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: March 13, 2015 PIA ID Number: **675**

1. What type of system is this? Legacy

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

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

Expatriate Database, EXPAT BD

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 Expatriate Database (Expat DB) provides a repository for information associated with U.S. citizens or permanent long-term residents abandoning their U.S. citizenship or terminating their long-term U.S. residency status. The database includes taxpayer information received from the Department of State (for individuals abandoning their U.S. citizenship), the Department of Homeland Security (for individuals terminating their long-term resident status), the expatriates themselves (via Form 8854, Initial and Annual Expatriation Information Statement), and the corresponding research results from IDRS and AIMS. The Expat DB provides compliance tracking information and workload identification information. The filing information is used to comply with the quarterly Federal Register reporting requirements per IRC 6039G(d). 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*) 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'. N/A

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	Yes	*Other Source:* Dept. of State and Dept. of Homeland Security

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	Yes	Yes	No

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Expatriation Information from DOS/DHS	Yes	No
Tax Return Tax Liability for 5 Tax Years	Yes	No

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

Identification and matching of information from Dept. of State or Dept. of Homeland Security with the Form 8854 information from the taxpayer.

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.)

IRC 6039G(d)

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

A "CLN Record Number" is used as an alternative identifier. The CLN is used to reference the hardcopy files.

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

None. The SSN/TINs are needed to properly identify and track the taxpayer for compliance purposes.

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

All of the following PII items are required for the business purpose of the system. The system is designed to collect, validate, and track information submitted by each source listed. Taxpayer (Tp) Name – From other federal agencies submitting expatriate information and from the taxpayer via a Form 8854. Taxpayer (Tp) SSN/TIN – From the taxpayer via a Form 8854 or from internal Master File searches based on information provided by other federal agencies. Taxpayer (Tp) Address – From the taxpayer via a Form 8854 or from internal Master File searches based on information provided by other federal agencies. Taxpayer (Tp) Date of Birth – From the taxpayer via a Form 8854 or from internal

Master File searches based on information provided by other federal agencies. Taxpayer (Tp) Tax Return Liability for 5 Tax Years – From the taxpayer via a Form 8854 or from internal Master File searches based on information provided by other federal agencies. Taxpayer (Tp) Expatriation Information – From the other federal agencies, namely Dept. of State (for former U.S. citizens) and Dept. of Homeland Security (for former U.S. lawful permanent residents)

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.

Access to the standalone program is limited to employees working on the Expatriation Program. If any other employee logs on to the standalone computer, they will not be able to see or access the Expat DB.

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:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
IDRS	Yes	08/03/2014	No	
IRP	Yes	03/12/2014	No	

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: No

e. Taxpayers (such as the 1040): Yes

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 filing information is used to comply with the quarterly Federal Register reporting requirements per IRC 6039G(d). The compliance tracking information is used to confirm if expatriates have met their expatriation tax requirements per IRC 877 or 877A. The workload identification information is used to determine which files require further follow-up to properly determine if the correct federal tax returns are being filed.

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	Yes
For employee purposes	No

		If other, what is the use?
Other:	Yes	To comply with IRC 6039G(d) - Publish Names in Federal Register

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.) Yes

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)	No		
State and local agency (-ies)	No		
Third party sources	No		
Other:	Yes	JITSIC Foreign Country Member	

** 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? N/A

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? Yes

19a. If **Yes**, how does the system ensure “due process”?

Record fields included in Expat DB to track missing Forms 8854 and any follow-up correspondence to secure missing information from the taxpayer.

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.

Form Number	**Form Name**
8854	Initial and Annual Expatriation Information Statement

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:

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

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 limited to IRS employees in the PCCS unit responsible for inputting, updating and/or maintaining the Expat DB. Access limited by system login SEID. Access determined by LIHC Dept. Manager and SME policy analyst. Requests to add/delete employees' access to Expat DB submitted via OS GetServices request.

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

PCCS unit manager overseas information received and corresponding input to Expat DB. Filer accuracy is verified by comparing F8854 information to IDRS, IRP and information from other agencies. Timeliness determined by managerial review of receipts, database input and quarterly reports to Federal Register. Completeness verified by periodic reviews of data elements by SME policy analyst, with questions and requests for corrections forwarded to the unit manager.

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 Expatriate Database is unscheduled. A request for records disposition authority for the Expatriate Database and associated records will be drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for database inputs, system data, outputs and system documentation will be published in the appropriate Records Control Schedule Document.

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.
The current Expatriate Database (Expat DB) is a standalone MS Access database housed on a standalone desktop located in the Low Income Housing Credit (LIHC) unit at the Philadelphia Campus. Access to the Expat DB is limited by desktop sign-on (SEID), with no remote access. Requests to add/delete users must be approved by the Dept. Manager and the SME policy analyst, then submitted to the local IT office. The Expat DB does not physically leave the LIHC unit. Weekly backups of the Expat DB are performed by the Dept. Manager and a copy sent secure messaging (e-mail) to the SME policy analyst.

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

The current Expatriate Database (Expat DB) is a standalone MS Access database housed on a standalone desktop located in the Low Income Housing Credit (LIHC) unit at the Philadelphia Campus. Access to the Expat DB is limited by desktop sign-on (SEID), with no remote access. Requests to add/delete users must be approved by the Dept. Manager and the SME policy analyst, then submitted to the local IT office. The Expat DB does not physically leave the LIHC unit. Weekly backups of the Expat DB are performed by the Dept. Manager and a copy sent secure messaging (e-mail) to the SME policy analyst.

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.

Access to the Expat DB is tested on a regular basis. New employees to the LIHC unit, or existing unit employees reassigned to the Expatriate Program and who are not profiled to access the Expat DB, are allowed to sign on the desktop system and try to access the Expat DB. If they have not been added to the list of SEIDs that can access the Expat DB, they cannot see or access the database. A request for local IT assistance is made whenever a user must be added or deleted from access to the Expat DB. Data integrity is checked by the unit manager and by the SME policy analyst on a periodic basis, with detailed review on a quarterly basis when the Federal Register list is due per IRC 6039G(d).

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)*? No

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

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	Compliance Programs and Project 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

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

NA