Date of Approval: **July 18, 2023**

PIA ID Number: **7883**

SYSTEM DESCRIPTION

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

CCH TeamMate, TM+

Is this a new system?

No

Is there a PCLIA for this system?

No

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

Financial Services Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

System Deployment/Milestone 5

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.

Commerce Clearing House (CCH) TeamMate is the industry standard in Audit Management Systems. The Department of the Treasury, Internal Revenue Service selected CCH TeamMate as its official electronic audit software package. TeamMate provides a platform to deliver high quality audits, standardize the work paper process, leverage auditor knowledge, enhance audit reporting and provide management with key information. TeamMate was designed for use across all business sectors for all types of audits. Audit departments of all sizes are using TeamMate to increase the efficiency and productivity of their entire audit

process, including risk assessment, scheduling, time and expense tracking, planning, execution, review, report generation, trend analysis, committee reporting and storage. CCH TeamMate enables users to create, review and approve audit documentation. CCH TeamMate enables users to cross-reference, import and track the status of results. CCH TeamMate enhances uniformity to documentation development, reviews and referencing of work papers improving quality assurance into the documentation process.

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)

Delivery of governmental benefits, privileges, and services

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

Some data obtained for internal controls testing include employee payroll data, taxpayer data etc.

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

The system does regularly use SSNs or TINs. The data that is obtained for testing controls for various processes, programs, and systems, occasionally contains SSNs or TINs.

Employer 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:

Standard Employee Identifier (SEID)
Mother's Maiden Name
Protection Personal Identification Numbers (IP PIN)
Criminal History
Medical Information
Certificate or License Numbers
Passport Number
Alien Number
Financial Account Numbers
Photographic Identifiers
Employment Information
Tax Account Information
Name
Mailing address
Phone Numbers
E-mail Address
Date of Birth
Place of Birth

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.

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?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

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 use of reporting to validate the safeguarding of assets and to facilitate internal audits share externally with the Government Accountability Office (GAO) and the US Department of Treasury. Certain transactions require obtaining data containing PII. TeamMate stores user's results analysis. There are no tests directly related to PII but the controls in place which sometimes include PII. Only users and leaders responsible for performing testing and reviews have access to the project.

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

As part of our internal controls testing, we verify the data for 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 42.001 Examination Administrative 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?

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?

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: U.S. Department of the Treasury
Transmission Method: Risk and Control Sharepoint site
ISA/MOU: Yes

Organization Name: Government Accountability Office
Transmission Method: Axway
ISA/MOU: Yes

Identify the authority.

OMB Circular A-123 Appendix A

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

Treasury/IRS 42.001 Examination Administrative Files

For what purpose?

For Financial Assurance Controls Testing (FACT).

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?

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.

5/13/2022

Please identify the ownership of the CSP data.

Third Party

Does the CSP allow auditing?

No

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.

The data collected does not come directly from the individual. Internal controls testing consists of evaluating a sample of data from various programs, processes, and systems to confirm if key controls are effective from preventing anything more than standard, acceptable risk.

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

No

Why not?

We are not communicating with individuals. We are evaluating sampled data from programs, processes, and systems which contain the information.

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

The system stores data to include our analysis to determine if key internal controls are effectively in place to prevent fraud, waste, and abuse. Data is restricted by people who are evaluating data or performing preliminary and secondary reviews.

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 Contractor 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 Only

IRS Contractor Employees

Contractor System Administrators: Administrator

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

Internal Revenue Manual guidance

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.

GRS 4.1 Item 020: Our team submits form 11671, Certificate of Record Disposal, to request approval to dispose of data six years or older. GRS 1.1: Financial Management and Reporting Records Item 001 GRS 1.1: Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. Item 010 GRS 1.1: Property, plant, and equipment (PP&E) and other asset accounting. item 030 GRS 1.1: Records supporting compilation of agency financial statements and related audit, and all records of all other reports. item 020 GRS 1.3 item 031 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 2.1: Employee Acquisition Records items 030, 040, 050, 060, 090, 120, 130, 150, GRS 2.2: Employee Management Records items 010, 020, 050, 060, 070, GRS 3.2: Information Systems Security Records 010 and 030 GRS 5.7: Agency Accountability Records 010, 020, 050

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

No

Describe the system's audit trail.

The system captures, date, time, and user activity (upload, approval, review) along with edit history of the document.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

It is a COTS product. A user acceptance testing would be completed when the system becomes active.

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: Under 50,000

Contractors: Under 5,000

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?

No