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: May 31, 2013 PIA ID Number: **411**

1. What type of system is this? New

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

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

SB/SEAbusive Transactions and Technical Issues Eme, ATTIEI

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:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	Under 100,000

4. Responsible Parties: N/A

5. General Business Purpose of System

The SB/SE, Examination, Abusive Transactions and Technical Issues (ATTI), Emerging IssuesTeam would like access to the Federal Trade Commission's Consumer Sentinel Database which compiles information from consumer complaints and makes this information available to authorized government law enforcement agencies. Two ATTI personnel who are on the ATTI Emerging Issues team will review this database to identify potential new, emerging abusive tax transactions. If the ATTI personnel identify such transactions, they will collect all relevant related information from the FTC Consumer Sentinel database. This information will primarily focus of the nature of the transaction but may include information on individuals involved in promoting or facilitating these tax-related scams. Although unlikely, it is possible that they may collect PII about 10 or more individuals who are promoting or facilitating such transactions. The 2 ATTI EI team personnel will send civil abusive tax transaction leads to the ATTI Lead Development Center by secure email. These personnel will retain the emails but will not otherwise retain any information obtain from the FTC database. Rather, we are using this database as another source of leads, especially in the area of tax-related identity theft scams. The ATTI Lead Development Center (LDC) will process these leads using its pre-existing process for accepting and review leads from all internal and external stakeholders. The LDC database is accessible in its "live" state by 4 LDC personnel. Other employee cannot access the database but receive information through weekly screen shots of the information. If the information relates to criminal tax scams, the EI personnel will send the information (by secure email) to the IRS Criminal Investigation Lead Development Center. Again, ATTI EI is not creating any database of the information uncovered but, instead, will route any leads to the appropriate civil or criminal IRS unit and will retain only the secure emails that are used to route the leads.

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

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

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	No	
Employees/Personnel/HR Systems	No	
Other	Yes	*Other Source:* Federal Trade Commissioner Consumer Sentinel Database

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	No	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

PII Name	On Public?	On Employee?
	No	No

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

If a SSN is available for an individual who is the subject of a consumer complaint involving an abusive tax transaction, we would use this information to determine whether there is already a promoter or preparer investigation or examination pending and to identify any other pertinent information about the scam or scheme with which the individual is associated (i.e. related entities).

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.)

I DO NOT KNOW. (NEED ASSISTANCE ON THIS.)

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

No alternate solutions.

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

As the SSN is the Taxpayer Identification Number, we will continue to use the SSN to identify whether any individual identified as promoting or facilitating abusive tax transactions is under investigation or examination and whether there are related taxpayers associated with the individual. I do not foresee a way to eliminate the use of the SSN if we obtain such information from the FTC database.

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

We have not been able to access the FTC Consumer Sentinel Database. We understand it is a compilation of consumer complaint accessible only to law enforcement. We presume that the database will contain whatever information the complainants were able to provide. So, we assume that in some cases, names and addresses will be available and in other cases, TINs. We will use whatever is relevant and available to determine the nature of the abusive tax transactions and, if a promoter investigation is authorized, whatever information we can obtain about the promoter.

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.

Two ATTI EI employees will log onto their computers as normally required by the IRS and subject to whatever audit trails exist for this process. The FTC and IRS Cybersecurity will require these 2 employees to have a special piece of hardware that will be associated with each of their individual computers to allow them to access the FTC database. (As mentioned previously, this database is only accessible by authorized law enforcement.) If there is any information in this FTC Consumer Sentinel database that relates to a new type of abusive tax transaction or potentially an individual who is promoting or facilitating such an abusive transaction, we will collect whatever information is available. Some will not be PII (e.g. how the transaction works), but some may be PII (e.g. the name and address and if available, TIN of an individual promoting the abusive transaction.) We will collect any relevant data. We will not separately maintain any information related to the leads except for the secure email that is used to transmit the lead to the ATTI Lead Development Center. The secure emails will be maintained in accordance with pre-existing records retention policies.

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: No

b. Other federal agency or agencies: Yes

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

Federal Trade Commission's Consumer Sentinel database that is a compilation of consumer complaints that is accessible to authorized law enforcement agencies only.

c. State and local agency or agencies: No

d. Third party sources: Yes

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

The Consumer Sentinel database is a compilation of consumer complaints. Accordingly, the source of the information in the database are consumers who have complained.

e. Taxpayers (such as the 1040): No

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

g. Other: No

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 Abusive Transactions and Technical Issues unit within SB/SE Exam is responsible for identifying and supporting IRS efforts to investigation and enjoin promoters of abusive transactions and to examine individual taxpayers who participate in these abusive transactions. As part of these efforts, ATTI has an Emerging Issues team. This team is tasked with finding ways to identify new abusive transactions before they are widely promoted to the detriment of both the Government and individual taxpayers. The FTC database contains valulable information about consumer complaints. We expect that there may be information about scams that involve tax issues, especially identity theft-related tax scams. We will review the FTC database. If we see new, abusive tax-related transactions, we will provide these leads to the appropriate IRS lead development center.

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	No	
		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

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

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

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

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20b. If **No**, how was consent granted?

Written consent	No
Website Opt In or Out option	No
Published System of Records Notice in the Federal Register	No
Other:	No

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

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

	Yes/No	**Access Level**
IRS Employees:	Yes	
Users		No Access
Managers		Read Only
System Administrators		No Access
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

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

There really is no "system" to "access." Two ATTI employees will have access to the Federal Trade Commission's system. (But I assume that is the subject of the FTC's PIA.) These 2 employees will note any information relevant to new abusive tax transactions and send, using secure email, the information to the ATTI Lead Development Center and if applicable to the IRS Criminal Investigation lead development center. The ATTI employees will not otherwise retain the information--except in retaining the email in accordance with existing records retention policies. The only people with "access" to this information are the people who process civil and criminal tax leads through existing processes for the IRS. In sum, 2 ATTI personnel will have access to the FTC database. Then, as applicable, personnel from the LDC or CI lead development center will have access in accordance with their duties to develop these leads. If the lead results in an authorized investigation, then this information will be shared with the civil or criminal agent handling the case. Presumably, his or her manager might view the information specific to the case, as well.

---

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

We are not using the information as anything but the beginning of a lead for civil or criminal tax investigations. It will be verified (or not) through other research that is performed by the LDC or criminal tax personnel as the research and develop potential cases. If a case is authorized, the revenue agent or special agent will further investigate and verify or correct information.

---

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.

ATTIEI is non-recordkeeping. It is not an official repository for any data or documents, and does not require a NARA-approved records control schedule to affect data disposition. Instead, ATTIEI refers to the access and collection of abusive tax scheme information from the Federal Trade Commission's Consumer Sentinel Database. This data is used to facilitate the research and pursuit of tax-related criminal investigations. Any information shared with CI and used pursuant to an investigation will be maintained in accordance with existing procedures for retaining investigation case files.

---

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

As noted previously, if we obtain any PII (we may not), it will be typed into a secure email. That secure email will be sent to the ATTI lead development center using its existing processes to handle civil tax leads from internal and external stakeholders. Our only "new system" is for 2 ATTI people to periodically review the FTC Consumer Sentinel database. If they see any new, abusive tax transactions, they will forward the description of the new scheme to the ATTI lead development center. (This would not be PII.) If there happens to be information about the individual who is promoting or facilitating the scheme, they would send any relevant information (which is PII) to the Lead Development Center. That is the full scope of our "system." So, the information is secured on the front end by the FTC and its limited access. As noted previously, our 2 employees will be required to have a special hardware token that is associated with only their computers that will allow them access to this database. We will place any relevant information into a secure email that is sent to the ATTI LDC. The email is then stored on the employees computer. There is no separate database for our proposed actions. (As noted previously, the LDC has a database and an established process for accepting both internal and external leads. As this is not a new process nor anything that we are developing, we do not further address this.) As we will only retain emails, this information will be protected by the employee's computer password and encryption.

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

There is no system, except: (1) the FTC system (I presume they have data protection controls); (2) the IRS computers. The "data" collected will reside in the 2 emloyees email. So, that information will be subject to the "normal" encryption and password protection to which IRS computers are subject. This information will be sent using secure messaging from the ATTI IRS employees to other ATTI employees at the LDC and at times IRS employees in the CI lead development center.

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.

The employees will always have to use to the hardware token to access the FTC database and will always use secure messaging to send any information to the IRS civil and criminal lead development centers.

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)*? Yes

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted? 08/08/2012

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.

Treas/IRS 42.021 Project and Program files

Treas/IRS 34.037 IRS 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