Date of Approval: March 9, 2015   PIA ID Number: **1663**

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

    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 Data Exchange Service, IDES, Milestone 3/4a PIA 1442

        Next, enter the **date** of the most recent PIA.   8/4/2015

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

        Were there other system changes not listed above?   Yes

        If yes, explain what changes were made.   Enable reciprocal reporting by the US to Model 1A foreign countries on assets and accounts held by foreign nationals in US financial institutions, update users to include Contractor help desk support

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
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	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 FATCA 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

    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	No	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)
No	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).

    At this time there is no mitigation strategy because SSNs are required by the Internal Revenue Code, but we are aware of IRS mitigation strategies.

    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
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
No	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
No	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
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that is not PII, 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)

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.

   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? 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

   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

---

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
Treas/IRS 24.30	IMF
Treas/IRS 24.046	BMF
Treas/IRS 42.021	Special Projects and Program Files
Treas/IRS 42.017	International Enforcement Program Information File
Treas/IRS 34.037	Audit Trail and Security Records System

   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?   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
ICMM	Yes	10/07/2015	Yes	01/06/2015

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 agency (-ies)?   No

11d. 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

11e. Does the system receive SBU/PII from **Taxpayer** forms?   No

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?   Yes

12a. 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 PIA?	PIA Approval Date	SA & A?	Authorization Date
ICMM	Yes	10/07/2015	Yes	01/06/2015

Identify the authority and 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

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

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

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

12e. 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 and 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, cloud, global position system (GPS), biometrics, RFID, etc.?   No

15. Does the system use cloud computing?   Yes

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

    16a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application?   No

        If **no**, when will the e-RA be conducted?   1/2/2017

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?
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 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

    18b. If 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.

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.
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

21a. 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 physcially arrived at the designated landing platform. IRS Users will have write access to upload a file and read access to Sentinel to review reports

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 ? Not Applicable

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

22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

The International Data Exchange Service (IDES) is non-recordkeeping for IRS purposes. It is a platform for secure communications and information sharing between Foreign Financial Institutions (FFIs) and Host Country Tax Administrations (HCTAs), for which the IRS is but one example. IDES is not the official IRS repository for any data or documents. The records/data transferred via IDES to IRS will be downloaded to LB&I's International Compliance Management Model (ICMM) and managed/maintained in accordance with ICMM data disposition instructions. ICMM is currently unscheduled. A request for records disposition authority for ICMM and associated records will be drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. LB&I has proposed a 10-year retention for ICMM recordkeeping data. When approved by the National Archives and Records Administration (NARA), disposition instructions for ICMM inputs, system data, outputs, and system documentation will be published in Document 12990 under Records Control Schedule 26 for Tax Administration - International, item number to be determined. Guidance for the capture and retention of audit-related records is found in IRM 10.8.3 Audit Logging Security Standards, section 10.8.3.2.2.

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?   4/16/2015

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

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?
ASCA

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?   Test results are stored in an approved IRS repository

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? Yes

If **yes**, please describe the outstanding issues. Several (25) security risks were identified in the Annual Security Control Assessment and mitigation activities are in process. Risks include lack of vulnerability assessments, lack of finalized audit plan, configuration weaknesses, lack of background investigations, authentication failures, no checks for unauthorized software as well as other weaknesses.

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.   2/1/2016

25b. **If yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?   Yes

L. NUMBER AND CATEGORY OF PII RECORDS

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

    26a. IRS Employees: Not Applicable
    26b. Contractors: Not Applicable
    26c. Members of the Public: 100,000 to 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

    If **yes**, provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable).

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

    If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

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