

NOTE: The following reflects the information entered in the PIAMS Website.

---

## A. SYSTEM DESCRIPTION

---

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

---

Date of Approval: 04/02/2014 PIA ID Number: 809

---

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

---

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Selection and Workload Classification Component 2 - Release 2.5 MS4B, (SWC C2)

---

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

---

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Not Applicable

---

4. Responsible Parties:

NA

---

5. General Business Purpose of System

---

The Selection and Workload Classification Component 2 (SWC\_C2) application provides a Business Rules Engine, which will execute business rules and filters against data obtained from a Large Business and International Division (LB&I) production database system, named LB&I Data Capture System (DCS-2). The objective of the system is to identify the tax returns that are the highest risk for errors and score those returns so that they may be selected for further review and possible examination. The system also provides explanations as to why a particular item on the return was identified as a potential risk. Due process is provided pursuant to 26 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact \*Privacy and request a search) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 04/22/2011

---

6b. If Yes, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
  - System is undergoing Security Assessment and Authorization Yes
- 

6c. State any changes that have occurred to the system since the last PIA

None

---

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. 015-000000165-LMSB

---

## B. DATA CATEGORIZATION

---

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems Yes  
Employees/Personnel/HR Systems Yes

Other Source: \_\_\_\_\_

Other No

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	No	No	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: No

PII Name On Public? On Employee?

No No

10a. Briefly describe the PII available in the system referred to in question 10 above.

SWC\_C2 utilizes entity information which includes Name, EIN, Address and Tax Return information for Large Business population.

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is not needed.

SWC\_C2 has application audit logging configured per IRM 10.8.3. SWC\_C2 system is ESAT compliant.

11a. Does the Audit Trail contain the Audit Trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

---

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If Yes, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: Yes If Yes, *specify*: Large Business Taxpayers

---

### C. PURPOSE OF COLLECTION

---

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

Risk issues represent areas of potential non-compliance with the tax code. By tracking these issues, the IRS will be in a better position to offer taxpayer assistance to correct or eliminate areas of non-compliance.

---

### D. PII USAGE

---

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration Yes

To provide Taxpayer Services Yes

To collect Demographic Data Yes

For employee purposes Yes

*If other, what is the use?*

Other: No

---

**E. INFORMATION DISSEMINATION**

---

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

\*\* Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	_____

*If other, specify:*

---

**F. INDIVIDUAL CONSENT**

---

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? No

18a. If Yes, how is their permission granted?

---

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent	_____
Website Opt In or Out option	_____
Published System of Records Notice in the Federal Register	_____
Other:	_____

---

**G. INFORMATION PROTECTIONS**

---

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

---

**21. Identify the owner and operator of the system:** IRS Owned and Operated

**21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?**

---

**22. The following people have use of the system with the level of access specified:**

	<b>Yes/No</b>	<b>Access Level</b>
IRS Employees:	<u>Yes</u>	
Users		<u>Read Only</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

**If you answered yes to contractors, please answer 22a.** (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

---

**22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation?**

**23. How is access to the PII determined and by whom?**

Access is granted through the On-Line 5081 by the Manager, and the SWC\_C2 system administrator.

---

**24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?**

SWC\_C2 relies on authoritative data sources such as BMF.

---

**25. 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

---

**25a. 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.**

The Selection and Workload Classification Component 2 (SWC C2) is non-recordkeeping. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. SWC C2 provides a Business Rules Engine that identifies potential high risk tax returns for further review and possible examination. Data used for executing business rules is pulled from LB&I's Data Capture System. All records housed in that system will be erased or purged from the system in accordance with approved retention periods. SWC C2 only retains the most recent data necessary to identify current potential areas of risk. The SWC C2 database is overwritten with each subsequent data load on a quarterly basis.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

---

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

SWC\_C2 uses COE EFS and transmittal to encrypt and transfer taxpayer files and database.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

SWC\_C2 does not allow transmission of data outside of IRS firewall. Data only resides on a secure server.

---

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

---

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

Access to SWC-C2 is limited to less than 15 IRS employees. Access is granted through an approved OL5081.

---

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

---

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)? Yes

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted? 03/22/2011

---

#### H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

---

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

---

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number

SORNS Name

Treas/IRS 42.001 Examination Administrative files

Treas/IRS 34.037 IRS Audit Trail and Security Records System

Treas/IRS 42.021 Compliance Programs and Project Files

Comments

**I. ANALYSIS**

---

*Authority: OMB M 03-22 & PVR #21- Privacy Risk Management*

---

**32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?**

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

**32a. If Yes to any of the above, please describe:**

n/a

[View other PIAs on IRS.gov](#)