Date of Approval: December 23, 2016 PIA ID Number: **2067**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Abusive Transactions Support Unit DataBase, ATSU-DB

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.

Abusive Transactions Support Unit DataBase, 508,

Next, enter the **date** of the most recent PIA. 11/8/2013

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**
Yes	**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 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 Criminal Investigation (CI), Department Of Justice (DOJ), subsequent claims concerning application of certain abusive transaction penalties and closed case reviews for Abusive Transaction Technical Issues (ATTI) analysts. This database has been identified as a process to be worked with the Enterprise Case Management system.

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 No On Spouse Yes On Dependent

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

Yes	**Social Security Number (SSN)**
Yes	**Employer Identification Number (EIN)**
Yes	**Individual Taxpayer Identification Number (ITIN)**
No	**Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)**
Yes	**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).

The system requires the use of full SSN and mitigation strategy is currently not required. No alternative exists currently for the application. This program is aware of and part of the IRS-wide SSN elimination and reduction program.

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.

Selected	PII Element	On Primary	On Spouse	On Dependent
No	**Name**	**No**	**No**	**No**
Yes	**Mailing address**	**No**	**No**	**No**
Yes	**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**
Yes	**Internet Protocol Address (IP Address)**	**No**	**No**	**No**
Yes	**Criminal History**	**No**	**No**	**No**
No	**Medical Information**	**No**	**No**	**No**
Yes	**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**
Yes	**Financial Account Numbers**	**No**	**No**	**No**
No	**Photographic Identifiers**	**No**	**No**	**No**
No	**Biometric Identifiers**	**No**	**No**	**No**
Yes	**Employment (HR) Information**	**No**	**No**	**No**
Yes	**Tax Account Information**	**Yes**	**Yes**	**Yes**

6c. 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
No	**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.**
No	**Proprietary data**	**Business information that does not belong to the IRS**
No	**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**
Yes	**Criminal Investigation Information**	**Information concerning IRS criminal investigations or the agents conducting the investigations.**

6d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. IRS files and databases, ACIS

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.

The ATSU Project database supports two primary functions: Inventory Control and Transmittal. The employee information (SEID, and Employment Information) is required to maintain an accurate account of work assignments. The Taxpayer (client), Promoter, and Tax Preparer information is stored for case support purposes. That information includes identification numbers (SSN, EIN, ITIN, and PTIN), contact information (mailing address, and phone numbers), Taxpayer return data (Financial Account Numbers, and Tax Account Information), Promoter/Preparer business information (IP Addresses, E-mail addresses, and Certificate or License numbers), and the Criminal History of the individuals associated with the particular case.

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

All data will be reviewed by site owners and management of the site owner. Any changes will be approved by management prior to making any changes in the system. Investigative purposes require that these data elements be collected to support the investigation regardless of whether or not another source exists.

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	**Special Projects and Program Files**
34.037	**IRS Audit Trail and Security Records System**

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. ## Official Use Only

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.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
ACIS	**Yes**	**08/21/2012**	**No**	

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

Form Number	Form Name
1040	**Individual Federal Income tax Form**

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? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
Preliminary investigations is done to see if the preparer/promoter is doing what the referral says he/she is doing. Tax returns are pulled and cursory reviews are performed to see if there are issues with the returns prepared. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Publication 1 "Your Rights as a Taxpayer" explains the rights of the taxpayer, which includes the right to challenge the IRS' position and be heard; and the right to appeal an IRS decision in an independent forum.

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-Only**
Sys. Administrators	**Yes**	**Read and Write**
Developers	**Yes**	**Read And Write**

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? SBSE LDC Program Manager

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 ? Yes

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? No

22b. 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.

The FTC Consumer Sentinel Db is an outside Agency utility. The IRS does not use it for recordkeeping. We will only collect any relevant data related to the identification of a promoter or facilitator of an abusive tax transaction. We will not separately maintain any information related to these type of leads, except for the secure email that is used to transmit the lead to the civil or criminal Lead Development Center. The secure emails will be maintained in accordance with records retention policies of IRM 1.15.6.

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? 12/20/2005

23.1 Describe in detail the system s audit trail. Site owner and manager are in charge of who has access to the database. These two individuals approve all persons with access and when they will lose access. System administrators maintain all data in folders that have specific rights granted to each user. Logs are created to track the files viewed by each user. These logs can be used to audit the data accessed by a given user as well as provide chain of custody documentation for the resource. Audit events captured by the system audit logs: Logon and logoff Password changes data object access such as open and closed. Reading, editing and deletion of object files. Date and time of event. The unique identifier (user name, SEID, application name, etc.) of the user or application initiating the event.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. The system has been in place for many years. Therefore, no test plan is needed.

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: Not Applicable
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? Yes

If **yes** , does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact *Disclosure* to determine if an accounting is required. Yes

End of Report