Date of Approval: **June 28, 2023**

PIA ID Number: **7686**

SYSTEM DESCRIPTION

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

SBSE BU Default Dedicated Environment, SBSE Default Env

Is this a new system?

Yes

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

M365 TRB (Technical Review Board)

Current ELC (Enterprise Life Cycle) Milestones:

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

No

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.

Small Business/Self Employed (SB/SE) has multiple internal processes that utilize SharePoint that are critical processes across the business unit. For example: We have approval processes; processing that ensure steps and balances are accounted for (per IRM requirements); various processes that send/track/document steps done at various levels of a specific process; we have input forms used internal to our organization that send data to SharePoint Online repositories; etc. Currently, these items are built in the Personal Productivity environment, which unfortunately means the solutions belong to an individual rather than to the group/business unit. A Business Unit environment will allow our organization to have more control over the lifecycle of the solutions; maintain governance and standards of the solutions; and centralize controls when migrating these processes to the cloud and virtualizing new processes. The SBSE environment resides within the IRS M365 Tenant and inherits all controls, policies, and permissions from the tenant. The applications built within the SBSE environment will use native M365 connections to data stored within the IRS M365 tenant. These connections inherit existing controls and policies from the IRS M365 Tenant.

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

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

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

There are many processes within SBSE that capture and maintain SSN's including forms, letters, and written documentation. This content is important for the review, approval, and case work. In several instances this could even be the official federal record and all the documents associated with the process would be attached and tored/retained in SharePoint.

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

There is no way that we could eliminate the use of SSN's in this environment.

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:

Photographic Identifiers
Name
Mailing Address
Phone Numbers
E-mail Address
Date of Birth
Standard Employee Identifier (SEID)
Criminal History
Medical Information
Certificate or License Numbers
Vehicle Identifiers
Passport Number
Alien Number
Financial Account Numbers
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:

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.

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.

PII: - Death records - General privacy - Health information, also known as Protected Health Information (PHI) Tax Information: - Federal Taxpayer Information (FTI), which includes individual and corporate (or other business) tax return information under IRC 6103 - Written determinations Financial information in the Finance category: - Bank Secrecy Act (31 U.S.C. Bank Secrecy Act protected reports filed by financial institutions) - International financial institutions Any documents containing PII that will support a case/casework, approval requests, and/or data storage could be part of the process. Specific Forms or source types will be dependent on the process and IRM procedures.

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.

The metadata captured in SharePoint that could be connected to Power Apps and the Dedicated Environment could include SSN/EIN as these are unique identifiers that would allow administrators and employees working these cases the ability to relocate associated content based on this unique number. Additionally, there are many forms letters and documents that include this information and this PII would also be stored in images and attachments that have been uploaded to the sites and connected to.

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

The documents that are uploaded and attached are created outside of SharePoint and the Dedicated Environment. Accuracy, timeliness, and completeness will be verified prior to upload. The metadata in SharePoint will typically be user input and as such, always be subject to user error. The metadata can be changed and will not be locked to address any user error that may be found up until which time the item becomes Federal Record if that applies to the process. Each process will have their own internal workflow for verification of PII prior to the record creation that would prevent any future changes.

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 49.001 Collateral and Information Requests System

IRS 26.013 Trust Fund Recovery Cases/One Hundred Percent Penalty Cases

IRS 26.019 Taxpayer Delinquent Account Files

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 36.003 General Personnel and Payroll Records

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 26.001 Acquired Property Records

IRS 44.001 Appeals Case Files

IRS 36.001 Appeals, Grievances and Complaints Records

IRS 42.008 Audit Information Management System

IRS 34.037 Audit Trail and Security Records

IRS 24.047 Audit Underreporter Case Files

IRS 10.001 Biographical Files, Communications and Liaison

IRS 10.008 Certified Professional Employer Organizations

IRS 42.021 Compliance Programs and Projects Files

IRS 00.002 Correspondence Files: Inquiries about Enforcement Activities

IRS 22.062 Electronic Filing Records

IRS 34.012 Emergency Preparedness Cadre Assignments and Alerting Roster Files

IRS 00.007 Employee Complaint and Allegation Referral Records

IRS 42.002 Excise Compliance Programs

IRS 42.001 Examination Administrative Files

IRS 42.002 Excise Compliance Programs

IRS 22.061 Information Return Master File

IRS 26.009 Lien Files

IRS 26.012 Offer in Compromise Files

IRS 26.014 Record 21, Record of Seizure and Sale of Real Property

IRS 00.008 Recorded Quality Review Records

IRS 10.004 Stakeholder Relationship Management and Subject Files

IRS 26.020 Taxpayer Delinquency Investigation Files

IRS 00.333 Third Party Contact Records

IRS 26.021 Transferee Files

IRS 42.005 Whistleblower Office 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: SharePoint Online
Current PCLIA: No
SA&A: No

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.

8/5/2022

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?

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. Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC. 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):

Data is captured prior to submission into SharePoint, and all means of consent would happen prior to entry. Sites with SBU/PII on them would have their own PIA with these procedures. Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

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

This PCLIA is in association with an environment for development. The data is captured and stored outside of Power Apps and flows in SharePoint Online. Due process would apply to the data source itself which is SharePoint Online. Sites with SBU/PII on them would have their own PIA with these procedures. Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 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 Only

Managers: Read Only

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor Developers: Read Write

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

PII/SBU is determined at the data source. All data would be captured from SharePoint and those sites would be required to maintain their own PIA regarding the data that would be used.

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.

Data Retention is maintained at the data source which is SharePoint Online. Each project that would utilize this environment would have their own data retention policy and PIA. RCS 9, 16, 20, 23, 22, 24, 28, 29, 32, 34, various items GRS 1.1, 2.1, 2.2, 2.3, 2.4, 2.6, 3.1, 3.2, 4.3, 5.1, 5.2, 5.4, 5.5, 5.7, 5.8, various items

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?

2/1/2022

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:

Any project that would require an STP would notate this requirement in their associated project PIA. This PCLIA would only cover the development environment itself, not the development or final product.

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: Under 5,000

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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

This environment will come with an Office 365 User Profile data connection. This allows applications to prepopulate fields with information from Active Directory such as name, SEID, job title, manager name etc. There are no tracking mechanisms turned on in this environment to capture the user’s current location or "track" a user other than when they access the application and their associated AD information.

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