

Date of Approval: January 26, 2016

PIA ID Number: **1635**

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

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Service Wide Employment Tax Research System , SWETRS, 208, O&M

Next, enter the **date** of the most recent PIA. 1/15/2013

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

No Addition of PII

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

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) 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

6a. 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 who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

<u>Yes</u>	Social Security Number (SSN)
<u>Yes</u>	Employer Identification Number (EIN)
<u>No</u>	Individual Taxpayer Identification Number (ITIN)
<u>No</u>	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
<u>No</u>	Practitioner Tax Identification Number (PTIN)

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.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On</u> <u>Primary</u>	<u>On</u> <u>Spouse</u>	<u>On</u> <u>Dependent</u>
Yes	Name	Yes	Yes	No

Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

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

6e. 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

6f. 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? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

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

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

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

SORNS Number

SORNS Name

42.021

Compliance Programs and Projects Files-Treasury/IR

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. N/A

E. INCOMING PII INTERFACES

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

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

If **yes**, enter the files and databases.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
IPM BDA	Yes	10/15/2014	Yes	07/17/2014
SCRIPS	Yes	01/09/2015	Yes	01/30/2015
MeF	Yes	12/17/2014	Yes	11/09/2015

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

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

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

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

If **yes**, identify the forms

<u>Form Number</u>	<u>Form Name</u>
Form 2678	Employer/Payer Appointment of Agent
Form 14492	Compliance Settlement Program
Form 8952	Application for Voluntary Classification Settlement Program (VCSP)
GITCA	Tip Agreement
TRDA	Tip Agreement
Form 8027	Employer's Annual Information Return
Form 14439	Employee Data Report

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

F. PII SENT TO EXTERNAL ORGANIZATIONS

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, cloud, global position system (GPS), biometrics, 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/is notice provided to the individual prior to collection of information? No

17b. 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

18a. 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 TRDA agreement or let the agreement expire for a 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

<u>IRS Employees?</u>	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

<u>Contractor Employees?</u>	<u>Yes/No</u>	<u>Access Level</u>	<u>Background Invest.</u>
Contractor Users			
Contractor Managers			
Contractor Sys. Admin.			
Contractor Developers			

21a. How is access to SBU/PII determined and by whom? The users must submit an OL5081 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.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ?
Not Applicable

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

22a. 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.

SWETRS data, employee tax returns and related documentation are approved for destruction 6 years after end of processing year under NARA Job No. NC1-58-78-4, and published in IRS Document 12990 under Records Control Schedule 29 for Tax Administration - Wage and Investment Records, item 65. However, in reviewing SWETRS-related recordkeeping practices for completion of this PIA, system owners and the IRS Records Office determined that a re-evaluation of RCS 29, item 65 description and disposition authority (at least as they relate to SWETRS functionality and use) are in order. SB/SE and the Records Office will work together to validate and potentially update the item (or create a new RCS item) to better fit SWETRS data collection activities and maintenance needs, and the electronic recordkeeping environment.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 12/7/2015

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

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process**, 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 MITS 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 MITS 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 MITS 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.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Doct

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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:

26a. IRS Employees: Under 50,000
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. 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 9/11 Commission Recommendations 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

N. ACCOUNTING OF DISCLOSURES

30. 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
