

Date of Approval: July 1, 2015

PIA ID Number: **1193**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. International Web Applications, INTLWebApps

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.

International Web Applications, INTLWebApps

Next, enter the **date** of the most recent PIA. 8/17/2012

Indicate which of the following changes occurred to require this update (check all that apply).

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>Yes</u>	New Interagency Use
<u>No</u>	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)

<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>Yes</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.

INTLWebApps is an application that captures tax information related to foreign individuals and entities (e.g. foreign partnerships, corporations, etc.). If for example, a foreigner or foreign entity (e.g. partnership) earns income from a United States source, then there are certain withholdings that need to take place for those earnings. An example of this is a foreign corporation that earned a dividend from a stock on a United States stock exchange. Another example is a foreigner who bought and sold a building in the United States. The tax withholdings are reported on various international tax returns prepared by or for those foreigners or foreign entities and then submitted to the IRS. No tax returns are uploaded or scanned into the application. As those forms are submitted, IRS personnel manually enter tax information into INTLWebApps for the purpose of maintaining, storing, and retrieving of the respective tax information. This information can subsequently be used for analysis, or for supporting a tax audit. The type of data maintained within INTLWebApps is considered privacy related such that Personally Identifiable Information (PII) and is contained within the application. The application houses the following types of information: International returns filed by a foreign person or entity that sells U.S. Real Property Interest (USRPI) in the United States (who invests in a domestic partnership in the United States). Income derives from a United States source for foreigners or foreign entities. Tax withholdings for foreigners and foreign entities earning income in the United States. An alien claiming exemption from withholding of income tax on independent or dependent personal service income because of a tax treaty. There are no external interfaces and only IRS personnel have access to this application. INTLWebApps is an application residing on an Oracle Database containing Oracle forms and reports. There are four modules/subsystems which facilitate the capturing of this data: Project 1446 Foreign Investment Real Property Tax Act (FIRPTA) Form 8233.

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 variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

<u>Yes</u>	Social Security Number (SSN)
<u>Yes</u>	Employer Identification Number (EIN)
<u>Yes</u>	Individual Taxpayer Identification Number (ITIN)
<u>No</u>	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
<u>Yes</u>	Preparer Taxpayer Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or variations of SSN s).

There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system. There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) No

6c. Does this system contain SBU information that it uses, collects, receives, displays, stores, maintains, or disseminates? No

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>Yes</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The INTLWebApps (FIRPTA, Project 1446, 8233) database is designed to collect relevant data to the processing of Forms 8288, 8288-A, 8288-B, 8233, 8804, 8805. and 8813. This data is used in corresponding with taxpayers, researching for up-front credit verification, and transmitting data records via Electronic File Transfer Utility (EFTU) to the Compliance Data Warehouse (CDW), the office of Statistics of Income (SOI), and the Enterprise Computing Center in Martinsburg (ECC-MTB) for upload to the Information Returns Master File (IRMF).

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 INTLWebApps (FIRPTA, Project 1446, 8233) database is designed to collect relevant data to the processing of Forms 8288, 8288-A, 8288-B, 8233, 8804, 8805. and 8813. This data is used in corresponding with taxpayers, researching for up-front credit verification, and transmitting data records via Electronic File Transfer Utility (EFTU) to the Compliance Data Warehouse (CDW), the office of Statistics of Income (SOI), and the Enterprise Computing Center in Martinsburg (ECC-MTB) for upload to the Information Returns Master File (IRMF).

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

Treasury/IRS 34.037 IRS Audit Trail and Security Records System

Treasury/IRS 42.001 Exam Administrative Files

Treasury/IRS 42.017 International Enforcement Program Information File

Treasury/IRS 42.021 Compliance Returns 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. N/A

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? 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?
The system uses data entered from tax returns filed by taxpayers. They are notified of such collection by the Privacy Act Notice in the tax return instructions.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? Yes

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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 and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Read-Only
Developers	No	

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Employees request access to the application by submitting an OL5081 which must be approved by their 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? 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.

International Web Applications (INTLWebApps - previously International National Standard Application, INTL NSA) system data is approved for deletion/destruction 7

years after end of processing year. The National Archives and Records Administration (NARA) approved these disposition instructions under Job No. N1-58-11-19 (approved 6/18/2012). These instructions are published under Records Control Schedule (RCS) 18 for the Enterprise Computing Center - Detroit (ECC-DET), Item 72. Approved retention periods for audit data, as well as other related tax withholding data are also approved/defined under Job No. N1-58-11-19. Audit trail archival logs for data are retained for 7 years after the end of the processing year. FIRPTA: Forms 8288/8288-A, Destroy paper and electronically-submitted files 7 years after the end of the processing year. Form 8288-B, Destroy paper and electronically-submitted files 6 years after the case is closed. See IRM 1.15.29, RCS 29 for Tax Administration - Wage and Investment Records, Items 75 and 223. Project 1446: All taxpayer electronic file data is destroyed when it has reached the 6th year after the end of the processing year as required by RCS 29. The records are extrapolated and then erased/deleted from the UNIX box. The data cannot be recovered. Refer to RCS 29, Item 56 (Job No. N1-58-95-1).

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? 6/17/2012

23.1 Describe in detail the system s audit trail. The INTL Webapps application (Project 1446, FIRPTA & Form 8233) relies upon the underlying Solaris 10 operating system (IT-24), Oracle database (IT-24) to fulfill many of the IRS audit requirements. Audit trails shall maintain a record of system activity both by system and application processes and by user activity of systems and applications. Determining what, when, and by whom specific actions were taken on an application system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations. This application audit plan will primarily focus its attention on application-specific audit requirements not fulfilled by the underlying operating systems, specifically taxpayer-related events and required data elements for those events. The application currently is not capturing any application-specific events. Since the application processes taxpayer data, all actions taken on that data (read & modify are the only application actions) must be recorded to the application audit trails log that will be sent to SAAS as a centralized repository. Infrastructure audit trails (comprised of operating system and Oracle database events) for INTL Webapps are collected and stored on the IT-24 (Unix Consolidated Platform). Specifically, application end user actions that trigger events on the Oracle database are syslogs captured and stored in *.xml files in /opt/app/oracle/audit/INTLWebapps. These events would be administrator and DBA actions pertaining to INTL Webapps. Audit events as a result of accessing the taxpayer data are not being captured, created, and sent to SAAS.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process**, describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

The application complies with the requirements of IRM 10.8.1.3 in regards to developer security testing; Annual Security Controls Assessment (ASCA) or Continuous Monitoring (CM) is

performed annually to determine if selected System Security Plan (SSP) controls are operating as intended. The Security Assessment and Authorization (SA&A) process is conducted on a three year cycle whereby all application information and control descriptions are updated and tested to ensure that the controls continue to work properly in safeguarding the PII. Findings from the SA&A are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? The results are stored in DocIT and transmittal checklist is provided.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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:	<u>Under 50,000</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>Not Applicable</u>
26d. Other:	<u>No</u>

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
