

---

**A. SYSTEM DESCRIPTION**

---

1. Enter the full name and acronym for the system, project, application and/or database. International Compliance Management Model Federal, ICMM-FIR

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 Compliance Management Model, 1790, M4B

Next, enter the **date** of the most recent PIA. 08/31/2016

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

<u>Yes</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>Yes</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	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)

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>Yes</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>No</u>	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.

The ICMM system will receive and manage information on foreign accounts held by US citizens. This information will be provided by US taxpayers, Foreign Financial Institutions (FFI) and the Host Country Tax Authorities (HCTA), as called for in the Foreign Account Tax Compliance Act (FATCA). Currently, individual taxpayers are directed to file Form 8938 with their individual tax return (Form 1040 and 1040-NR). Effective for Filing Season 2017/Tax Year 2016 was the Form 8938 to be attached to business entities tax returns, Forms 1120, 1120-S, 1065, and 1041. Specifically, ICMM will provide functionality in several key areas to support FATCA implementation: 1. Receive, process and store electronically submitted FFI account reports utilizing the Form 8966. The data is submitted in the Extensible Markup Language (XML) format utilizing the FATCA Intergovernmental Schema. The FATCA Intergovernmental XML schema is a standard format that the Internal Revenue Service (IRS) will use for automatic exchange of FATCA data with Intergovernmental Agreement (IGA) jurisdictions. 2. Support full data capture of any FFI account reports submitted using Form 8966 in paper format. Incoming data that originated as paper forms are input. Paper forms are transmitted to the IRS Integrated Submission and Remittance Processing facilities, where they are transcribed into an unstructured file format for communication to ICMM-FIR. The transcribed data is transmitted to ICMM-FIR by secure channels to protect sensitive information. Upon arrival at ICMM-FIR, the data is extracted and validated.

---

## 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            Yes    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)  
Yes    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).

None. Social Security Numbers (SSNs) are part of the data transmitted under Internal Revenue Code (IRC), Title 26, Section 6038D.

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.

<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>	<u>Selected</u>	<u>PII Element</u>
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	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
Yes	Mother's Maiden Name	No	No	No
Yes	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
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

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
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.
Yes	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.

SSNs are the primary key used by auditors and analysts to tie together tax forms relating to a tax case. The replacement of this identifier with a masked identification would not be feasible. SSNs are permissible from IRC 6109, "Identifying Numbers" which requires individual taxpayers to include their SSNs on their income tax returns.

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

Data received electronically and via Forms 8966, 8938, and 1042-S will be validated in applicable Generalized Mainframe Framework and Information Returns Processing pipeline processes. Data received on new Form 8966 will be validated on receipt against the FATCA Intergovernmental Schema, an XML schema. The current FATCA XML Schema is v2.0.

---

## **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 numbers and the complete the name of the SORN.

<u>SORNS Number</u>	<u>SORNS Name</u>
IRS 42.017	International Enforcement Program Information Files
IRS 42.021	Compliance Programs and Project Files
IRS 34.037	Audit Trail and Security Records System
IRS 22.026	Form 1042 Index by Name of Recipient

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.

<u>System Name</u>	<u>Current PCLIA</u>	<u>Approval Date</u>	<u>SA&amp;A?</u>	<u>Authorization Date</u>
Integrated Submissions and Remittance Processing	Yes	01/25/2017	Yes	01/27/2016
Modernized e-file R10	Yes	02/23/2016	Yes	11/09/2015
International Data Exchange Service (IDES)	Yes	03/09/2016	Yes	04/16/2015
IRS Integrated Exchange Portal (IEP)	Yes	12/15/2015	Yes	02/12/2014

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? 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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
FFI and HCTA	Transcribed through ISRP	No
United States Withholding Agents	Encrypted Data Package through IEP	Yes
FFI and HCTA	Encrypted Data Package through IEP	Yes
Territory Financial Institution	Encrypted Data Package through IEP	Yes

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

If **yes**, identify the forms

<u>Form Number</u>	<u>Form Name</u>
1042-S	Foreign Person's U.S. Source Income Subject to Withholding
8938	Statement of Specified Foreign Financial Assets
8966	Foreign Account Tax Compliance Act Report
8957	Foreign Account Registration Form (FATCA)

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.

<u>System Name</u>	<u>Current PCLIA</u>	<u>Approval Date</u>	<u>SA&amp;A?</u>	<u>Authorization Date</u>
IDES	Yes	03/09/2016	Yes	04/16/2015
IRS IEP	Yes	12/15/2015	Yes	02/12/2014

Identify the authority and for what purpose? The US will share bank deposit and interest data of foreign account holders from certain countries on a reciprocating basis with certain foreign tax administrations under agreements intended to boost FATCA acceptance and implementation. Sharing terms will be governed by Competent Authority Agreements with foreign governments involved.

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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
HCTAs per IGAs with US	<b>Encrypted through IEP to IDES</b>	<b>No</b>

Identify the authority and for what purpose? Reciprocal reporting by the US, per the Treasury Intergovernmental FATCA agreement, 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, 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?

FATCA legislation was passed in March 2010 to expand the IRS visibility into overseas activities of US taxpayers for tax compliance purposes by 1) requiring US taxpayers to declare foreign financial accounts and assets to the IRS, and 2) enabling the IRS to enter into agreements with foreign banks and other financial institutions for reporting and withholding on certain US assets and accounts. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

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):

Per FATCA legislation passed in March 2010. In order to improve international tax compliance, ICMM will ensure the safe, secure delivery, and storage 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. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC.

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

The data will be used by Large Business and International (LB&I) Division compliance to enhance/expand compliance enforcement on US taxpayers who have investments located outside the United States. This data will also be used to enhance/expand compliance enforcement on non-resident aliens who have business activities in the US. Taxpayers have the right to raise objections and provide additional documentation in response to formal IRS actions or proposed actions, to expect that the IRS will consider their timely objections and documentation promptly and fairly, and to receive a response if the IRS does not agree with their position. Notice, consent and due process are provided in the tax forms instructions, and pursuant to 5 USC. Enrolled Practitioner Program System assistants will be providing support to FFIs and HCTA that contact the IRS regarding error notifications they have received as a result of the processing of their submitted files by ICMM.

---

**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

<u>IRS Employees?</u>	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Read-Only
Developers	Yes	Read-Only

Contractor Employees? Yes

<u>Contractor Employees?</u>	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	High
Contractor Managers	Yes	Read-Only	High
Contractor Sys. Admin.	No		
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? Access to the system is role based. Data access is determined by the manager based upon a user's position and need-to-know. The manager will request a user be added. They must fill out Form 5081, Information System User Registration/Change Request, to request access to application. A user's access to the data is terminated when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information System Security Rules on Form 5081. All users access must be approved by LB&I Data Solutions.

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? 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.

ICMM is scheduled. A request for records disposition authority for ICMM and associated records (including Forms 8966 and 8938, and 1042-S, regardless of format) was approved (Disposition Authority-0058-2016-0005). A 10-year retention for ICMM recordkeeping data was included in the schedule. As approved by the National Archives and Records



Administration, 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 51 at next publication update.

---

## 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? 04/20/2017

23.1 Describe in detail the system's audit trail. The ICMM audit plan has been routed for signature. Appendix I of the audit plan provides details of the system's audit trail. The ICMM-FIR audit extract for Security Audit and Analysis System (SAAS) will be stored in an Access Control List protected directory that is only accessible to the ICMM-FIR application and the Enterprise File Transfer Utility (EFTU) utility. EFTU will copy the ICMM-FIR audit extract to the SAAS folder for processing and then move the extract file into the archive folder. The audit log directory is listed as a critical element in Appendix G as part of the Operating System ICMM-FIR Component table. Refer to the Oracle, JavaBeans Open Sources Software Operations Network and Linux audit plans for protection of infrastructure audit logs.

---

## 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 Privacy Controls are tested as part of the Annual Security Controls Assessment for FATCA.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Document Management for IT Projects (DocIT). You can find more about this application at [http://docit.web.irs.gov/docit\\_help/login.htm](http://docit.web.irs.gov/docit_help/login.htm).

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? 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. 09/11/2015

25b. 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:

- 26a. IRS Employees: Not Applicable  
26b. Contractors: Not Applicable  
26c. Members of the Public: More than 1,000,000  
26d. Other: Yes

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).

FFI more than 100,000 and HCTA under 500.

---

**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**

---