Date of Approval: **March 06, 2023**

PIA ID Number: **7478**

SYSTEM DESCRIPTION

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

Technical Operations, TechOps

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.

Cybersecurity and Privacy Governance Board (CPGB)

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?

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.

Cybersecurity Operations is responsible for ensuring the security and resilience of the IRS's information and information systems in support of the federal tax administration processes through 24/7 cyber incident management, cyber/fraud analytics, compliance monitoring/reporting and situational awareness. IT Cybersecurity protects taxpayer information and the Internal Revenue Service's electronic systems, services, and data from internal and external cyber security related threats by implementing World Class security practices in planning, implementation, management, and operations. IT Cybersecurity will preserve the confidentiality, integrity and availability of the IRS and its assets. We must protect IRS information and information systems from threats - criminal, insider, or self-

inflicted accidental events - that weaken our security. Moreover, taxpayer information and the IRS ability to leverage technology to support modernized tax administration business processes must have the highest level of trust and confidence.

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).

The Cybersecurity Fraud Analytics and Monitoring program requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. Technical Operations has implemented technologies into the IRS enterprise that monitor the IRS applications and platforms to detect attacks, and indicators of

potential attacks, and data loss prevention. Some of those technologies may capture SSN as they attempt to exit the IRS, or while being transported to other systems. Technical Operations will ingest those events.

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 audit logs that TechOps collects may include sensitive information such as SSN which are forwarded by other IRS information monitoring systems. SSNs are 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
Standard Employee Identifier (SEID)
Protection Personal Identification Numbers (IP PIN)
Internet Protocol Address (IP Address)
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.

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.

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.

Logs containing information related to Network Internet Protocol address (IP address). Server names. A Uniform Resource Locator (URL), also referred to as a web address. Domain Name Servers (DNS).

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

PII for personnel administration is 5 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 Federal Information Security Modernization Act (FISMA) directs federal agencies to develop and implement procedures for detecting, reporting, and responding to computer security incidents. IRS implements these requirements through their Computer Security Incident Response Center (CSIRC). CSIRC serves as a central mechanism for receiving and disseminating computer security incident information and provides a consistent capability to respond to and report cyber-related incidents. It includes capabilities that provide infrastructure security components to prevent and detect emerging threats. PII is needed for intelligence gathering, intrusion analysis, and reporting confirmed cyber incidents. The business objective of Cybersecurity Fraud Analytics and Monitoring (CFAM) is to detect and prevent identity theft and frauds. To achieve this, CFAM relies on the monitoring and analyzing of log transactions with IRS's online services. These transactions records contain PII/SBU including SSNs/TINs, Internet Protocol (IP) addresses, email addresses, phone numbers, refund amounts, home addresses, etc. They are the core data fields for CFAM's analytic and modeling effort to detect suspicious access patterns and identify potential Identity Theft (IDT)/fraud perpetrators and victims. SSN/TIN: the main item CFAM users to identify a taxpayer and extract online transactions related to his/her account. CFAM also receives SSN/TIN information from Return Information Control System (RICS)/Criminal Investigation (CI)/ Treasury Inspector General for Tax Administration (TIGTA) when they request CFAM's collaboration in various investigations. Additionally, CFAM also uses SSN/TIN to request further information from IRS organizations/databases, such the Return Review Program (RRP) or Compliance Data Warehouse (CDW). Finally, CFAM also uses SSN/TIN to extract family clusters and detect abnormal filing patterns. Internet Protocol Address (IP addresses)/Email addresses/Phone numbers: CFAM uses these items to detect and identify suspicious online accesses and activities.

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

The data that Technical Operations receives is a machine-to-machine connection from internal IRS systems that are deemed reliable, and the data is validated for accuracy by the sending system as described in the system's PCLIA. TechOps will maintain audit log information that consist of PII data. TechOps will conduct required security tests and continuous monitoring activities to verify and validate that IRS Audit Trail Requirements are met in accordance with IT Security Policy and Guidance (IRM 10.8.1). Access to audit management functionality shall only be authorized to CSIRC systems administrators. This will protect audit information and tools from unauthorized access, modification, and deletion. Audit Trail Records shall be backed up daily onto a different system. IRS information systems shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support investigation and response to suspicious activities within the

organization. The stored data CSIRC, User Behavior Analytics Capability (UBAC), Cybersecurity Fraud Analytics and Monitoring (CFAM) and User & Network Services (UNS) analysts use is presented in a read-only format; therefore, analysis does not affect the integrity of the raw data.

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 36.003 General Personnel and Payroll 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: eAuthentication
Current PCLIA: Yes
Approval Date: 6/16/2021
SA&A: Yes
ATO/IATO Date: 9/15/2022

System Name: IRS Perimeter Security (GSS-1)
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 2/3/2023

System Name: Transcript Delivery System (TDS) (eServices)
Current PCLIA: Yes
Approval Date: 11/16/2021
SA&A: Yes
ATO/IATO Date: 11/10/2022

System Name: Return Review Programs
Current PCLIA: Yes
Approval Date: 10/17/2022
SA&A: Yes
ATO/IATO Date: 6/2/2022

System Name: Integrated Customer Communications Environment
Current PCLIA: Yes
Approval Date: 12/13/2022
SA&A: Yes
ATO/IATO Date: 6/29/2022

System Name: Streaming Data Monitoring Tool (SDMT)
Current PCLIA: Yes
Approval Date: 12/15/2021
SA&A: Yes
ATO/IATO Date: 3/7/2022

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?

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: Treasury Inspector General for Tax Administration
Transmission Method: Encrypted email
ISA/MOU: No

Organization Name: Criminal Investigation
Transmission Method: Encrypted email
ISA/MOU: No

Organization Name: Return Integrity & Compliance Services
Transmission Method: Encrypted email
ISA/MOU: No

Organization Name: Privacy, Governmental Liaison and Disclosure's
Transmission Method: Encrypted email
ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 1040
Form Name: U.S. Individual Income Tax Return

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?

Yes

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

System Name: Enterprise Physical Access Control System (EPACS) #6701
Current PCLIA: Yes
Approval Date: 8/19/2022
SA&A: Yes
ATO/IATO Date: 3/21/2022

Identify the authority.

5 U.S.C 301, 1302, 2951, 4118, 4308 and 4506 18 U.S.C. 1030 (a)(2)(B) 26 U.S.C. 7801 Executive Orders 9397 and 10561.

For what purpose?

To identify and track any unauthorized accesses to sensitive but classified information and potential breaches or unauthorized disclosures of such information.

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: Treasury Inspector General for Tax Administration
Transmission Method: encrypted email
ISA/MOU: No

Organization Name: Criminal Investigation
Transmission Method: encrypted email
ISA/MOU: No

Organization Name: Return Integrity & Compliance Services
Transmission Method: encrypted email
ISA/MOU: No

Organization Name: Privacy, Governmental Liaison and Disclosure's
Transmission Method: encrypted email
ISA/MOU: No

Identify the authority.

The authority was given by the ACIO Associate Chief Information Officer of Cybersecurity and the Director of Security Operations.

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

This system has been designated exempt from sections (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 PII data is shared for the purpose of supporting criminal investigations, identifying potential tax refund fraud, and facilitating treatment for the taxpayers that were victimized. TIGTA - Treasury Inspector General for Tax Administration CI - Criminal Investigation RICS - Return Integrity & Compliance Services PGLD - Privacy, Governmental Liaison and Disclosure's.

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?

No

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?

IT Security Policy and Guidance IRM 10.8.1.4.1.7 System-Use Notifications states, IRS Information Systems (networked and standalone) with an interactive access interface shall display an approved system-use notification message/warning banner for IRS-approved notification message/warning banner text) before granting access to the system. The system-use notification message/warning banner shall inform potential users that: The user is accessing a U.S. Government information system. (a) System usage may be monitored, recorded, and subject to audit; (b) Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; (c) The use of the system indicates consent to monitoring and recording; and (d) There shall be no expectation of personal privacy on these information systems. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. Our legal right to ask for information is Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. They say that taxpayers must file a return or statement with us for any tax they are liable for. Their response is mandatory under these sections.

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

No

Why not?

TechOps does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent, and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC. Or if gathered from tax form: The IRS has the legal right to ask for information per Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for". Their response is mandatory under these sections.

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

The Technical Operations process and procedures are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. Due process is provided 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 Only

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Only

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

The Technical Operations system utilizes the IRS Business Entitlement Access Request System (BEARS) application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access via BEARS to their local management for approval consideration. Users are not permitted access without a signed BEARS form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the BEARS form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access. Users are assigned to specific modules of the application and specific roles within the modules and accounts follow the principle of least privilege which provide them the least amount of access to PII data that is required to perform their business function after receiving appropriate approval.

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.

Any records generated and maintained by the system will be managed according to requirements under IRS Records Control Schedule 17 Information Technology and General Records Schedule 3.2 Information Systems Security Records Items 010, 030 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. All records housed in the TechOps system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Primarily Data collected by CSDW fall under Computer security incident handling, reporting and follow-up records fall under General Records Schedule 3.2 item 020 and should be maintained for a minimum of three years after all necessary actions have been completed but longer retention is authorized. IRS Records and Information Management (RIM) Program and Cyber landed on seven years to ensure compliance and ensure they are maintained in accordance with GRS 3.2 item 020.

SA&A OR ASCA

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

In-process

When is the anticipated date of the SA&A or ACS completion?

1/15/2023

Describe the system's audit trail.

Technical Operation Audit Trails: a. Date b. Time c. Systems' Information (e.g., name, address) d. Employee ID e. Action taken (e.g., read, write, execute, delete) will be configured in accordance with IRS IT Security Policy and Guidance (IRM 10.8.3).

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

Continuous Monitoring (eCM) (now called Annual Security Control Assessment (ASCA)) 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: More than 100,000

Contractors: Under 5,000

Members of the Public: More than 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?

Yes

Explain the First Amendment information being collected and how it is used.

The system collects information supplied via Tax forms to validate Taxpayers are who they say they are when they are requesting their Taxpayer documents. These factors are used as a validation process.

Please list all exceptions (any one of which allows the maintenance of such information) that apply:

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance (as noted in Q17).

Will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges under Federal programs?

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.

Technical Operations will receive and store IRS Network's system log data, which contains IP Address, Email Address and SEID of IRS employees and contractors accessing IRS systems and IRS facilities.

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