Date of Approval: February 12, 2019 PIA ID Number: **3861**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Service-Wide Employment Tax Research System, SWETRS

2. Is this a new system? No

2.a. If no, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If yes, enter the full name, acronym, and milestone of the most recent PCLIA.

SWETRS PIA # 1635

Enter the approval date of the most recent PCLIA. 01/26/2016

If yes Indicate which of the following changes occurred to require this update (check all that apply).

No Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
No Conversions
No Anonymous to Non-Anonymous
No Significant System Management Changes
No Significant Merging with Another System
No New Access by IRS employees or Members of the Public
No Addition of Commercial Data / Sources
No New Interagency Use
No Internal Flow or Collection
Yes Expiring PCLIA

Were there other system changes not listed above? No

3. 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).

3.a. Check the current Enterprise Life Cycle (ELC) Milestones (select all that apply).

No Vision & Strategy/Milestone 0
No Project Initiation/Milestone 1
No Domain Architecture/Milestone 2
No Preliminary Design/Milestone 3
No Detailed Design/Milestone 4A
No System Development/Milestone 4B
No System Deployment/Milestone 5
Yes Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

A.1 General Business Purpose

5. 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 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. SWETRS users are able to generate reports on employment tax non-compliance data via the Business Objects reporting capability.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6.a. If 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

If yes, check all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
No	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
No	Interfaces with external entities that require the SSN
Yes	Legal/statutory basis (e.g. where collection is expressly required by statute)
No	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

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.

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? Yes

If yes, specify the information.

Selected	PII Element
Yes	Name
Yes	Mailing address
No	Phone Numbers
Yes	E-mail Address
No	Date of Birth
No	Place of Birth
Yes	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
No	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If yes, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
Yes	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. Are there other types of SBU/PII used in the system? No

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

Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)

Yes SSN for tax returns and return information is Internal Revenue Code Section 6109

No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

No PII for personnel administration is 5 USC

No PII about individuals for Bank Secrecy Act compliance 31 USC

No Information by CI for certain money laundering cases may be 18 USC

6.f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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 via the Business Object reporting capability hosted by the Business Intelligence Core Competency Center (BICCC).

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

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 IPM, SCRIPS, and 94X-XML will automatically load in the right format. SWETRS receives data from SCRIPS and 94X-XML daily and from IPM annually. The schedule is in accordance with established agreements between the SWETRS project office and the project office of the individual data source suppliers.

C. 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.

9. 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

If yes, enter the SORN number(s) and the complete the name of the SORN(s).

SORNS Number	**SORNS Name**
IRS 42.021	Compliance Programs and Projects Files

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11.a. If yes, does the system receive SBU/PII from IRS files and databases? Yes

If yes, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Integrated Production Model (IPM)/Big Data Analytics (BDA)	Yes	11/03/2017	Yes	05/04/2019
Modernize e-file (MEF)	Yes	02/23/2016	Yes	04/03/2018
SCRIPS	Yes	11/28/2017	Yes	11/19/2018

11.b. Does the system receive SBU/PII from other federal agency or agencies? No

11.c. Does the system receive SBU/PII from State or local agencies? No

11.d. Does the system receive SBU/PII from other sources? No

11.e. Does the system receive SBU/PII from Taxpayer forms? Yes

If yes, identify the forms.

Form Number	Form Name
Form 2678	Employer/Payer Appointment of Agent
Form 14492	Compliance Settlement Program
Form 8952	Application for Voluntary Classification Settlement Program (VCSP)
Gaming Industry Tip Compliance Agreement Program	Tip Agreement
Tip Rate Determination Agreements	Tip Agreement
Form 8027	Employer's Annual Information Return
Form 14439	Employer Data Report

11.f. Does the system receive SBU/PII from Employee forms (such as the I-9)? No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? No

17.b. If 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.

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

18.a. If 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).

19. 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.

I. INFORMATION PROTECTION

20. 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

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	No	
Developers	Yes	Read and Write

Contractor Employees? No

21.a. How is access to SBU/PII determined and by whom? The users must submit an Online5081 to request access to the SWETRS data. The request must be approved by the users' managers before being forwarded to the SWETRS Business Unit (BU). The SWETRS BU are responsible for reviewing the request and ensuring the user are added to the appropriate access control list in order for the user to receive proper access to the SWETRS data.

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22.a. If yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and 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.

I.2 SA&A OR ASCA

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

23.a. If yes, what date was it completed? 11/30/2018

23.1 Describe in detail 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a. If yes, was the test plan completed? Yes

24.a.1. If yes, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? DocIT (Web-based document management system)

24.a.2. If yes, were all the Privacy Requirements successfully tested? Yes

24.a.3. If yes, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process 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.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26.a. IRS Employees:	Under 50,000
26.b. Contractors:	Not Applicable
26.c. Members of the Public:	More than 1,000,000
26.d. Other:	No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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

End of Report