Date of Approval: **March 12, 2023**

PIA ID Number: **7556**

SYSTEM DESCRIPTION

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

Chief Financial Officer - Tableau and Power BI, CFO Data Viz

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?

Chief Financial Office -Tableau Enterprise Visualization, ID 6490, Final Approval 12/31/2021

What is the approval date of the most recent PCLIA?

12/13/2021

Changes that occurred to require this update:

New Access by IRS employees or Members of the Public

Were there other system changes not listed above?

Yes

What were those changes?

Expansion of approved data visualization software to include both Tableau and Power BI.

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

Not applicable. The business unit chief executive is approving this PCLIA.

Current ELC (Enterprise Life Cycle) Milestones:

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

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.

Tableau and Power BI enable data visualization and analysis capabilities to provide timely and reliable reporting for more effective decision-making at all levels. Neither Tableau nor Power BI store or move Sensitive But Unclassified (SBU) /Personally Identifiable Information (PII) data, but rather point to and use data in place. Data connections include flat files such as Excel, Text and .csv files as well as connections to Microsoft SharePoint lists. Tableau and Power BI support the IRS Business Intelligence Strategy and will also enable users to increase productivity. Data visualization examples include but are not limited to use of Integrated Talent Management (ITM) and Discovery Directory data to monitor completion of mandatory briefings; use of Integrated Financial System (IFS) data to monitor staffing levels against budget and to monitor. Concur data is used to report on mission critical travel and to analyze travel voucher accuracy. IFS and Concur data is used to monitor business units' financial performance scorecard results. Financial Management Information System (FMIS) data is used to analyze custodial revenue and identify outliers in social security deferrals. SharePoint list data is utilized to generate reports that highlights status of CFO commitments and priority projects. This information is used to perform various analysis, reporting, and reconciliations in support of business operations, Treasury Inspector General for Tax Administration (TIGTA) requests, and the annual financial statement audit.

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)
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.

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.

Tableau and Power BI dashboards display specific SBU/PII data as required for monitoring, analysis, or decision-making. Data visualization examples include but are not limited to: use of ITM and Discovery Directory data to monitor completion of mandatory briefings; use of IFS data to monitor staffing levels against budget; use of Concur data to report on mission critical travel and to analyze travel voucher accuracy; use of IFS and Concur data to monitor business units' financial performance scorecard results; use of 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. IRS will use both internal and third-party data collected by federal and state agencies which are stored on IRS owned custodial data bases and the data is validated for accuracy by the system sending the data as described in that system's PCLIA. This data and the referrals are used to perform further research and verification using IRS systems and IRS data to determine audit potential or other appropriate action. Where indicators of non-compliance exist, IRS will take the necessary enforcement actions to ensure compliance.

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

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: Microsoft 365
Current PCLIA: Yes
Approval Date: 7/29/2022
SA&A: Yes
ATO/IATO Date: 2/7/2023

System Name: Financial System (IFS)/Procurement for Private Sector (PPS)
Current PCLIA: Yes
Approval Date: 5/11/2021
SA&A: Yes
ATO/IATO Date: 1/13/2023

System Name: Financial Management Information System (FMIS)
Current PCLIA: Yes
Approval Date: 10/1/2020
SA&A: Yes
ATO/IATO Date: 8/20/2022

System Name: Integrated Talent Management (ITM)
Current PCLIA: No
SA&A: No

System Name: ConcurGov
Current PCLIA: Yes
Approval Date: 5/24/2021
SA&A: Yes
ATO/IATO Date: 6/11/2020

System Name: Discovery Directory (Corporate Authoritative Directory Service (CADS))
Current PCLIA: Yes
Approval Date: 9/18/2020
SA&A: Yes
ATO/IATO Date: 1/30/2020

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?

Yes

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

No

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

No

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

No

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

No

Does this system disseminate SBU/PII to other Sources?

Yes

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

Organization Name: Internal Sources
Transmission Method: CFO Tableau Enterprise Visualization
ISA/MOU: No

Organization Name: Government Accountability Office
Transmission Method: Images, PowerPoint, Word and/or Excel files
ISA/MOU: No

Organization Name: Internal Sources
Transmission Method: Power BI Workspace
ISA/MOU: No

Organization Name: U.S. Treasury Inspector General for Tax Administration (TIGTA)
Transmission Method: Images, PowerPoint, Word and/or Excel files
ISA/MOU: No

Identify the authority.

26 U.S.C. 6103; 31 U.S.C. § 3515

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

IRS 42.008: Audit Information Management System; This system is exempt from 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(1), (e)(4)(G) -(I) and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). (See 31 CFR 1.36).

For what purpose?

The information is primarily disseminated internally to conduct different types of analysis, reconciliation, research, or reporting. Mandatory reports of reconciliation of accounting/financial information may be disseminated to auditors at the Government Accountability Agency (GAO) or the U.S. Treasury Inspector General for Tax Administration (TIGTA) as required for financial or program audits.

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.

2/7/2023

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?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

Tableau and Power BI do not collect information. Instead, information is obtained from various IRS systems of record and files. Notice, consent, and due process are provided at the point of origin (such as tax forms). The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number. Any individual information is received from a system that provides employees with notice and rights to consent and/or amend, as needed.

Notice comes through such communications as the Privacy Act notification on HR Connect and e-Performance, SETR, and other personnel systems. Employee rights are covered through appropriate legal and National Treasury Employees Union (NTEU) contractually negotiated process for remediation.

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

No

Why not?

Tableau and Power BI do not collect information. Because information is obtained from various IRS systems of record and files, notice, consent, and due process are provided at the point of origin (such as tax forms). The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information. Employee rights are covered through appropriate legal and NTEU contractually negotiated process for remediation.

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

Tableau and Power BI do not by themselves provide for due process. Because information is obtained from various IRS systems of record and files, notice, consent, and due process are provided at the point of origin (such as tax forms). The system does not replace any individual taxpayer's right to due process, as dictated by the Internal Revenue Manual guidelines. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. However, due to the nature of this system, individuals may not receive specific notice that their information has been collected. Employee rights are covered through appropriate legal and NTEU contractually negotiated process for remediation.

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 Tableau dashboards is managed via the Business Entitlement Access Request System (BEARS). Access is granted on a need-to-know basis, depending on the user's roles and responsibilities. The BEARS enrollment process requires that an authorized manager and a secondary approver within the Office of the Chief Financial Officer approve requests on a case-by-case basis. Users are given the minimum set of privileges required to perform their regular and recurring work assignments, and they are restricted from changing the boundaries of their access without management approval. The employee's access will be terminated once they no longer require access. Deletion from the active access role is also performed through the BEARS. Access to Power BI dashboards is managed by content administrators and owners, who are responsible for the data they share through the Power BI dashboard. Access is granted on a need-to-know basis, depending on the user's roles and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments, and they are restricted from changing the boundaries of their access without content administrators or owners' approval. The employee's access will be terminated once they no longer require access. Deletion from the active access role is managed by content administrators and owners.

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.

GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records: Data displayed in Tableau or Power BI are not the official records and therefore the Tableau Server or Power BI instances are not considered an official recordkeeping system. 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?

11/2/2020

Describe the system's audit trail.

Tableau is managed by the Business Intelligence Core Competency Center (BICCC) within Information Technology. Tableau Server includes auditing capability that tracks user activity in the system, from successful sign-on to workbooks viewed/accessed, refreshed, or created. Each transaction is recorded in the audit tables. The latest Security Assessment and Authorization for Tableau as part of the Enterprise Business Intelligence Platform (EBIP) is dated 11/2/2020. Power BI is managed by the Microsoft 365 Program Management Office within Information Technology. The platform records multiple types of audit data within the Microsoft 365 G5 logs. The latest FedRAMP Security Threat Analysis Report for M365 is dated 2/7/2023.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

For Tableau, the Enterprise Business Intelligence Platform (EBIP) is responsible for the System Test Plan. EBIP is currently in the Operations and Maintenance phase of its lifecycle. Annual Security Control Assessment occurs annually to ensure that controls remain in place to properly safeguard PII. For Power BI, the Microsoft 365 Program Management Office is responsible for the System Test Plan. Microsoft 365 is currently in the Operations and Maintenance phase of its lifecycle. Annual Security Control Assessment occurs annually to ensure that controls remain in place to properly safeguard PII.

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: Under 100,000

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?

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