Date of Approval: May 16, 2018 PIA ID Number: **3456**

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, PCIA 1193

Next, enter the **date** of the most recent PIA. 7/1/2015

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
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
Yes	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.

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. INTLWebApps consists of two National Standard Application (NSA) application systems that process data for the International Program. These are Foreign Investment Real Property Tax Act Database (FIRPTA DB) and Project 1446 (PROJ 1446). This application was previously named International National Standard Application Database (INTLNSA).

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 No 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 Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The INTLWebApps system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer for intergovernmental communications. There is no known mitigation strategy planned to eliminate the use of SSNs for the system. The SSN is required for the use of this system. The SSN number is needed to research and locate records in response to the request.

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
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	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
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
Yes	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
No	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
Yes	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
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? No

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 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 another location 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
IRS 34.037	Audit Trail and Security Records System
IRS 42.001	Exam Administrative Files
IRS 42.017	International Enforcement Program Information Files
IRS 42.021	Compliance 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? Yes

If **yes**, enter the files and databases.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Compliance Data Warehouse (CDW)	Yes	03/18/2016	Yes	11/12/2015
Information Returns Master File (Parent IRP)	Yes	03/19/2017	Yes	10/22/2015

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 agencies? 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
8233	Exemption from Withholding
8288	U.S. Withholding Tax Return for Disposition by Foreign Persons of U.S. Real Property Interests
8288 - B	Statement of Withholding on Dispositions by Foreign Persons of U.S. Real Property Interests
8288 - A	Statement of Withholding on Dispositions by Foreign Persons of U.S. Real Property Interests
8804	Annual Return for Partnership Withholding Tax
8805	Foreign Partner's Information Statement of Section 1446 Withholding Tax
8813	Partnership Withholding Tax Payment Voucher

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, 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 affective 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 affective 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

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
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? 1. A potential user will request access via the [Online] OL5081 system. This request has to be approved by the potential user's manager based on a user's position and need-to-know.

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). Documents stored in this Site Collection and these sites and sub-sites are the official records and therefore these sites and sub-sites are considered an official recordkeeping system. The Site Owner will ensure that Site documents are appropriately destroyed/deleted when no longer needed for reference. Official recordkeeping copies of International Web Applications records are maintained in accordance with Records Control Schedule (RCS) 18, item 72, RCS 29, item 56, 72, and 223 published in 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)? Yes

23a. If **yes**, what date was it completed? 4/5/2018

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. INTLWebApps is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

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 regard 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)? Findings from the SA&A are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings.

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: Under 50,000
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