS emails are managed in accordance with General Records Schedule (GRS) 6.1, item 010 (CAPSTONE Permanent) and 011 (All others) Temporary 20 years.

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?

6/10/2021

Describe the system's audit trail.

Mailbox activity is audited and stored within Microsoft Exchange.

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 PMP SharePoint site

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?

All security-related testing.

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: More than 1,000,000

Other: Yes

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

The public's information is not collected directly by O365. However, information provided by and pertaining to members of the public may be stored in O365.

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?

Yes

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? Contact Disclosure to determine if an accounting is required.

Yes