

Date of Approval: July 28, 2015

PIA ID Number: **1402**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. FATCA Foreign Financial Institution Registration S, FATCA FFI Registration System

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.

FATCA Foreign Financial Institution Registration System

Next, enter the **date** of the most recent PIA. 11/19/2014

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

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

Were there other system changes not listed above? Yes

If yes, explain what changes were made. Additions to the system's audit trail.

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

Yes Preliminary Design/Milestone 3

Yes Detailed Design/Milestone 4A

Yes 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.

The Foreign Accounts Tax Compliance Act (FATCA) was passed into law in March 2010 with the objective of improving the IRS's visibility into overseas movements of income by US individual and business taxpayers. FATCA requires US withholding agents to withhold 30% on payments to Foreign Financial Institutions (FFIs) that do not abide by FATCA provisions for reporting on accounts held by US persons and entities and withholding on payments to accounts held by "recalcitrant" US persons and entities. The purpose of the FATCA Foreign Financial Institution Registration (FATCA-FFIR) system is to enable the IRS to enter into agreements with FFIs to engage in these withholding and reporting activities under the FATCA legislation. In order to comply with the timeframes set for implementation of this legislation, FATCA-FFIR system became operational August 2013. The FATCA-FFIR system registers FFIs electing to comply with US FATCA legislation (part of 2010 HIRE Act). For Foreign Financial Institutions, the system will request Financial Institution name and other information for the entity for which the application is being made and for a Responsible Officer (RO) for the applying FFI. FFI Registration must be capable of managing related FFI applications across a range of ownership structures, referred to as FFI Groups. FFI Registration System supports LB&I's primary goal to strengthen international perspectives and compliance approaches. Specifically, the FATCA-FFIR System supports the objectives to develop international compliance solutions and expand international stakeholder relationships and cooperation. FFI Registration System initiates the process of working with international institutions to ensure proper tax compliance outlined in the FATCA legislation. FFI Registration System also supports LB&I's goal to integrate end-to-end processes and systems, specifically aligning to the objective to integrate end-to-end Information Technology (IT) infrastructure to support the business process. FFI Registration is incorporating IT solutions by implementing an online portal to facilitate the registration process. FATCA-FFIR System is an application that is accessible via IRS.gov. Internal IRS users connect through the Employee User Portal (EUP). External users connect to the registration system through the Integrated Enterprise Portal (IEP), and the FFI List is accessible via the Public User Portal (PUP). To access the FATCA FFI Registration System, the Financial Institution establishes an account. Once they choose to create an account they create their own unique access code (rules apply to make it secure). The system then generates a FATCA ID that is used in combination with their access code to access their account. The FFI then completes the registration, providing Responsible officer (RO) information. Included in this RO information are the RO's name and business email address. The FFI then submits their registration. When a change in registration status occurs, an email notification is sent to the RO's business email requesting the RO to check their FATCA account for an update. FI Registration, including Branch information, is screened and if approved, FIs and Branches are assigned Global Intermediary Identification Numbers (GIINs). GIINs are published monthly on the FFI List. In Release 2.0, approved Sponsoring Entity type FIs will have the ability to add Sponsored Entities including Sponsored Subsidiary Branches. The Sponsored Entities and Sponsored Subsidiary Branches will be screened and if approved, assigned GIINs. These GIINs will be included in the FFI List. Also being added in Release 2.0 is the ability for member type FIs in approved or limited conditional status to transfer from their current expanded affiliated group (EAG) to another EAG and the ability for FIs to change their FI type.

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 variations of SSN s (i.e. last 4 digits, etc.)? No

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>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	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
No	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 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)

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>No</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The purpose of the system is to register Foreign Financial Institutions (FFIs) electing to comply with US FATCA legislation (part of 2010 HIRE Act). Information needed to identify the Responsible Officer (RO) and POC's within the Financial Institution are required. The RO delegates authorization to the Point of Contacts (POCs) including authorization for the POCs to complete Form 8957, FATCA Registration, to take other FATCA related actions, and to obtain access to the FI's tax information. The RO or authorizing official also certifies that the information submitted on the registration is accurate and complete, and agrees that the Financial Institution will comply with FATCA obligations. The PII collected for the Responsible Officer and POCs of the financial institution is used to notify the FI of account status changes as well as correspond with the FI regarding FATCA issues.

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

The Financial Institution provides the SBU/PII regarding the RO and POCs through the FATCA Registration System. To insure accuracy and completeness, the Registration System performs required field and format validation on the RO and POC information when submitted and saved. The FI cannot submit their registration form if the information submitted is not complete. The FI can edit the RO and POC information as needed due to changes or as necessary. The FI is responsible for keeping this information up to date. The FATCA Registration System does not make any determination pertaining to an individual's rights, benefits, and/or privileges.

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? No

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? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

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? No

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? Yes

If **yes**, what was the approved level of authentication?

Level 1: Little or no confidence in the asserted identity's validity.

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?

Instructions are included on screen as to what information is required. There is also a corresponding User Guide that provides detailed information. Some fields are required and some fields are optional. If the FI is not able to provide the required information, they cannot complete the registration process.

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):
If the FI is not able to provide the required information, they cannot complete the registration process. Optional fields are at the discretion of the FI.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Not applicable.

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

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? The FATCA FFI Registration entrant will only be able to access the PII data that was input by that entity. IRS will utilize OL5081 groups to determine which IRS employees need access to registration data through EUP and reports via Business Objects to perform their job duties.

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? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

NARA approved IRS's request for disposition approval for FATCA FFI Registration System recordkeeping data (Job No. DAA-0058-2013-0011, signed by the Archivist of the United States, 9/12/2013). FI registration data will be maintained for 10 years after the FI has been terminated or has withdrawn as a participating FI. All approved disposition instructions for system inputs, master file data, outputs and system documentation will be published in IRS Document 12990 under Records Control Schedule 26 for Tax Administration - International, item 50 when next updated.

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? 8/20/2014

23.1 Describe in detail the system's audit trail. The FATCA Registration system records audit events to the SAAS Audit system utilizing the SAAS Audit system AMDAS message queue. Audit events are placed on the SAAS Audit system AMDAS message queue where they are consumed by the SAAS Audit application and recorded. The SAAS Audit record for the FATCA Registration system consists of: User ID - ICCE01 or SEID; User Type - REGT or IRSEE; System - FATCA; and Event Type - FA. The following events are recorded to SAAS Auditing for successful and unsuccessful results: Create a FATCA registration user account record; Delete a FATCA registration user account record; Retrieve a FATCA

registration user account record; Create a FATCA registration user account password; Reset a FATCA registration user account password; FATCA registration user account login to the registration application; and FATCA registration user account logout from the registration application. Create a FATCA registration record; Delete a FATCA registration record; Update a FATCA registration record; Retrieve a FATCA registration record; Override a FATCA registration record; Suspend a FATCA registration record; and Terminate a FATCA registration record. Create a FATCA registration Branch record; Suspend a FATCA registration Branch record; and Terminate a FATCA registration Branch record. Cancel a FATCA registration agreement; Transfer is finalized for a FATCA registration account; Approve a Sponsored Entity record; Approve a Sponsored Subsidiary Branch record; Update a Sponsored Entity record; Reject a Sponsored Entity record; Reject a Sponsored Subsidiary Branch record; Suspend a Sponsored Entity record; Suspend a Sponsored Subsidiary Branch record; and Terminate a Sponsored Entity record

J. PRIVACY TESTING

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

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 12/16/2014

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?

Testing that is scheduled to be done for Release 2.0 includes: Unit testing – performed by the Developers on their individual workstations; Dev Testing – performed by the Developers in the DEV environment; AQT Testing – Performed by the AQT Testers in the AQT Environment; 508 Testing – Performed concurrently with AQT in the AQT environment; SAT Testing – Performed by EST in the SAT environment; UAT – performed by the customer in the SAT environment; Performance Testing – performed by Performance Testing in the PETE environment; and DSRT – Deployment Site Readiness Testing – combination of SA, DBA and Development Team testing done prior to go-live in a pre-production environment to ensure all the pieces parts are ready to go. All test results are documented and stored in the approved IRS repositories by the Development Team staff. We will NOT be using live data for any of this testing. It will be all created data only. All development staff are required to attend 6-8 hours of Security and Privacy related training classes annually in accordance with the FISMA guidelines governing their positions and length of service. Certification of completion is managed via their Organizational chain of command and completion is mandatory. All development staff must attend annual UNAX certification and other Privacy and Security related mandatory briefings.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees:	<u>Not Applicable</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>100,000 to 1,000,000</u>
26d. Other:	<u>No</u>

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
