Date of Approval: **February 07, 2022**

PIA ID Number: **6757**

SYSTEM DESCRIPTION

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

Service-Wide Employment Tax Research System, SWETRS

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?

SWETRS PIA # 3861

What is the approval date of the most recent PCLIA?

12/12/2019

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

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

IT's Compliance Domain Executive Steering Committee (ESC).

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.

The Service Wide Employment Tax Research System (SWETRS) is an Internal Revenue Service (IRS) application that is used to monitor, compare, and evaluate information related to special programs, issues, and projects that identify areas of Employment Tax non-compliance. Using this information, available efforts can be focused on the more significant non-compliance issues. Certain records within SWETRS may be used to select businesses or individuals for compliance actions. The application was deployed into production on December 15, 2008. The SWETRS project provides the capability to: Centralize a uniform and systematic method of employment tax case selection, thereby increasing the efficiency of workload selection; Automate current labor-intensive, manual analysis of data not available in any other application, while incorporating fraud and collectability indicators; Deliver case inventory to a requesting user, as well as provide useful managerial reports; Implement a standardized method of case selection and delivery of case inventory to a requesting user (Pre-filing, Outreach, Enforcement - both Field and Campus Collection); Collect, capture, and store in the Remote Data Entry (RDE) feature of SWETRS various employment tax forms submitted by employers, preparers & agents. Obtain reports via the business objects web intelligence portal.

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:

Legal/statutory basis (e.g., where collection is expressly required by statute)

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

The SSN number is needed to research and locate records in response to the request.

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 known mitigation strategy planned to eliminate the use of SSN for the system; SSN is required for the use of this system. The SSN number is needed to research and locate records in response to the request.

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:

Name
Mailing address
E-mail Address
Standard Employee Identifier (SEID)
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.

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?

No

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

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.

SWETRS is used to provide a means to monitor, compare and evaluate information related to special programs, issues and projects that identify areas of Employment Tax non-compliance. Using this information, available efforts can be focused on the more significant non-compliance issues. SWETRS provides employment tax non-compliance data to its users through reports generated via the Business Object reporting capability hosted by the Business Intelligence Core Competency Center (BICCC). These reports can be run on-demand or on an as needed basis.

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

SWETRS receives data from trusted internal sources. The data received by SWETRS is verified by the various applications as being complete and accurate prior to being transmitted to SWETRS. Additionally, the SWETRS system schema is configured in accordance with its data sources; the date, when it is received from Service Center Recognition Imaging Processing System (SCRIPS), and Research, Applied Analytics & Statistics Data Management (RAAS) will automatically load in the right format. SWETRS receives data from SCRIPS and RAAS daily The schedule is in accordance with established agreements between the SWETRS project office and the project office of the individual data source suppliers. Data files transferred from SCRIPS and RAAS to SWETRS are protected by using secure Enterprise File Transfer Utility (EFTU) to transmit the 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 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: RAAS
Current PCLIA: Yes
Approval Date: 2/23/2016
SA&A: Yes
ATO/IATO Date: 4/3/2018

System Name: SCRIPS
Current PCLIA: Yes
Approval Date: 11/25/2020
SA&A: Yes
ATO/IATO Date: 4/16/2020

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?

Yes

Please identify the form number and name:

Form Number: Form 2678
Form Name: Employer/Payer Appointment of Agent

Form Number: Form 14492
Form Name: Compliance Settlement Program

Form Number: Form 8952
Form Name: Application for Voluntary Classification Settlement Program (VCSP)

Form Number: Form 14493
Form Name: Employee Data Report

Form Number: CSP CLOS440, CLOSWC, CLOSCC, VCSP
Form Name: Classification Settlement Agreements

Form Number: Gaming Industry Tip Compliance Agreement Program
Form Name: Tip Agreement

Form Number: Tip Rate Determination Agreements
Form Name: Tip Agreement

Form Number: Form 8027
Form Name: Employer's Annual Information Return of Tip Income and Allocated Tips

Form Number: Form 14439
Form Name: Employer Data Report

Form Number: Schedule R
Form Name: Allocation Schedule for Aggregate 941/940/943 Filers

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: Federal Unemployment Tax Act Tier 1 (FUTA:FUTATIER1)
Current PCLIA: No
SA&A: No

System Name: Security Audit and Analysis System (SAAS)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 4/29/2020

Identify the authority.

EFTU Authorizations via Form 14598

For what purpose?

Federal Unemployment Tax Act Tier 1 (FUTA:FUTATIER1): Data is received from the States and then compared to the FUTA Masterfile to identify potential tax adjustment cases. The resulting data is downloaded to FUTA TIER2 for case processing and reconciliation. Security Audit and Analysis System (SAAS): Implements a data warehousing solution that provides on-line analytical processing (OLAP) access to audit trail data to detect security

violations. SAAS collects, stores, and reports audit trail data for the investigation of instances of Unauthorized Access (UNAX) violations against Internal Revenue Service (IRS) applications.

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?

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?

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?

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.

This is generally not applicable to the application. The data collected is from data that is submitted by various sources, employers, employees, third parties, and/or are part of a rev rule or rev proc or announcement. The information within SWETRS comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. SWETRS 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, and pursuant to 5 USC.

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):

This is generally not applicable to the application. Employers, employees and third parties are able to utilize free will in submitting the various documents. The data collected is from data that is submitted by various sources, employers, employees, third parties, and/or are part of a rev rule or rev proc or announcement. The information within SWETRS comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. SWETRS 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, and pursuant to 5 USC. Providing the data is a condition for participation in a tip agreement. If the data is not provided, IRS can go forward for revocation of a Tip Rate Determination Agreement (TRDA) or let the agreement expire for a Gaming Industry Tip Compliance Agreement (GITCA).

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

This is generally not applicable to the application. In the event a correction, redress or access is required it would follow the general process in place as applicable. The data collected is from data that is submitted by various sources, employers, employees, third parties, and/or are part of a rev rule or rev proc or announcement. The information within SWETRS comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. SWETRS 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, 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 Write

Managers: Read Write

Developers: Read Write

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

Access Request System (BEARS) request to gain access to the SWETRS data. The BEARS process requires the user's manager to review and approve the access request before the request is forwarded to SWETRS to add the user SEID to the approved SWETRS functional groups. A user's access to the SWETRS system data terminates when it is no longer required. The SWETRS system ensures that all access accounts to the system that have been inactive for more than 45 days are disabled. The SWETRS system removes all SWETRS system accounts after 90 days of inactivity.

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.

All records housed in the SWETR will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and

1.15.6 and will be destroyed using IRS Records Control Schedules (RCS) 29, item 65 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

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?

1/26/2022

Describe the system's audit trail.

SWETRS audit trails capture user access, failed login attempts, user logouts, opening/closing of files and other activities mandated by IRM 10.8.3. The SWETRS audit log records an audit trail of user actions and shall include the following information for each audit entry: User ID, Date/Time of Event, Event Description, and source IP address of access.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

DocIT (Web-based document management system)

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

The SWETRS Business Unit with the assistance and guidance of IT Cybersecurity, ensures that routine security-related activities are conducted on the SWETRS application. These activities include, but are not limited to: security assessments, audits, system hardware and software maintenance, security certifications, and testing and/or exercises. Advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations. Coordinating and planning activities occur prior to conducting any security related activities affecting the application. When security audits, Security Control Assessment (SCA), Security Impact Assessments (SIA), Security Risk Assessments (SRA) or certification activities are required, the Business Unit Security PMO, Security Assessment Services (SAS) and IT Cybersecurity communicate with the Business Unit (BU) to ensure that they understand the scope of the security activity to be conducted. The BU coordinated with IT Cybersecurity and SB/SE Security Program Management Office to ensure that testing is conducted. After these security assessments are done, they are combined into one Security Assessment Report.

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: Not Applicable

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?

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