Date of Approval: February 19, 2019 PIA ID Number: **3918**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. International Data Exchange Service, IDES

2. Is this a new system? No

2.a. If no, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If yes, enter the full name, acronym, and milestone of the most recent PCLIA.

International Data Exchange Service, IDES PIA #1663

Enter the approval date of the most recent PCLIA. 03/09/2016

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

No Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
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
No Internal Flow or Collection
Yes Expiring PCLIA

Were there other system changes not listed above? No

3. What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym. AD International Information Processing and Exchange (IIPE)

3.a. Check the current Enterprise Life Cycle (ELC) 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.
IDES will provide secure and reliable transport of the 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.

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

6.a. 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 all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
Yes	Interfaces with external entities that require the SSN
Yes	Legal/statutory basis (e.g. where collection is expressly required by statute)
Yes	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed.

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 memorandum M-17-12 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.

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

If yes, specify the information.

Selected	PII Element
Yes	Name
Yes	Mailing address
No	Phone Numbers
No	E-mail Address
Yes	Date of Birth
Yes	Place of Birth
No	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
Yes	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

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

6.e. 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

6.f. 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.

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 of Americans living abroad.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

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.

C. 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.

9. 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

If yes, enter the SORN number(s) and the complete the name of the SORN(s).

SORNS Number	SORNS Name
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 System

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

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

11.a. If yes, does the system receive SBU/PII from IRS files and databases? Yes

If yes, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
International Compliance Management Model (ICMM)	Yes	12/18/2017	Yes	11/28/2017

11.b. Does the system receive SBU/PII from other federal agency or agencies? No

11.c. Does the system receive SBU/PII from State or local agencies? No

11.d. Does the system receive SBU/PII from other sources? Yes

If 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	Transmission method	ISA/MOU
ICMM-IDT (IEP)	Encrypted File via IEP from ICMM-FIR protected by TLS v 1.2	Yes

11.e. Does the system receive SBU/PII from Taxpayer forms? Yes

If yes, identify the forms.

Form Number	Form Name
Form 8966	FATCA Report

11.f. Does the system receive SBU/PII from Employee forms (such as the I-9)? No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If yes, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
ICMM	Yes	12/18/2017	Yes	11/28/2017

Identify the authority. Reciprocal reporting by the US to Model 1A foreign countries (Host Country Tax Authorities) 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 (Host Country Tax Authorities) on assets and accounts held by foreign nationals in US financial institutions.

12.b. Does this system disseminate SBU/PII to other Federal agencies? No

12.c. Does this system disseminate SBU/PII to State and local agencies? No

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12.e. Does this system disseminate SBU/PII to other Sources? Yes
If 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	Transmission method	ISA/MOU
Host Country Tax Authority with Intergovernmental Agreement	Encrypted File	No
ICMM-IDT (IEP)	SDT	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.

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, Radio Frequency Identification (RFID), etc.? No

15. Does the system use cloud computing? Yes

15.a. If yes, Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified? Yes

If yes, Date Certified. 05/09/2016

15.b. Please identify the ownership of CSP data. IRS

15.c. Does the CSP allow auditing? Yes

Who audits the CSP data? 3rd Party

15.d. Please select background check level required for CSP. Moderate

15.e. Is there a breach/incident plan on file? Yes

15.f. Privacy laws (including access and ownership) can differ in other countries. If any data is considered SBU, will this cloud be Continental US (CONUS) only for:

Storage	Yes
Transmission	Yes
Maintenance (including backups)	Yes
Troubleshooting	Yes

16. Does this system/application interact with the public? Yes

16.a. If yes, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

16.a.1. If yes, when was the e-RA conducted? 07/25/2018

If yes, what was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity.

If Level 2, Confidence based on:

Single Factor Identity Validation

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? Yes

17.a. 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?
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."

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18.b. If individuals do not have the opportunity to give consent, 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.

19. 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, tax payers may avail themselves to their normal due process rights in their dealings with LB&I compliance.

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) Contractor 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 and Write
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	Yes	Read-Only	Moderate
Contractor Sys. Admin.	Yes	Read and Write	High
Contractor Developers	Yes	Read-Only	Moderate

21.a. 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.

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? No

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? In-process

23.b. If in process, when is the anticipated date of the SA&A or ASCA completion? 03/05/2019

23.1 Describe in detail 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).

J. PRIVACY TESTING

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

24.a. If yes, was the test plan completed? Yes

24.a.1. If yes, where are 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).

24.a.2. If yes, were all the Privacy Requirements successfully tested? Yes

24.a.3. If yes, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? Annual Security Control Assessment (ASCA).

K. SBU Data Use

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

25a. If yes, was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If yes, provide the date the permission was granted. 09/27/2018

25.b. If yes, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

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

26.a. IRS Employees:	Not Applicable
26.b. Contractors:	Not Applicable
26.c. Members of the Public:	100,000 to 1,000,000
26.d. 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 Recommendations of the 9/11 Commission 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

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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