Date of Approval: **July 20, 2023**

PIA ID Number: **7838**

SYSTEM DESCRIPTION

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

CFO BU dedicated environment, CFO-BU-Prod

Is this a new system?

Yes

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

M365 Technology 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.

Chief Financial Officer (CFO) 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 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 CFO environment resides within the IRS M365 Tenant and inherits all controls, policies, and permissions from that tenant. The applications built within the CFO 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:

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

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

Employee, vendor, and taxpayer data is used for unpaid tax assessment transactions. Federal agencies require, in administration of their activities, a system of accounts which identifies each person individually. Tableau and Power BI require the use of Taxpayer Identification Numbers (TINs) because no other identifier can be used to uniquely identify a taxpayer at this time. The use of TINs is permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. The use of IRS employee's SSNs are permissible for personnel administration according to 5 USC & Executive Order 9397. Therefore, the statistical and research data tools will require the use of SSNs because no other identifier can be used to uniquely identify individuals at this time.

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

No mitigation at this point as the level of detail required for analysis dictates these unique identifiers. Federal agencies require, in administration of their activities, a system of accounts which identifies each person individually. The use of IRS employee's SSNs are permissible for personnel administration according to 5 USC & Executive Order 9397. Tableau and Power BI require the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. The use of SSNs is permissible from Internal Revenue Code (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)
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:

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.

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.

Employee travel information, including location, authorization amounts, voucher amounts. Other employee information, including training requests, training completion, and projects assigned to employees. Vendor information, including vendor name, invoice numbers, invoice amounts and payment amounts.

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

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 SBU identifiers such as name, SEID, and M365 profiles that would allow employees submitting forms to be identified for a response from the Business Unit (BU). Other SBU information, such as addresses, and employment information is captured and saved to SharePoint to streamline administrative processes and collect contact information of business partners external to CFO. The use of Concur data to report on mission critical travel and to analyze travel voucher accuracy; use of Integrated Financial System (IFS) and Concur data to monitor business units' financial performance scorecard results; use of Financial Management Information System (FMIS) data to monitor and identify outliers in social security deferrals; and use of SharePoint list data to report on project towards completion of CFO priority projects. There is no reasonable substitute for SSN, EIN, or TIN to identify taxpayers, employees and/or vendors for this analysis.

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

The underlying systems providing SBU/PII have internal programming consistency checks and record counts and are considered reliable and have been verified by the internal source or external agency providing the information through completion of audits and reviews. Hence, source of information is considered accurate, timely, and complete. The other 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 SBU information 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 42.008 Audit Information Management System

IRS 36.003 General Personnel and Payroll Records

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 22.054 Subsidiary Accounting Files

IRS 42.021 Compliance Programs and Projects Files

IRS 35.001 Reasonable Accommodation Request 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 sites
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

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

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):

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

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

Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC." because as stated due process applies to the data source. SharePoint Online and some of the PII on the SharePoint comes from tax information.

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 Users: Read Only
Contractor Developers: Read Write

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

Business Entitlement Access Request System (BEARS) or is access granted by an administrator.

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. GRS 1.1 Item 001 - Financial management and reporting administrative records - Destroy when 3 years old, but longer retention is authorized if needed for business use. GRS 1.1 Item 011 - All other copies - Copies used for administrative or reference purposes - Destroy when business use ceases. GRS 1.3 Item 010 - Budget formulation, estimates, justification, and submission records, fiscal year 2017 and forward - Destroy 6 years after close of fiscal year, but longer retention is authorized if required for business use. GRS 1.3 Item 020 - Budget execution records - Destroy 6 years after close of fiscal year, but longer retention is authorized if required for business use. Temporary. GRS 1.3 Item 030 - Budget reports - Full fiscal - year reports - Destroy when 5 years old, but longer retention is authorized if required for business use. GRS 1.3 Item 31 - All other reports - Destroy when 3 years old, but longer retention is authorized if required for business use. RCS 16 Item 1 - Budget Correspondence Files - Destroy when 2 years old. RCS 16 Item 2 Budget Background Records - Destroy 1 year after the close of the fiscal year covered by the budget. RCS 16 Item 3a - Budget Reports Files - Annual report (end of fiscal year) - Destroy when 5 years old. RCS 16 Item 3b - All other reports - Destroy 3 years after the end of the fiscal year. RCS 16 Item 4 - Budget Apportionment Files - Destroy 2 years after the close of the fiscal year. RCS 16 Item 5 - Accountable Officers' Files. (NARA - GRS 6) - Destroy 6 years and 3 months after period covered by account. RCS 16 Item 6 - GAO Exceptions Files General Accounting Office notices of exceptions such as Standard Form 1100, formal or informal and related correspondence. (NARA - GRS 6) - Destroy 1 year after exception has been reported as cleared by GAO. RCS 16 Item 7a - Certificates Settlement Files, Certificates covering closed account settlements, supplemental settlements, and final balance settlements - Destroy 2 years after date of settlement. RCS 16 Item 7b - Certificates covering period settlements - Destroy when subsequent certificate of settlement is received. RCS 16 Item 9a - Accounting Administrative Files - Files used for workload and personnel management purposes - Destroy when 2 years old. RCS 16 Item 9b - All other files - Destroy when 3 years old. RCS 16 Item 16 - RRA 98 Section 1204 Certification Records - Destroy 3 years after closure. RCS 16 Item 18 - Chief Financial Officer Accounts Receivable Dollar Inventory (ARDI) Management System (CAMS). RCS 17 Item 29C - Financial Planning System (FPS) - (C) Outputs: Budget data is transferred to the Integrated Financial System (IFS). FPS also produces reports used for executive level review of actual versus planned spending - Delete/Destroy 3 years after cutoff. GRS 5.2: Transitory and Intermediary Records: Data displayed are not the official records. The dashboard developers will ensure that data and reports are appropriately destroyed/deleted when no longer needed for reference. These copies are maintained in accordance with General Records Schedule (GRS) 5.2, item 020 Intermediary Records published in IRS Document 12829. Disposition: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

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), site 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 a System Test Plan 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: 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