

Date of Approval: **September 17, 2021**

PIA ID Number: **6109**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

International Web Applications, INTLWebApps

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

International Web Applications, INTLWebApps

What is the approval date of the most recent PCLIA?

5/16/2018

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Wage and Investment Risk Committee, W&I RC

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e., system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

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.

International Web Applications (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).

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

When there is no reasonable alternative means for meeting business requirements

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

There is no planned mitigation strategy to mitigate or eliminate the use of social security numbers on the system. There is no alternative to the use of the SSN. There is significance in the use of the SSN in the system. The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use Social Security Numbers (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.

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.

Employer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing address
Phone Numbers
E-mail Address
Date of Birth
Place of Birth
Standard Employee Identifier (SEID)
Passport Number
Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Are there other types of SBU/PII used in the system?

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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 (Foreign Investment in Real Property Tax Act (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 for upload to the Information Returns Master File (IRMF).

How is the SBU/PII verified for accuracy, timeliness, and completion?

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). SBU/PII data is not verified at this point of

the process. Data is transcribed into the INTLWebApps system and transferred through EFTU to IRMF. The SBU/PII is verified by IRP (Information Returns Processing) Pre-posting. This is an entirely separate system.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

IRS 42.001 Examination Administrative Files

IRS 42.017 International Enforcement Program Information Files

IRS 42.021 Compliance Programs and Projects Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Compliance Data Warehouse (CDW)
Current PCLIA: Yes
Approval Date: 9/16/2020
SA&A: Yes
ATO/IATO Date: 11/1/2018

System Name: Information Returns Master File (Parent IRP)
Current PCLIA: Yes
Approval Date: 3/10/2020
SA&A: Yes
ATO/IATO Date: 11/1/2018

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 8233
Form Name: Exemption from Withholding

Form Number: 8288
Form Name: U.S. Withholding Tax Return for Disposition by Foreign Persons of U.S. Real Property Interests

Form Number: 8288 - B
Form Name: Statement of Withholding on Dispositions by Foreign Persons of U.S. Real Property Interests

Form Number: 8288 - A
Form Name: Statement of Withholding on Dispositions by Foreign Persons of U.S. Real Property Interests

Form Number: 8804
Form Name: Annual Return for Partnership Withholding Tax

Form Number: 8805
Form Name: Foreign Partner's Information Statement of Section 1446 Withholding Tax

Form Number: 8813
Form Name: Partnership Withholding Tax Payment Voucher

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Information Returns Processing (IRP)
Current PCLIA: Yes
Approval Date: 3/16/2020
SA&A: Yes
ATO/IATO Date: 10/22/2015

System Name: Statistics of Income Distributed Processing System (SOIDPS)
Current PCLIA: Yes
Approval Date: 7/2/2019
SA&A: Yes
ATO/IATO Date: 3/1/2019

System Name: Security Audit and Analysis System (SAAS)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 4/29/2020

Identify the authority.

Authority and purpose is pursuant to section 6103(h)(1) of the Internal Revenue Code (IRC). IRC 6103(h)(1) provides for disclosure of returns and return information to officers and employees of the Department of the Treasury (including IRS) whose official duties require access for tax administration.

For what purpose?

Tax administration

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

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

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.

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.

INFORMATION PROTECTION

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

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Read Write

Developers: Read Only

How is access to SBU/PII determined and by whom?

A potential user will request access via the Business Entitlement Access Request System (BEARS). This request has to be approved by the potential user's manager based on a user's position and need-to-know.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

In-process

When is the anticipated date of the SA&A or ACS completion?

6/18/2021

Describe the system's audit trail.

The INTLWebApps 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 primarily focuses 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. 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 (Security Audit and Analysis System) as a centralized repository. Infrastructure audit trails (comprised of operating system and Oracle database events) for INTLWebApps 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. These events would be administrator and Database Administrator (DBA) actions pertaining to INTLWebApps. Database 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.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

A process is in place to test, develop, and document all proposed changes. This includes using a formal test plan to document testing process, its scope, expected results, final results and summary. Developers test and create evaluation plans, and use test data to ensure that changes to the application work properly without introducing new problems

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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