

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: February 11, 2015

PIA ID Number: **858**

---

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

---

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

Advanced Research Lab, ARL

---

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: Under 5,000

Members of the Public: Not Applicable

---

## 4. Responsible Parties:

---

N/A

---

## 5. General Business Purpose of System

---

The purpose of the Intelligent Business Solutions Advanced Research Lab (IBS ARL) baseline environment is to provide a means to test analytic tools that can be used to support various types of research, econometric modeling, forecasting, and compliance studies based on the analysis of Internal Revenue Service (IRS) data. The hardware and software will exist in a highly secure and controlled network environment that is being configured to support the test and exploration of these analytic tools. Due process for use of results 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: 8/10/2009 12:00:00 AM

---

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 No
- 

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

No changes, PIA needs to be renewed

---

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'. NA

---

## 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 No

Other No

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

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)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	No	No
Date of Birth	Yes	No	No

**Additional Types of PII:** No

No Other PII Records found.

10a. What is the business purpose for collecting and using the SSN ?

SSN are used to match with other sources of data in identifying individuals and exploring areas of noncompliance and abusive tax avoidance schemes.

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.)

The IRS Restructuring and Reform Act

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

there is no alternative, SSNs are critical in identifying and investigating individuals' tax obligations and mitigating noncompliance.

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

n/a

Describe the PII available in the system referred to in question 10 above.

Taxpayer information collected from IRTF and BRTF is used for various analytics in identifying noncompliance or abusive tax avoidance schemes. Data sources from the Exchange of Information (OECD) and State Department (Passport and Embassy) are matched with IRS data to determine tax

compliance and avoidance.

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.

For each auditable event the audit trails capture, at minimum, the following information: Date and time that the event occurred; The unique identifier (e.g., user name, Standard employee identifier (SEID), application name, etc) of the user or application initiating the event; Type of event (including all identification and authentication attempts (successful and unsuccessful) and commands directly initiated by the user); and Subject of the event (e.g., the user, file, or other resource affected); the action taken on that subject; and the outcome status (success or failure) of the event.

- 11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

- 
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:

**System Name** **Current PIA?** **PIA Approval Date** **SA & A?** **Authorization Date**

CDW                      Yes                      12/14/2012                      Yes                      01/24/2012

- b. Other federal agency or agencies: Yes

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

State Department

- c. State and local agency or agencies: No

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

- d. Third party sources: Yes

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

SEC Edgar Database Exchange of Information Data from OECD Passport and Embassy data from State Department

- e. Taxpayers (such as the 1040): Yes

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

- g. Other: No If **Yes**, specify:

---

### 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.

The purpose of the Intelligent Business Solutions Advanced Research Lab (IBS ARL) baseline environment is to provide a means to test analytic tools that can be used to support various types of research, econometric modeling, forecasting, and compliance studies based on the analysis of Internal Revenue Service (IRS) data. PII data is used to investigate and identify areas of noncompliance or tax avoidance. Individuals' data is used to match up with other data sources to obtain a complete picture of taxpayer profile and whether tax obligations have been met. Current projects work with auditors from the Offshore Compliance Unit, TEGE and LB&I.

---

### 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	<u>Yes</u>
To provide taxpayer services	<u>Yes</u>
To collect demographic data	<u>Yes</u>



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 Write</u>
Developers		<u>Read Write</u>
Contractors:	<u>Yes</u>	
Contractor Users		<u>Read Only</u>
Contractor System Administrators		<u>Read Write</u>
Contractor Developers		<u>Read Write</u>
Other:	<u>No</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? Yes

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

Users must be given approval by their management as well as RAS management to obtain access. An ONLINE 5081 request must also be submitted to register all users to the ARL

---

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

The quality of the data relies on the business unit (or other data source) that presents it to IBS ARL for analytic modeling. Publicly available data is beyond the control of the system. The data itself is not important for the function of IBS ARL as it only uses the data to test tools and reporting (trending and analytics) formats for the business units.

---

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? No

---

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.

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.

Advanced Research Lab is unclassified. System owners will work with the IRS Records Office to further assess recordkeeping potential and draft a request for records disposition authority for submission to the National Archives and Records Administration (NARA), if deemed necessary. Copies of data used in the testing environment (but maintained elsewhere for official recordkeeping purposes) will be deleted by a Guttman algorithm when no longer needed in preparation for the next testing session.

---

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

The ARL is a secure environment with all IT and FISMA requirements in place.

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

Data resides on servers under IT control.

---

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.

The servers undergo regular patching and security controls by CSIRC.

---

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

---

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

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

---

## 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**

IRS 42.021 Compliance Programs and Project Files

Treas/IRS 34.037 Audit Trail and Security Records System

## 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) No

Provided viable alternatives to the use of PII within the system No

New privacy measures have been considered/implemented No

Other: No

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

'NA'