Date of Approval: **February 28, 2022**

PIA ID Number: **6709**

SYSTEM DESCRIPTION

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

International Data Exchange Service, IDES

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 Data Exchange Service, IDES PIA #3918

What is the approval date of the most recent PCLIA?

2/18/2019

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.

AD International Information Processing and Exchange (IIPE)

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.

IDES will provide secure and reliable transport of the Foreign Account Tax Compliance Act (FATCA) Foreign Financial Institution (FFI) account reports and US Bank Deposit and Interest (BDI) between foreign countries and the United States. IDES will manage the exchange of encrypted files between correspondents and pass encrypted electronic files to International Compliance Management Model (ICMM). ICMM will also prepare outgoing data files for exchange via IDES.

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:*
>
> Interfaces with external entities that require the SSN
>
> Legal/statutory basis (e.g., where collection is expressly required by statute)
>
> 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 alternative to the use of the SSN. The SSN is the significant part of the data being processed. IDES 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.

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. IDES requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Other Taxpayer 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
Date of Birth
Place of Birth
Financial Account Numbers
Tax Account Information

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

No

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.

In order to improve international tax compliance and as required by FATCA, the third-party reporting data transmitted through IDES will be compared with information provided by taxpayers on their returns. This includes the SSN, name, mailing address, date of birth, place of birth, financial account numbers and tax account information of Americans living abroad.

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

IDES is a pass-through system used to transmit encrypted data from foreign sources through ICMM-International Data Transfer (ICMM-IDT) to ICMM-FATCA International Return (ICMM-FIR). Encryption validation checks are complete upon upload to IDES. If encryption is not validated, the upload is immediately rejected. Additional validation checks are completed by ICMM-IDT (also a pass-through) and ICMM completes additional checks for timeliness and accuracy of data once decrypted.

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 24.030   Customer Account Data Engine Individual Master File

IRS 24.046   Customer Account Data Engine Business Master File

IRS 42.021   Compliance Programs and Projects Files

IRS 42.017   International Enforcement Program Information Files

IRS 34.037   Audit Trail and Security Records

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: International Compliance Management Model (ICMM)
Current PCLIA: Yes
Approval Date: 10/27/2020
SA&A: Yes
ATO/IATO Date: 8/12/2020

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?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: ICMM-IDT (IEP)
Transmission Method: Encrypted File via IEP from ICMM-FIR protected by TLS v 1.2
ISA/MOU: Yes

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: Form 8966
Form Name: FATCA Report

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: ICMM
Current PCLIA: Yes
Approval Date: 10/27/2020
SA&A: Yes
ATO/IATO Date: 8/12/2020

Identify the authority.

Reciprocal reporting by the US to Model 1A foreign countries on assets and accounts held by foreign nationals in US financial institutions.

For what purpose?

Reciprocal reporting by the US to Model 1A foreign countries on assets and accounts held by foreign nationals in US financial institutions.

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?

Yes

Identify the other source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Host Country Tax Authority with Intergovernmental Agreement
Transmission Method: Encrypted File
ISA/MOU: No

Organization Name: ICMM-IDT (IEP)
Transmission Method: SDT
ISA/MOU: Yes

Identify the authority.

Reciprocal reporting by the US to Model 1A foreign countries on assets and accounts held by foreign nationals in US financial institutions.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

Reciprocal reporting by the US to Model 1A foreign countries on assets and accounts held by foreign nationals in US financial institutions.

For what purpose?

Reciprocal reporting by the US to Model 1A foreign countries on assets and accounts held by foreign nationals in US financial institutions.

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?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

11/13/2017

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

3rd Party

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Yes

When was the e-RA completed?

7/13/2021

What was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity
Confidence based on Single Factor Identity Validation

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?

Notice is provided by Internal Revenue Service in the instructions to the form: "We ask for the information on this form to carry out the Internal Revenue laws of the United States. Chapter 4 of the Code requires certain withholding agents and foreign financial institutions to report information with respect to certain U.S. accounts, substantial U.S. owners of passive non-financial foreign entity (NFFEs), U.S. accounts held by owner documented FFIs, and certain other accounts as applicable based on the filer's chapter 4 status. Form 8966 is used to comply with this reporting requirement."

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

No

Why not?

In order to improve International Tax Compliance, IDES will ensure the safe, secure delivery of third-party reporting data required under FATCA. This data will be compared to information provided by taxpayers on their returns and enable better case selection for international compliance operations.

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

IDES delivers third party report data on FATCA to the IRS. That data will be used by LB&I compliance in a manner similar to other sources of third-party reporting data, taxpayers may avail themselves to their normal due process rights in their dealings with LB&I compliance.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and operated; IRS owned, contractor operated; contractor owned and operated).

Contractor 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

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Read Write

Contractor Developers: Read Only

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

IDES is a managed service that delivers third party reporting data. The host does not have the ability to open the encrypted data files while in transit. All the host will see is their packet of information is being sent to the IRS from the sending party. The data file is not decrypted until it has physically arrived at the designated landing platform. IRS Users will have write access to upload a file and read access to Sentinel to review reports. Also, access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user to be added. They must submit the request via the Online 5081 process to request access to the System.

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?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

SA&A OR ASCA

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

Yes

What date was it completed?

3/2/2021

Describe the system's audit trail.

IDES is a managed services project, and the system audit trail has been put in place by the vendor. The vendor will meet the requirements of IRM 10.8.3 and IRM 10.8.1. as indicated in the draft audit plan. Deficiencies in the audit solution are being assessed. The following minimum events are captured with additional information contained in the audit plan a. Any attempt to Logon; b. Logon ID (authorization and identification); c. Date and time of each logon/logoff attempt; d. Devices used to logon/logoff; e. Function(s) performed once logged on; and f. Network performance (Moderate and High impact only).

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)?

Test results are stored in TFIMS (Treasury FISMA Inventory Management System).

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?

Annual Security Control Assessment (ASCA).

SBU DATA USE

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

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

9/23/2021

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: 100,000 to 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?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Not Applicable