
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Foreign Investment Real Property Tax Act Database, FIRPTA DB

2. Is this a new system? Yes

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	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 purpose of this PCLIA is to cover the initial process of receiving federal, state or local data from agencies or from a third party vendor to initiate Foreign Investment in Real Property Tax Act (FIRPTA) compliance and potential campaigns. This application is for an umbrella PCLIA which will be used to cover the process of receiving and sometimes evaluating the data to determine if further investigation or action is warranted. Information sent to the IRS from all federal, state, or local agencies or from third party vendors will be reviewed by the business unit and then merged with existing IRS systems. The data may be used for campaign support and for compliance, i.e. FIRPTA income tax withholding pertaining to foreign investment in property in the United States. Foreign Investment in US Real Property is a Large Business & International (LB&I) initiative and has been an emerging tax issue due to incentives for foreign nationals to invest in real property in the United States. The disposition, including but not limited to a sale or exchange, liquidation, redemption, gift, transfer, etc., of U.S. real property interests by foreign persons is subject to the FIRPTA income tax withholding. Withholding Agents are required to withhold 15% (10% for dispositions before February 17, 2016) of the total amount realized on each disposition. Withholding agents may be held accountable if they fail to withhold and the foreign payee fails to pay the required U.S. taxes. Withholding is essential since gains realized from the sale of the property are usually shifted offshore. IRS executives support this data collection to advocate Campaign generation and champion compliance activities. The objective of this initiative: (1) Determine number and magnitude of real property purchased by foreign nationals/investors. (2) Obtain subsequent sales details of the subject property and potential withholding (W/H) obligations required by the sale. (3) Compare potential withholding obligations and match against pertinent IRS forms. The FIRPTA DB will be a separate module within Compliance Data Warehouse (CDW) and would therefore abide by the proper protocols and controls pertaining to the parent application, CDW.

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 Yes 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)
Yes	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).

CDW currently provides for masked and unmasked SSN or TINs based on business needs and required approval process to gain access to PII. The Office of Management and Budget memorandum M-07-16 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The Foreign Investment Real Property Tax Act Database (FIRPTA DB) system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
No	SEID	No	No	No
Yes	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	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
Yes	Passport Number	No	No	No

Yes	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
Yes	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
Yes	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
No	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. Transaction details including but are not limited to the following: Historical Ownership, Physical Description of Real Property, Purchaser/Seller

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.

Taxpayer SSN, TINs, property information and other PII are part of the data received from the federal, state, and local agencies to provide IRS third party data to perform research and determine if further investigation or actions are needed.

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

The sources providing SBU/PII are reliable and have been verified by the agency providing the information through completion of audits and reviews. Hence, source of information is considered accurate, timely, and complete. IRS will use the third party data provided through these referrals to perform further research and verification using IRS systems and IRS data to determine audit potential or other appropriate action. Where indicators of non-compliance exist, IRS will take the necessary enforcement actions to ensure compliance.

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.

<u>SORNS Number</u>	<u>SORNS Name</u>
treas/IRS 42.021	special programs and project files

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? 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)? Yes

If **yes**, for each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agenc Agreement (ISA) /Memorandum of Understanding (MOU).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
New York City Department of Finance	Secure Data Transfer	No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

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? No

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

The information collected is gathered from property appraiser offices in separate counties in various states. This information is not reported to the IRS directly since the counties manage and record the transfer of real estate within their boundaries. This information can be available to public users directly via the property appraiser's website or via other recordable records in the applicable county court and records websites.

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? Information is often gathered by third party sources, state, and local agencies in the course of conducting official business.

19. How does the system or business process ensure due process regarding information access, correction and redress?

This system won't allow due process because it only receives the data to move to systems that process the data. The systems that process the data will offer due process where further investigative action will be completed in order to identify and select cases that need additional research. Information will be stored in a secure location and only accessible by authorized IRS personnel for official business use.

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

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level(Read Only/Read Write/Administrator)</u>
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	Yes	Read And Write

Contractor Employees? Yes

<u>Contractor Employees?</u>	<u>Yes/No</u>	<u>Access Level</u>	<u>Background Invest. Level</u>
Contractor Users	Yes	Read and Write	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Read and Write	Moderate
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? Data access will require Online 5081 form approval from manager and system administrator.

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 ? No

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? Yes

22a. 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.

Since data will be stored in CDW, process will follow CDW data requirements per PIA #1682. CDW data is approved for destruction 10 years after end of the Processing Year or when no longer needed for operational purposes, which-ever is later (Job No. N1-058-10-007). Retention requirements for CDW inputs, outputs and system documentation are also stipulated under that NARA-approved authority. When next updated, CDW disposition instructions will be published as item 54 under Records Control Schedule 27 for Compliance Research (IRS Document 12990).

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)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Do not know

23.1 Describe in detail the system s audit trail. IRS users must have permissions before they can access the secure data transfer folders. IT will not grant permissions until the folder point of contact approves the permissions. Audit trails are on the systems where the data is subsequently transferred/worked. Per CDW, the audit trail contains the audit trail elements as required in current IRM 10.8.3, Audit Logging Security Standards.

J. PRIVACY TESTING

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

24c. If **no**, please explain why. The records will only be stored in the system. No testing is required.

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: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
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? No

End of Report
