

---

**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: 12/18/2013

PIA ID Number: **508**

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):

Abusive Transactions Support Unit DataBase, ATSU-DB

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: Under 100,000

---

**4. Responsible Parties:**

---

System Owner		Subject Matter Expert (SME) Contact	
Name	XXX	Name	XXXX
Title	XXX	Title	XXXX
Business Unit	Small Business Service	Business Unit	Small Business Service
Phone Number	XXXX	Phone Number	XXXX
E-mail Address	XXXXXX	Email Address	XXXXXX
System Designated Approval Authority (DAA)/Authorizing Official (AO)			
Name	XXX	Phone Number	XXXX
Title	XXXX	E-mail Address	XXXX
Business Unit	Not Applicable		

---

**5. General Business Purpose of System**

---

The Abusive Transactions Support Unit database is used for reference purposes and to establish patterns in behavior when information is needed to establish reason for the examination, case support, actions taken on the case, (sometimes for more than one reason for the same taxpayer and year) assistance to CI, DOJ, subsequent claims concerning application of certain abusive transaction penalties and closed case reviews for ATTI analysts.

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) No

6a. If **Yes**, please indicate the date the latest PIA was approved:

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)
- System is undergoing Security Assessment and Authorization

---

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

---

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?

If no PII is present, the pages between this page and the signature page will have <b>BLANK</b> answers.
--

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 Yes

*Other Source:*  
 Administrative information  
 such as dates of actions and  
 contacts

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	Yes	No
Date of Birth	No	No	No

**Additional Types of PII:** Yes

**PII Name On Public? On Employee?**

DBA Name Yes No  
 Website URL Yes No  
 DBA Address Yes No

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

The Name, address, TIN, business name, DBA, EIN, and business address. Also, the name of the Technical Advisor associated with the investigation.

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.)

SBSE Delegation Order 4.60

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

None. We need the SSN identifier to compare with data from ERCS and IDRS.

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

NA

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.

No audit trails. The system is only used by the ATSU group.

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:

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): 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 ATSU Project database supports two primary functions; Inventory Control and Transmittal.

---

### 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 No

To collect demographic data No

For employee purposes Yes

Other: No

*If other, what is the use?*

---

**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? Not Applicable

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 Write</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Write</u>
Developers		<u>Read Write</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?

SBSE LDC Program Manager

---

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

PII is bulk loaded from Spreadsheet files. There are no crosschecks other than visual verification by the database users.

---

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.

We are presently discussing retention needs with RMO, Tracee Taylor, and have submitted a draft records destruction plan for data no longer needed.

---

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

Database currently resides at the following: \\ODN0010CPOSC3\SQL2005 server\sql instance. MITS ASA AD is James J. Johnson, TIER 2 WINTEL specialists. The following individual currently administers tasks related to the ATSU\_ProjectDB: Mindy Keller. The administrator will have the following permissions: dbread,dbwrite, dbowner.

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

The data is on a SQL server with a MS Access user front end for data input and reports. User access and interactions with is limited to the MS Access form and report objects. Those objects allow for following access to the ATSU\_ProjectDB: dbread, dbwrite. The ATSU group within the SBSE LDC program are the only users of the database.

---

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? No

---

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

LDC program manager approves all access. Only ATSU employees and the above system administrative staff currently have access to the live database.

---

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**

Treas/IRS 42.021 Special Projects and Program Files

Treas/IRS 34.037 IRS ausidt trail and security records system

**Comments**

