TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

While the Financial Institution Registration System Deployed on Time, Improved Controls Are Needed

September 30, 2014

Reference Number: 2014-20-094

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
2 = Risk Circumvention of Agency Regulation or Statute

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

WHILE THE FINANCIAL INSTITUTION REGISTRATION SYSTEM DEPLOYED ON TIME, IMPROVED CONTROLS ARE NEEDED

Highlights

Final Report issued on September 30, 2014

Highlights of Reference Number: 2014-20-094 to the Internal Revenue Service Chief Technology Officer and the Commissioner, Large Business and International (LB&I) Division.

IMPACT ON TAXPAYERS

The deployment of the Financial Institution Registration System (FRS) supports provisions of the Foreign Account Tax Compliance Act (FATCA). Taxpayers meeting the reporting requirements threshold began reporting their foreign financial assets on Form 8938, *Statement of Specified Foreign Financial Assets*, beginning with the 2012 Filing Season. Foreign financial institutions are required to report to the IRS information about financial accounts that exceed certain thresholds held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest. Withholding agents will withhold a 30 percent tax on taxpayers who fail to properly report specified financial assets related to U.S. investments. Expenditures for FRS development totaled approximately $16.7 million for Fiscal Year 2011 through Fiscal Year 2013. In Fiscal Year 2014, funding available for the FATCA Program was $46.6 million.

WHY TIGTA DID THE AUDIT

Our objective was to determine whether the IRS Information Technology organization has adequately mitigated systems development risks for the FRS. TIGTA reviewed risk management processes, the FRS solution architecture, Systems Acceptability Testing results, security testing results, and access controls implemented for users of the FRS. TIGTA also assessed IRS actions taken to ensure that the FRS electronic signature process is as reliable as is appropriate for the intended purpose.

WHAT TIGTA FOUND

The IRS deployed FRS Release 1.1 in December 2013 to provide functionality to Foreign financial institutions and authorized IRS employees. Our review found that the IRS has not yet: (1) approved and implemented FRS business performance measures; (2) completely traced FRS system-specific security requirements to security controls, test cases, and test results; (3) fully evaluated the risks of using electronic signatures for registration forms; (4) fully documented FRS system access controls design, implementation, and functionality; (5) **********2********** **********2********** *****2*********; and (6) integrated an automated tool suite to enable effective requirements management.

WHAT TIGTA RECOMMENDED

The Chief Technology Officer should (1) implement business performance measures to quantify the benefits of the IRS's FRS investment; (2) completely trace FRS system-specific security requirements to controls, test cases, and test results to ensure security requirements are fully tested prior to deployment; (3) determine whether a particular technology and set of procedures for electronic signatures as selected are as reliable as is appropriate for the intended purpose; (4) document system access controls in sufficient detail to permit analysis and testing; (5)**********2********** **********2**********; and (6) apply integrated automated tools to manage FATCA systems requirements traceability. TIGTA also recommends that the Commissioner, LB&I Division, complete a risk analysis and cost-benefit analysis to assess the likelihood and cost of not implementing enforceable electronic signatures.

The IRS agreed with two recommendations but disagreed with five recommendations related to security requirements traceability, electronic signatures, security access controls, and integrating automated requirements management tools.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 30, 2014

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER
COMMISSIONER, LARGE BUSINESS AND INTERNATIONAL DIVISION

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – While the Financial Institution Registration System Deployed on Time, Improved Controls Are Needed (Audit # 201420013)

This report presents the results of our review of the Financial Institution Registration System (FRS). The overall objective of this review was to determine whether the Internal Revenue Service (IRS) Information Technology organization has adequately mitigated systems development risks for the Foreign Account Tax Compliance Act FRS. This audit is our second review of the IRS's system development activities for the FRS and is included in our Fiscal Year 2014 Annual Audit Plan. Our review addresses the major management challenges of *Implementing Major Tax Law Changes*, *Globalization*, and *Security for Taxpayer Data and Employees*.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

FATCA	Foreign Account Tax Compliance Act
FFI	Foreign Financial Institution
FI	Financial Institution
FRS	Financial Institution Registration System
FY	Fiscal Year
GIIN	Global Intermediary Identification Number
IGA	Intergovernmental Agreement
IRS	Internal Revenue Service
IT	Information Technology
LB&I	Large Business and International
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PMO	Program Management Office
ReqPro	Rational RequisitePro
RQM	Rational Quality Management
SAT	Systems Acceptability Testing
SCA	Security Controls Assessment
SP	Special Publication
TIGTA	Treasury Inspector General for Tax Administration

Background

The Foreign Account Tax Compliance Act (FATCA)[1] Program is an important development in the Internal Revenue Service's (IRS) efforts to improve U.S. tax compliance involving foreign financial assets and offshore accounts. In 2010, Congress enacted the FATCA legislation as part of the Hiring Incentives to Restore Employment Act[2] to:

- Combat tax evasion by U.S. persons holding investments in offshore accounts.
- Expand the IRS's global presence.
- Pursue international tax and financial crimes.
- Fill a gap in the IRS's information reporting system.
- Generate additional enforcement revenue.

The FATCA legislation directly affects three key groups:

- **Taxpayers.** Taxpayers meeting the reporting requirements threshold must report their foreign financial assets on Form 8938, *Statement of Specified Foreign Financial Assets*, as an attachment to their Federal income tax returns beginning with the 2012 Filing Season.[3]
- **Foreign Financial Institutions (FFI).** FFIs include any non-U.S. entity that accepts deposits, holds financial assets, or engages in the business of investing, including foreign banks, foreign branches of U.S. banks, and businesses organized under a foreign law that would be a securities broker-dealer if located in the U.S. (*e.g.*, money transmitter, currency exchanger). FFIs are required by the FATCA to report to the IRS information about financial accounts that exceed certain thresholds held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.
- **Withholding Agents.** Withholding agents will withhold a 30 percent tax on taxpayers who fail to properly report specified financial assets related to U.S. investments.

[1] Pub. L. No. 111-147, Subtitle A, 124 Stat 71, *96-116 (2010) (codified in scattered sections of 26 U.S.C.).
[2] Hiring Incentives to Restore Employment Act (HIRE), Pub. L. No. 111-147, 124 Stat. 71 (2010).
[3] See Appendix IV for a glossary of terms.

IRS Information Technology (IT) organization Program Management Office (PMO) governance

Within the IRS's IT organization, the Enterprise IT PMO is the IRS's systems integrator to manage programs based on the Enterprise Life Cycle, ensuring coordination across information technology delivery partners and business stakeholders for successful project delivery to production. The Enterprise IT PMO provides systems integration and has an emphasis on major IRS business systems modernization programs such as the Customer Account Data Engine 2, Modernized e-File, the Electronic Fraud Detection System, the Return Review Program, and the FATCA Program.

The newly established FATCA IT PMO managed the development and deployment of the FRS and will oversee future FATCA systems development efforts.

The FATCA IT PMO was established in January 2014 when the IRS approved the FATCA IT PMO's Program Management Plan. This office oversees the design, development, and deployment of information technology projects to fulfill FATCA Program requirements. In addition, the FATCA IT PMO coordinates with IRS information technology project development leads and other IRS information technology delivery partners to manage the funding for FATCA development projects. Actual expenditures on Financial Institution (FI) Registration System (FRS) development totaled approximately $16.7 million for Fiscal Year (FY) 2011 through FY 2013. According to information provided by the IRS in preparing its FY 2015 Budget Submission to Congress, FY 2014 funding available for the FATCA Program was $46.6 million.

According to the FATCA IT PMO, the IRS will deliver FATCA systems development projects over a period of at least five years, from the initial development of the FRS in Calendar Year 2011 to the planned deployment of other FATCA systems in Calendar Year 2015. The FATCA IT PMO is responsible for designing, developing, and deploying FATCA projects to meet the IRS's Large Business and International (LB&I) Division's business needs. Once these projects are fully deployed, operations and maintenance duties for the FATCA systems will transition to other operational units within the IT organization.

Figure 1 provides a timeline of key milestones for the FATCA Program.

Figure 1: FATCA Program Deployment Timeline

Key Dates	Description
January 01, 2012	The IRS began accepting Form 8938. In Calendar Years 2012 and 2013, only U.S. individual taxpayers were required to file Form 8938 and attach it to a Form 1040, *U.S. Individual Income Tax Return*, or Form 1040NR, *U.S. Nonresident Alien Income Tax Return*.
January 28, 2013	The Department of the Treasury (Treasury) and the IRS issued final regulations and addressed FATCA Intergovernmental Agreements (IGA).
August 19, 2013	The FATCA registration portal opened to the public. Paper registration Forms 8957, *Foreign Account Tax Compliance Act (FATCA) Registration*, can also be used.
January 01, 2014	Each financial institution should have finalized its registration information electronically in the FRS or by filing Form 8957 for paper registrations.
April 25, 2014	FFIs and sponsoring entities must complete registration by this date to ensure inclusion on the initial IRS FFI List.
June 02, 2014	The IRS published the initial FFI List, and monthly updates will follow. As of June 30, 2014, the LB&I Division website reports that 77,000 FFIs have registered to date (includes online and paper, with and without Global Intermediary Identification Numbers (GIIN)).
July 01, 2014	Withholding begins on U.S. payments to FFIs,[4] nonfinancial foreign entities, and direct account holders of participating FFIs using Form 1042, *Annual Withholding Tax Return for U.S. Source Income of Foreign Persons.*
January 01, 2015	FFI information reporting begins for reporting of Tax Year 2014.
March 15, 2015	FFIs and sponsoring entities in non-IGA and Model 2 IGA countries are to file the first information reports for Tax Year 2014. As of June 30, 2014, Treasury recognizes that 39 IGAs have been signed; another 62 IGAs are under negotiation. Of the total 101 IGAs, 88 are Model 1 agreements for which FFIs report to the IRS through their host country taxing authorities. The remaining 13 are Model 2 agreements for which the FFIs report directly to the IRS.
March 31, 2015	FFIs and U.S. withholding agents are to file Form 1042-S, *Foreign Person's U.S. Source Income Subject to Withholding*, regarding withholding during Calendar Year 2014. U.S. withholding agents may have a reporting obligation with respect to payments made to U.S.-owned nonfinancial foreign entities.
September 30, 2015	Model 1 IGA reporting is due for Tax Year 2014. This includes reporting by host country taxing authorities and reciprocal reporting by the U.S. via the International Data Exchange Service.
January 31, 2016	The IRS plans to implement a full FATCA compliance program.

Source: IRS LB&I Division FATCA timeline.

[4] If the FFI does not comply with the FATCA rules, beginning in 2014, "withholdable payments" payable to it for both its own account and on behalf of its customers will be subject to U.S. Federal income tax withholding. Withholdable payments include items of U.S.-source fixed or determinable, annual or periodical income, such as interest and dividends, as well as gross proceeds "from the disposition of any property of a type which can produce interest or dividends from sources within the United States."

Figure 2 shows the multiple FATCA software development projects that the IRS plans to develop and implement between 2013 and 2015.

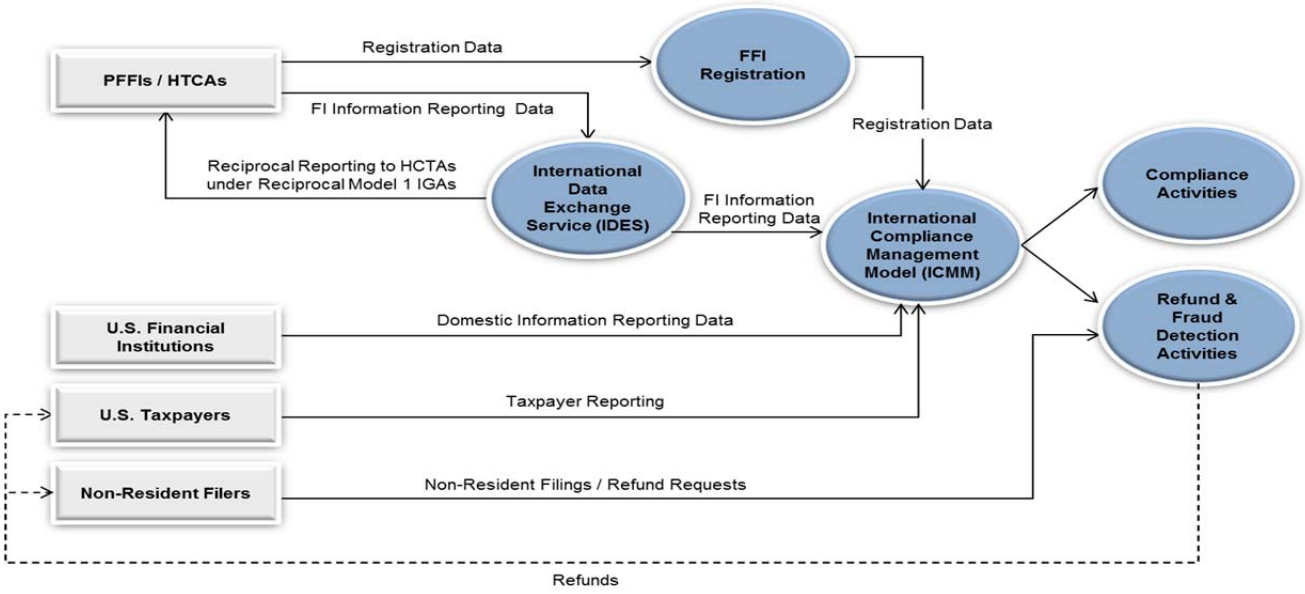
Figure 2: Key FATCA Software Development Projects

Project	Description of Related Steps and Capabilities
FRS	Register FFIs and issue a GIIN. Publish the approved IRS FFI List. Provides a search and download tool.
Taxpayer Reporting – Form 8938 Transcription	Provide taxpayers with the ability to update Form 8938 to facilitate taxpayer reporting.
International Data Exchange Service	Facilitate secure electronic submission, receipt, and exchange of FATCA data among financial institutions from many countries; service is expected to accommodate an estimated 600,000 FIs, including FFIs.
International Compliance Management Model	Develop database and extract, transform, and load FATCA data.
Withholding Payment Processing	Process and track withholding deposits and associated reporting from U.S. withholding agents and FIs.
Refund Processing & Fraud Detection	Process returns with requests for refunds against withholding deposits. Implement processes to identify and prevent potential refund fraud.
FATCA Compliance Strategy	Identify and integrate data elements for compliance case selection and case management.

Source: IRS LB&I Division.

Figure 3 depicts the relationship and data integration points between the FATCA software development projects and information provided by the FFIs, withholding agents, and U.S. account holders.

Figure 3: Relationship Among FATCA Software Development Projects



Source: IRS LB&I Division FATCA conceptual diagram. HCTA = Host Country Taxing Authority. PFFIs = Participating FFIs.

The FRS

The FRS is intended to register those FFIs electing to comply with the U.S. FATCA legislation as well as to publish and maintain a list of participating FFIs for use by U.S. holders of overseas accounts, financial institutions, and other participating FFIs in determining withholding responsibilities. Figure 4 provides an overview of FRS users and related system functionality.

Figure 4: FATCA FRS Users

FRS Users	Description
FFIs (Release 1.1 Drop 1)	FFI staff will use the FRS to create, edit, and submit applications for registered FFI status and receive notification of approval/disapproval. An FFI can create an account online, submit its FFI registration data, update its FFI account, receive notifications of events concerning registration or account actions, and read the IRS FFI List. The IRS issues GIINs to registered FFIs.
Authorized IRS Employees (Release 1.1 Drop 2)	The IRS employees supporting the FFI registration function will use the system to enter registration data, modify FFI accounts, run management reports, and extract data on FFIs for analysis.
External Third Parties (Release 2)	U.S. withholding agents and approved FFIs will need to know whether FFIs are participating in the FATCA in order to determine if 30 percent withholding should be applied to payments to FFI accounts held or controlled by U.S. persons or entities.

Source: FATCA Iterative Design Specification Report.

The FRS will provide several functions including user accounts, FFI agreements, and FFI certifications. The user account function manages user accounts. The FFI agreements function confirms input data and agreement type as entered by the FFI and ensures that the agreement is ultimately signed. The FFI certification function ensures that FFIs certify to their status as a deemed-compliant FFI by providing a withholding agent with the required documentation.

Figure 5 provides an overview of system development activities and milestones for the FRS.

Figure 5: System Development Activities and Milestones for the FRS

FRS Development Activities	Date
System development of the FRS started	April 25, 2011
FATCA regulations issued	February 8, 2012
FATCA IT PMO approved	September 13, 2012
FRS Release 1.0 terminated	November 5, 2012
FRS Release 1.1 redesigned	January 7, 2013
Final FATCA regulations issued	January 28, 2013
Scope and schedule changes to develop FRS Release 1.1 approved	January 31, 2013
FRS Release 1.1 Drop 1 deployed	July 29, 2013
FRS Release 1.1 Drop 2 deployed	December 9, 2013
FFIs needed to finalize their registrations	January 1, 2014
Form 8957 paper registrations accepted	January 1, 2014
Completed FFI registrations will be included in initial IRS FFI list	April 25, 2014
GIINs assigned to FFIs	April 25, 2014
Initial IRS FFI List was published with monthly updates planned	June 2, 2014

Source: IRS IT organization, FATCA IT PMO, FRS timeline.

FRS architecture

**********2**********

**********2**********

**********2**********

**********2**********.

The IRS terminated FATCA FRS Release 1.0 in November 2012 due to scope changes resulting from the finalization of proposed FATCA regulations and IGA negotiations. The IRS IT organization subsequently redesigned and deployed FRS Release 1.1 Drop 1 in July 2013 on behalf of FATCA's IRS business owner, the LB&I Division. Drop 1 provided functionality for FFIs to create an account via the Registered User Portal and submit a completed registration

(Form 8957). The Treasury Inspector General for Tax Administration (TIGTA) previously reported on systems development for the FRS in 2013.[5]

This review was performed at the IRS IT organization offices at the New Carrollton Federal Building in Lanham, Maryland. We obtained information from management and personnel in the FATCA IT PMO, the Cybersecurity organization, and the LB&I Division offices in Lanham, Maryland, and in Washington, D.C. The review was performed during the period October 2013 through July 2014. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[5] TIGTA conducted a prior audit of FRS Release 1.1 Drop 1. TIGTA, Ref. No. 2013-20-118, *Foreign Account Tax Compliance Act: Improvements Are Needed to Strengthen Systems Development Controls for the Financial Institution Registration System* (Sept. 2013).

Results of Review

Earlier Business Performance Measures Would Strengthen the System Development Process

While the IRS has begun developing business measures for the FRS since our last review, those measures were not yet in place to guide development for the FRS or before system deployment in December 2013. The Government Performance and Result Act Modernization Act of 2010 (GPRAMA),[6] however, emphasizes the importance of: (1) establishing annual performance goals to define the level of performance; (2) expressing goals in an objective, quantifiable, and measurable form; (3) providing a description of how the performance goals are to be achieved; and (4) establishing a balanced set of performance indicators to be used in measuring or assessing progress toward each performance goal. These same performance measurement principles are reflected in IRM 2.16.1, *Enterprise Life Cycle Guidance*, which states that the purpose of the Business Solution Architecture Stage is to specify the business system requirements and structure for a complete solution that implements the system concept and includes an initial performance engineering model, *e.g.*, measureable objectives.[7] This policy also requires that by the time an IRS system is deployed, a measurement system should be in place to support assessment of the system's functional performance to achieve its stated business needs.[8] In addition, for adequate capital planning and investment management, the IRS is required to monitor capital investments to ascertain that planned quantitative and qualitative benefits are realized.[9]

The IRS has employed an incremental delivery approach for FATCA information technology projects and divided the FRS Project into two production releases, deployed in July and December 2013 respectively. However, performance measures were not in place for TIGTA's consideration during our review of Drop 2. Further, the IRS has not yet implemented performance goals and measures for FRS Release 1.1, Drop 1. Performance measures are needed to support assessment of the system's functional performance to achieve its stated business needs.

In February 2014, LB&I Division officials informed us that they were working on five performance measures for the FATCA registration process and the associated FFI List search and download tool; two measures pertain to the LB&I Division and three pertain to the FATCA IT PMO. LB&I Division officials explained that a working group has been tasked with

[6] Pub. L. No. 111-352, 124 Stat. 3866 (Jan. 4, 2011).
[7] IRM 2.16.1.2.3.3.5, *Business Solution Architecture Stage* (Sept. 4, 2010).
[8] IRM 2.16.1.2.3.3.12, *Deployment Stage* (Aug. 3, 2008).
[9] IRM 2.16.1.2.6.8, *Strategy and Capital Planning* (Sept. 4, 2010).

fully developing these measures and ensuring that the measures are tracked once the following three FRS components became operational in June 2014, *i.e.*, registration, publication of the FFI List, and backend processing to screen applicants to determine if they are on an excluded country listing.

It has been almost a full year since the first delivery of FRS functionality, and the IRS has not yet determined expected benefits from this significant information technology investment. Further, we believe that future FATCA system development efforts would benefit from the earlier partnering of the LB&I Division with the IRS IT organization to develop and publish performance measures which will ensure that adequate governance is in place to align information technology strategy with business strategy and to measure the effectiveness and efficiency of FATCA information technology investments.

Recommendation

Recommendation 1: The Chief Technology Officer should ensure that the IRS IT organization and the LB&I Division coordinate to timely develop and implement adequate business performance measures to quantify net benefits for information technology investments in support of the FATCA.

> ***Management Response:*** The IRS agreed with this recommendation, stating that the Commissioner, LB&I Division, is responsible for the business measures for the FATCA FRS and has developed these measures. The Chief Technology Officer agreed to incorporate these measures in the IRS's FY 2016 budget submission.
>
> ***Office of Audit Comment:*** Business performance measures are important to measure and quantify the net benefits of the IRS's information technology investment in the FATCA FRS. While the IRS reported that it had developed measures for the FATCA FRS, these business measures were not made available to TIGTA for review. Although the IRS has agreed to incorporate the measures into the FY 2016 budget submission, TIGTA believes that the IRS's corrective actions should focus on implementing business performance measures and assessing the system's performance.

System-Specific Security Requirements Must Be Traced to Test Cases and Test Results to Ensure Secure Deployment

As a part of the security assessment and authorization process, the IRS Cybersecurity organization conducted a FATCA FRS event-driven Security Controls Assessment (SCA) prior to FRS Release 1.1 Drop 2 deployment to ensure that the FRS's security controls were in place and functioning as intended. The Cybersecurity organization issued its FRS Security Assessment Report on November 22, 2013. The event-driven SCA included analysis and testing of key nontechnical and technical security controls that had changed from FRS Release 1.1 Drop 1 to Release 1.1 Drop 2. The purpose of the event-driven SCA was to ensure that the

FATCA FRS met the established security controls in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (NIST SP 800-53), Revisions 3 and 4.[10] The FATCA FRS Application System Security Plan, hereafter referred to as the System Security Plan, addressed NIST SP 800-53 security controls, and the FATCA SCA traced NIST security controls to test cases and test results.

NIST SP 800-53 also provides direction for managing Federal information systems using a system development life cycle methodology that includes information security considerations. The NIST document is cross-referenced to the International Organization for Standardization's guidance on controls pertaining to information systems development and particularly security requirements analysis and specification. In addition, IRS IRM 2.127.2, *Software Testing Standards and Procedures – IT Software Testing Process and Procedures*, provides guidelines for developing system requirements and requires bidirectionally tracing those requirements to their sources and test cases, executing the test cases, recording test results, and tracing the test cases to the test results.[11] IRM 10.8.1, *Information Technology Security, Policy and Guidance*, also emphasizes integrating security into an IRS-approved systems development life cycle.[12] This policy stipulates that: (1) security requirements shall be incorporated into the system requirements and (2) security requirements shall be tracked, updated, and validated throughout a system's life cycle.

NIST SP 800-37[13] stresses that security requirements are a subset of the overall functional and nonfunctional (*e.g.*, quality, assurance) requirements levied on an information system and are incorporated into the system development life cycle simultaneously with the functional and nonfunctional requirements. This special publication recognizes that without the early integration of security requirements, significant expense may be incurred by the organization later in the life cycle to address security considerations that could have been included in the initial design. The NIST stresses that when security requirements are considered as an integral subset of other information system requirements, the resulting system has fewer weaknesses and deficiencies and, therefore, fewer vulnerabilities that can be exploited in the future. As such, these actions are needed to ensure that systems, including the FRS, adequately address unique risks and operate as intended long-term based on established system-specific security requirements.

While the IRS traced NIST security controls to test cases and test results, it did not trace FRS system-specific security requirements to security controls, test cases and test results prior to

[10] NIST, NIST SP 800-53 Rev. 3, *Information Security: Recommended Security Controls for Federal Information Systems and Organizations* (Aug. 2009). Also, NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) (includes updates as of Jan. 15, 2014).
[11] IRM 2.16.1, *Enterprise Life Cycle Guidance* (April 25, 2012).
[12] IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (May 3, 2013).
[13] NIST, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information System* (Feb. 22, 2010).

deployment. The IRS indicated that while there was no assurance that all FRS security requirements were tested as part of its security testing, 100 percent of all applicable NIST SP 800-53 security controls were tested in the SCA before the FRS Project received its final authorization to operate in November 2013. We believe that if security test case development, security control traceability, and security testing focuses only on required NIST SP 800-53 security controls, unique FRS security requirements could go untested. This could have an adverse impact on FATCA system functionality and operations. Moreover, verification of system-specific security requirements are needed to mitigate unique risks for FATCA systems regarding the threat of unauthorized access or modification of Personally Identifiable Information (PII) and other sensitive data.

Recommendation

Recommendation 2: The Chief Technology Officer should ensure that system-specific security requirements are traced to test cases and test cases to test results to ensure the completeness of FRS security testing. This will also provide assurance that adequate system-specific security will be in place throughout the life cycle of the FRS.

> ***Management Response:*** The IRS disagreed with this recommendation. The IRS stated that TIGTA did not provide any FRS-specific security test cases to the IRS as examples of this deficiency. Instead, TIGTA presented the recommendation based on a one-time initiative taken by the Customer Account Data Engine 2 project wherein every NIST security control had been traced in some manner to some type of testing and included in the security documentation. This is not a standard practice within the IRS.
>
> ***Office of Audit Comment:*** NIST guidance cites three different types of security controls, including system-specific, common, and hybrid controls. System-specific security controls are controls that are unique to the application. TIGTA is concerned that FATCA FRS's system-specific security requirements were not sufficiently traced to security controls, test cases, and test results; this key system development control is needed to ensure that FATCA system-specific security requirements are adequately tested prior to deployment. IRS policy requires all system requirements, including security requirements, to be traced to test cases and test results. The IRS needs to reassess the methodology it uses to implement this policy because its current methodology appears incomplete as the IRS only traces security controls to test cases and test results, not system-specific security requirements to controls, to test cases, and to test results. Given the lack of full traceability of security controls, the IRS cannot be assured that FATCA system-specific security requirements are fully tested prior to deployment. The IRS management response states that TIGTA did not find any specific examples of this control weakness. TIGTA notes that the scope of our system development review did not include a detailed analysis or validation of all FRS system requirements, including system-specific security requirements. We considered the risk mitigation controls

applied by the IRS to ensure adequate development and testing of FRS requirements, including requirements for security, as required by both IRS policy and by the NIST criteria that is referenced in the report.

Actions Are Needed to Evaluate Risks With Electronic Signatures for New Registration Forms

In January 2014, the IRS FATCA FRS website began allowing FFIs to file Forms 8957 electronically from anywhere in the world without the need to print, complete, and mail paper forms. As of July 17, 2014, approximately 99 percent of Forms 8957 were filed electronically. Form 8957 requires users to check an on-screen box and manually key in their name to indicate their electronic signature; the names are not verified to data on file. TIGTA asked the IRS to provide its risk analysis assessing whether the FATCA signature process is sufficiently reliable. The IRS informed us that a risk assessment for using electronic signatures in the FRS had not been completed during FRS development. During interviews with the FATCA IT PMO, Enterprise Services function, Solution Engineering function, and LB&I Division representatives, IRS officials also informed us that neither the LB&I Division nor the FATCA IT PMO have identified electronic signature requirements for the FRS.

The use of electronic signatures in transactions involving Federal agencies is primarily governed by one of the following laws: the Government Paperwork Elimination Act[14] or the Electronic Signatures in Global and National Commerce Act.[15] The Government Paperwork Elimination Act requires that, when practicable, Federal agencies use electronic forms, electronic filing, and electronic signatures to conduct official business with the public by 2003. It further encourages Federal Government use of a range of electronic signature alternatives.[16] The Electronic Signatures in Global and National Commerce Act, enacted June 30, 2000, facilitates the use of electronic records and signatures in foreign commerce. In January 2013, a report titled *Usage of Electronic Signature in the Federal Government*[17] provided important guidance on the use of electronic signatures and encouraged adherence to these laws. This guidance pertains to the use of electronic signatures for legal signing purposes in the context of electronic transactions. A signature, whether electronic or on paper, is the means by which a person indicates an intent to associate himself with a document in a manner that has legal significance. Key provisions of the January 2013 guidance follows.

[14] Pub. L. 105–277 Title XVII.
[15] Pub. L. 106–229, 114 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch. 96.
[16] OMB Circular A-130, *Management of Federal Information Resources*, Appendix II, *Implementation of the Government Paperwork Elimination Act* (Nov. 2000).
[17] Uniform Electronic Transactions Act, approved by the National Conference of Commissioners on Uniform State Laws on July 23, 1999, adopted by 47 states as of November 2010.

Electronic Signature Guidance to Federal Agencies:

1. ***Determine whether an electronic signature is necessary***. The organization should determine whether an electronic signature is required or recommended for legally binding an individual to the transaction. It is up to the organization to determine the value of any particular transaction and what level of security is required to reduce the risk of fraud.

2. ***Consider the signing requirements for legally enforceable electronic signatures***. It is critical that the electronic signature and the associated signing process satisfy all of the applicable legal requirements (form of signature, intent to sign, signature must be attached to or associated with the electronic record, identify and authenticate the signer, and integrity of the signed record).

3. ***Conduct risk analysis to assess the likelihood and cost of not implementing enforceable electronic signatures***. A risk analysis should be conducted to consider the potential challenges to the enforceability of an electronic signature. The risk analysis should include the likelihood of a successful challenge to the validity of the electronic signature and the monetary loss or other adverse impact that will result from a successful challenge to the enforceability of the electronic signature. The risk analysis should address concerns regarding the enforceability of the resulting signature. Specifically, the risk analysis should consider the:

    - Risk that an alleged signer, or other interested third party, will be able to successfully repudiate the electronic signature, deny that it was made with an intent to sign, or challenge the integrity of the signed record.

    - Loss, cost, or other impact of such a successful challenge to the enforceability of the signed record.

    The risk analysis should reach an overall risk-level determination and be documented. The risk-level determination should be used to determine the options available for each of the five signature requirements in item 2 above (form of signature, intent to sign, signature must be attached to or associated with the electronic record, identify and authenticate the signer, and integrity of the signed record).

4. ***Decide overall risk-level determination of risk***. An overall risk determination of low, moderate, or high needs to be decided for the intended purpose of the transactions.

5. ***Act on the risk assessment results***. The risk-level determination should be used to determine the options available for each of the five signature requirements discussed in item 2 above. For example, for low- and moderate-risk transactions, any electronic form of signature is acceptable (clicking an on-screen button, checking an on-screen box, typing one's name, or using a personal identification number). However, for high-risk transactions, the only acceptable electronic form of signature is a cryptographically based digital signature.

According to an IRS announcement in January 2013, "The IRS has never established a formal set of e-signature [electronic signature] standards for the tax industry."[18] Further, the IRS IT organization has not developed or implemented an enterprise electronic signature solution or a standardized web-based security solution to identify and authenticate individuals signing tax forms or registration forms.

IRM 2.16.1 provides for a complete set of business system requirements to include information system requirements including functional, data, interface, information system, performance, and operational requirements including information system management and procedural requirements.[19] However, the requirements management steps completed for the FRS did not address functionality for electronic signatures. These electronic signatures are applied to Forms 8957 that are implemented with the FRS electronic registration process. Without a risk-based approach to developing and implementing electronic signatures for the FRS, the IRS has not yet fully considered and addressed the possibility that FRS users, including FFIs, could:

- Repudiate the electronic signature, *i.e.*, deny checking an on-screen box or signing the registration form;
- Deny any intent to sign; or
- Challenge the integrity of the record or signature.

Further, if the IRS cannot enforce the electronic signatures implemented with the FRS, the risk of monetary loss or other adverse effects could hinder goals for international tax administration as needed to implement the FATCA.

Recommendations

Recommendation 3: The Chief Technology Officer should ensure that the FATCA IT PMO determines whether the particular technology and set of procedures that comprise the signing process are as reliable as is appropriate for the intended purpose.

> ***Management Response:*** The IRS disagreed with this recommendation, stating that no business requirements existed to provide an e-Signature capability for the FATCA FRS. The Chief Technology Officer delivered the system per business requirements. TIGTA was provided with the legal analysis undertaken by the Associate Chief Counsel, International, on whether an electronic signature was needed.
>
> ***Office of Audit Comment:*** A documented risk-based analysis is important in considering the adequacy of an electronic signature solution for the FRS. The risk

[18] IRS, Internal Revenue Bulletin No. 2013-4, Announcement 2013-8, *Recommendations for Proposed e-signature Standards* (Jan. 22, 2013).
[19] IRM 2.16.1.2.3.3.5, *Business Solution Architecture Stage* (Sept. 4, 2010).

analysis should consider the likelihood of a successful challenge to the validity of the electronic signature and the monetary loss or other adverse impact from a successful challenge to the enforceability of the electronic signature. Although the IRS has implemented a "check in the box" signature solution for the FRS, the IRS could not provide any evidence that it had evaluated the risks associated with its decisions prior to implementing an electronic signature solution. Therefore, TIGTA cannot determine whether the particular technology and set of procedures that comprise the signing process are as reliable as appropriate for the intended purpose. The Chief Technology Officer should monitor the LB&I Division's completion of the corrective action for Recommendation 4 below. If the LB&I Division determines that the electronic signature technology and accompanying procedures that comprise the signing process are required, then the IRS should revisit the applicability of Recommendation 3 to implement an electronic signature capability for the FATCA FRS.

Recommendation 4: The Commissioner, LB&I Division, should ensure that the LB&I Division completes a thorough risk analysis and cost-benefit analysis to better assess the likelihood and cost of not implementing enforceable electronic signatures for the FRS.

Management Response: The IRS agreed with this recommendation, stating that the LB&I Division has provided TIGTA with a report that outlined the decision on Part Four of the FATCA FRS regarding the signature. In addition, the LB&I Division is completing a risk assessment to document the decision.

Office of Audit Comment: While the IRS agreed to complete a risk assessment, its statement that the risk assessment will be performed to document the decision is problematic. The decision should be based on the outcome of the risk assessment, not vice versa.

Improvements in System Access Controls Are Needed to Ensure Confidentiality and Data Integrity

During our review, we found that key security documents did not adequately describe how access controls were designed and implemented for the FRS. Further,********2********** **********2**********. The following criteria apply to FRS access controls, including authentication and authorization of system users:

- NIST SP 800-53 requires that the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
- NIST SP 800-53 requires that the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

- IRM 10.8.1 requires the developer of the information system to provide:[20]
  - A description of the functional properties of the security controls to be employed. Functional properties of security controls describe the functionality, *i.e.*, the security capabilities, functions, or mechanisms visible at the control interfaces.
  - Design and implementation information for the security controls to be employed in sufficient detail to permit analysis and testing of the controls, to include security-relevant external system interfaces, high-level design, low-level design, source code, and hardware schematics.

Our analysis of FRS authentication and authorization controls for external and internal FRS users is presented in Figure 7.

Figure 7: Analysis of FRS Authentication and Authorization Controls

Access Controls	Design & Implementation
	Authentication & Authorization
External FRS Users	**********2**********2**********2**********2**********The system was developed where: • **********2**********2**********2**********2**********. • **********2**********. • External users can select their role from four predefined application roles. ***2**** **********2**********. • Neither the System Security Plan, the Business Systems Requirements Report, nor the Design Specification Report included sufficient documentation to describe fully the access controls design, implementation, and functionality. Because of the lack of sufficient documentation, we were unable to fully evaluate access controls for external users.
Internal FRS Users	**********2**********2**********, where: • **********2**********. • Neither the System Security Plan, the Business Systems Requirements Report, nor the Design Specification Report included sufficient documentation to fully describe the access controls design, implementation, and functionality. Because of the lack of sufficient documentation, we were unable to fully evaluate access controls for internal users.

Source: TIGTA discussions and review of security documentation.

[20] IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (May 3, 2013).

The importance of adequate system access controls is well documented in Federal policy and guidance. NIST SP 800-53 states that a security incident could result in a breach to the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system. More specifically, because FRS security documentation was insufficient and the*****2**** **********2**********, we could not fully evaluate the adequacy of FRS access controls.

Recommendations

Recommendation 5: The Chief Technology Officer should ensure that the developer provides design and implementation documentation for the system security access controls in sufficient detail to permit analysis and testing of the controls.

> ***Management Response:*** The IRS disagreed with this recommendation, stating that the FRS is fully documented in the approved Design Specification Report. ***2***is appropriately referenced as part of the design, but a detailed design for this tool is not required as part of the Design Specification Report. The IRS also notes that the FRS was designed and developed by a fully integrated team of IRS and contractor personnel managed by IRS leadership.
>
> ***Office of Audit Comment:*** Security documentation in sufficient detail to enable analysis and testing of security controls is required for the FRS. Although the Design Specification Report references***2***, it does not provide sufficient detailed information on how to facilitate *internal* users' access controls. More critically, there is an absence of documentation for the**********2********** **********2**********.

Recommendation 6: The Chief Technology Officer should mitigate the risks associated with using**********2********** **********2**********.

> ***Management Response:*** The IRS disagreed with this recommendation, stating that it followed the process established at the time. **********2********** **********2**********2**********As part of the IRS's normal infrastructure review, a later version of the framework will be considered.
>
> ***Office of Audit Comment:*** **********2********** **********2**********2**********. TIGTA maintains that this risk requires definitive corrective actions to ensure adequate system security for the FRS. **********2********

**********2**********
*********2**********.

Improved Traceability of System Requirements to Testing Can Be Achieved Through Available Automated Tools

According to IRM 2.16.1, requirements management requires end-to-end traceability from customer needs, to requirements, to logical design, to physical design , to test cases, and to test results to verify that demonstrated functionality is consistent with required functionality.

The Rational RequisitePro (ReqPro) automated tool is the IRS's Enterprise Architecture standard for requirements management during system development . The IBM Rational Quality Manager (RQM) automated tool is the IRS's Enterprise Architecture standard for test case management during systems development. For FRS Release 1.1, ReqPro was used to generate a Requirements Traceability Verification Matrix to record and track requirements from inception through Systems Acceptability Testing (SAT) of the requirements. SAT management stated that they do not currently use full automation afforded by the Rational Tools Suite to integrate ReqPro with RQM for the FRS. Regarding the use of RQM for the FATCA, SAT management stated that they are moving away from the use of manual spreadsheets to implementing requirements in RQM, which will allow better traceability in the future. FATCA Program, FRS Project, and stakeholder personnel should fully use ReqPro and RQM to maintain bidirectional traceability from requirements to test cases to test results and thereby ensure that all requirements are fully tested prior to deployment. Figure 8 shows an overview provided to TIGTA on how these automated tools are used during IRS systems development processes.

Figure 8: IRS Requirements Management and Test Management Automated Tools

Current Tool(s)	Enterprise Architecture Recommended Standard	IRS Usage
ReqPro	Rational Requirements Composer	Create requirements and business rules
Rational ClearCase, Rational ClearQuest	Rational Team Concert	Track defects for testing and development and allow traceability
RQM	RQM	Manage requirements and test cases, and provide defect reporting
Rational Insight	Rational Insight	Produce the Requirements Traceability Verification Matrix and create dashboards
Rational System Architect	Rational System Architect	Create business process models and provide bidirectional traceability
	System Architect Web Client	

Source: IRS Rational Tools Integration Overview and Next Steps, December 6, 2013.

In March 2013, to implement complete requirements traceability, the IRS initiated a tools assessment to determine how to fully integrate and leverage the IRS's investment in IBM's Rational Tools Suite. The assessment identified the following benefits:

- Complete traceability from requirements to test cases to test results.
- Improved visibility into project status and performance through customizable dashboards at the individual, project, and program level.
- Integrated logical repository linking components to business architecture, design, and operations enabling for synchronization across artifacts.
- Enhanced team collaboration capabilities.
- Standardization across the enterprise to provide an established set of uniform standards, processes, and artifacts.

On November 18, 2013, the Associate Chief Information Officer, Enterprise Services, agreed to take ownership of the Rational Tools Suite and governance process and identified the following next steps:

- Establish governance and tool ownership processes.
- Drive Rational Tools Suite adoption.
- Define the Rational Tools Implementation Toolkit to meet the needs of simultaneous adoption for the enterprise.
- Build and deploy a Rational Tools Implementation Toolkit.

Recommendation

Recommendation 7: The Chief Technology Officer should ensure that a standard suite of integrated, automated tools is implemented to manage future FATCA system requirements, test cases, and bidirectional traceability.

> ***Management Response:*** The IRS disagreed with this recommendation, stating that the FRS was developed using the most current set of integrated, automated tools available, which are still the current standard. At such time when newer tools become available, the FRS will migrate to those along with the rest of the IT organization.
>
> ***Office of Audit Comment:*** TIGTA recommends that the FATCA IT PMO take the initiative to fully implement the most effective and efficient tools currently available to ensure complete FATCA requirements traceability. Complete requirements traceability for FATCA systems is needed to ensure successful requirements management, that the systems meet required functionality, and that IRS business needs are adequately addressed.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS has adequately mitigated system development risks for the FRS Project. To accomplish our objective, we performed the following procedures:

I. Determined the effectiveness of risk management controls in place for the FATCA Program and the FRS Project, including system and Enterprise Architectures, budget provisions, system or project requirements[1] management processes, performance measures and milestones, system development life cycle, and other applicable IRM guidance.

A. To obtain an understanding of the FRS as deployed, requested that the IRS provide a demonstration of the FRS that was deployed on December 9, 2013.

B. Ensured that FATCA risks are properly identified, monitored, and mitigated in accordance with applicable guidance.

C. Reviewed the FATCA Program and FRS Project Enterprise Architecture and determined whether the IRS plans to or has implemented technologies pertaining to electronic signatures or digital signatures and complied with guidance to Federal Agencies.

D. Inquired and documented the IRS's funding strategy for the FATCA Program. We documented approved funding and actual expenditures for the FATCA Program for Fiscal Years 2011–2014.

E. Obtained, reviewed, and evaluated FATCA Program and FRS Project defined business performance measures for information technology systems that relate to legislative responsibilities and goals for improving tax administration. We ascertained if measures are being monitored and achieved.

F. Obtained an understanding of tools that the IRS IT organization is using to design, develop, test, and deploy the FATCA system. This information will be used for future audit planning purposes.

G. Developed a timeline to identify key legislative, regulatory, and business drivers for the system. We also included key milestones and deadlines that affect systems development. We documented the size of the FFI population and number of IGAs.

[1] See Appendix IV for a glossary of terms.

II. Determined whether SAT of FRS Release 1.1 was performed in accordance with established IRS testing guidelines and evaluate test plan documentation and test results for the project.

III. Determined whether required system security requirements are guiding the FRS Project. We ensured that security testing was adequately planned and executed and considered the status of project responses for possible failed test cases.

A. Reviewed security guidelines including IRM 10.8.1[2] and NIST SP 800-53.[3]

B. Compared the controls in the FRS System Security Plan to the required FATCA **moderate** category security controls contained in NIST SP 800-53 to ensure that the required NIST security controls have been incorporated into the FATCA systems.[4] For any required NIST moderate security controls that were not included in the System Security Plan, we discussed the controls with the Cybersecurity organization to assess the potential impact of not including the controls.

C. Obtained and reviewed the System Security Plan to identify the security controls that should be designed into the FATCA Program. We ensured that the IRS has traced security requirements to security controls to security test cases and results.

D. For security controls in the System Security Plan, identified controls with an implementation status of partially in place or not in place. We determined if these security controls were properly resolved prior to deployment.

E. Determined if an authorization to operate was approved by an appropriate official for the FRS Project as deployed to date; the authorization to operate should be dated prior to deployment.

F. Determined that adequate security controls have been implemented to protect the FRS database by reviewing authentication and authorization of internal and external users.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRM and related IRS and

[2] IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Dec. 23, 2013).
[3] NIST, NIST SP 800-53 Rev. 3, *Information Security: Recommended Security Controls for Federal Information Systems and Organizations* (Aug. 2009). Also, NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) (includes updates as of Jan. 15, 2014).
[4] The IRS has rated the FRS in the moderate category per NIST guidelines. The moderate security categorization describes the potential adverse impacts to IRS operations, assets, and individuals should the information and information system be compromised through a loss of confidentiality, integrity, or availability.

Federal Government guidelines and the processes followed in the development of information technology projects. We evaluated these controls by conducting interviews with management and staff, observing testing activities, and reviewing documentation. Documents reviewed included the FATCA IT PMO Program Management Plan, the FATCA IT PMO Risk Management Plan, and other documents that provided evidence of the extent to which the IRS is adequately managing systems development risks for the FATCA Program.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Gwendolyn McGowan, Director
Carol Taylor, Audit Manager
Mark Carder, Lead Auditor
Hung Dam, Information Technology Specialist
Kevin Liu, Technical Audit Group Manager
Sylvia Sloan-Copeland, Senior Auditor
Lynn Ross, Senior Auditor
Larry Reimer, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Deputy Commissioner, Large Business and International Division SE:LB
Deputy Commissioner (International) Executive Assistant SE:LB:IN
Deputy Chief Information Officer for Operations OS:CTO
Director, Privacy, Governmental Liaison and Disclosure OS:P
Associate CIO, Applications Development OS:CTO:AD
Associate CIO, Cybersecurity OS:CTO:C
Associate CIO, EIT PMO OS:CTO:EI MP
Director, Risk Management Division OS:CTO:SP:RM
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Glossary

Term	Definition
Application	In information technology, the use of a technology, system, or product.
Artifact	One of many kinds of tangible by-products produced during the development of software. Some artifacts help describe the function, architecture, and design of software. Other artifacts are concerned with the process of development itself—such as project plans, business cases, and risk assessments. In connection with software development, artifacts are largely associated with specific development methods or processes.
Bidirectional Traceability	Bidirectional traceability of requirements can be established from the source requirement to its lower level requirements and from the lower level requirements back to their source. Such bidirectional traceability helps determine that all source requirements have been completely addressed and that all lower level requirements can be traced to a valid source. Also, once test cases are developed for associated requirements, bidirectional traceability enables requirements to trace to test cases and test cases to trace to requirements.
Business Objects	A broad category of business processes that are modeled as objects. A business object can be as large as an entire order processing system or a small process within an information system.
Business Systems Requirements Report	This report documents a feasible, quantified, verifiable set of requirements that define and bound the business system or subsystem(s) being developed or enhanced by the project.
Customer Account Data Engine	The technology foundation that will provide the IRS with the capability to manage its tax accounts in a way that is central to the achievement of the IRS's modernization vision. This system's goal is to create current, complete, and accurate authoritative data stores and construct the related tax administration systems processes.
Design Specification Report	Documents the logical and physical design of a proposed solution from all applicable perspectives. The Design Specification Report is created in the Preliminary Design phase (Milestone 3) and is updated with physical design details during the Detailed Design phase (Milestone 4A).

Term	Definition
Digital Signature	Encrypted data produced by a mathematical process applied to a record using a hash algorithm and public key cryptography. The encrypted data are such that a person having the initial record and the public key that allegedly corresponds to the private key used to create the encrypted data can accurately determine: (1) whether the encrypted data were created using the private key that corresponds to such public key and (2) whether the initial message has been altered since the encrypted data were created. The encrypted data constituting the digital signature are sometimes used as an electronic signature, are sometimes used as part of a process to authenticate a person or device, and are sometimes used to verify the integrity of the record.
Electronic Fraud Detection System	The primary application used by the Wage and Investment Division's Return Integrity and Correspondence Services to process revenue protection activities.
Employee User Portal	IRS portal that allows IRS employee users to access IRS data and systems, such as tax administration processing systems, financial information systems, and other data and applications, including mission-critical applications. Modernization registration and authentication are required for access to sensitive and mission-critical applications, and all user interactions with those systems are encrypted from workstation to portal across the IRS internal network. It allows IRS employee users with local area network accounts (Windows Network Login) to access Intranet sites, selected applications, nonsensitive data, and selected sensitive processing for which network encryption and modernization logon are not required (*e.g.*, employee access to selected elements of their own personnel data). IRS network authentication is a basic requirement for access to any materials or services and is also required to access modernization registration and authentication.
Enterprise Architecture	A unifying overall design or structure for an enterprise that includes business and organizational aspects of the enterprise as well as technology aspects. Enterprise Architecture divides the enterprise into its component parts and relationships and provides the principles, constraints, and standards to help align business area development efforts in a common direction. An Enterprise Architecture ensures that subordinate architectures and business system components developed within particular business areas and multiple projects fit together into a consistent, integrated whole.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Financial Institution (FI)	Any foreign financial business or entity (*e.g.*, banks, hedge funds), in which a U.S. taxpayer may hold an account or financial/ownership interest, that may attempt to enter into an agreement with the IRS under the FATCA to become an approved FI.

Term	Definition
Foreign Financial Institution (FFI)	FFIs include any non-U.S. entity that accepts deposits, holds financial assets, or engages in the business of investing. This includes foreign banks, foreign branches of U.S. banks, and businesses organized under a foreign law that would be a securities broker-dealer if located in the U.S., *e.g.*, money transmitter, currency exchanger.
Global Intermediary Identification Number (GIIN)	An identification number that is assigned to a participating FFI or a registered deemed-compliant FFI after its FATCA registration is submitted and approved.
Integrated Enterprise Portal	The new platform for all portal applications. It represents a multiyear upgrade to the entire online portal infrastructure. It is also the first instance of an innovative, managed service, providing an external private cloud infrastructure.
Intergovernmental Agreement (IGA)	A U.S. Department of the Treasury agreement with foreign governments (countries) to implement the information reporting and tax withholding provisions of the FATCA via an automatic exchange of information. IGAs generally allow for government-to-government reporting of the information and address privacy laws and the disclosure of account holder information. Model 1 agreements require FFIs to report to the IRS through their host country taxing authorities. Model 2 agreements require FFIs to report directly to the IRS.
International Organization for Standardization	International Organization for Standardization is an independent, nongovernmental membership organization and the world's largest developer of voluntary international standards.
*********2********	**************************2************************************* **************************2************************************* ******************2******************
Large Business and International (LB&I) Division	The LB&I Division serves corporations, subchapter S corporations, and partnerships with assets greater than $10 million. These entities typically have large numbers of employees, deal with complicated issues involving tax law and accounting principles, and conduct their operations in an expanding global environment.
Modernized e-File	Modernized e-File receives and processes e-file returns in an Internet environment. Many returns are received through the Registered User Portal using a component called the Internet Filing Application. Modernized e-File provides for real-time processing of acknowledgements, streamlined error detection, standardization of business rules and requirements across form types, the capability to attach portable document format files, and the capability for IRS employees to view return data through the Employee User Portal and the Business Objects Server.

Term	Definition
National Institute of Standards and Technology (NIST)	A nonregulatory Federal agency, within the Department of Commerce, responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
Nonfinancial Foreign Entities	Nonfinancial foreign entities are considered small, unsophisticated investment entities like family trusts unless they are professionally managed. If professionally managed, these entities are considered FFIs, but the expectation is that the manager (also now deemed to be an FFI) will complete FATCA reporting.
Open Source	In production and development, a development model that promotes a universal access via free license to a product's design or blueprint, and universal redistribution of that design or blueprint, including subsequent improvements to it by anyone.
Participating FFI	A participating FFI will enter into a registration agreement with the IRS to identify U.S. accounts, report certain information to the IRS regarding U.S. accounts, and withhold a 30 percent tax on certain U.S. payments to nonparticipating FFIs and account holders who are unwilling to provide the required information.
Personally Identifiable Information (PII)	PII is information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of PII are name, Social Security Number, date of birth, place of birth, address, and biometric records.
Public User Portal	The Public User Portal (formerly the Digital Daily) is the IRS external or Internet portal that allows unrestricted public access to nonsensitive materials and applications, including forms, instructions, news, and tax calculators. No authentication is required for access to any materials on the Public User Portal.
Registered User Portal	The IRS external portal that allows registered individuals and third-party users (registration and login authentication required) and other individual taxpayers or their representatives (self-authentication with shared secrets required) to access the IRS for interaction with selected tax processing and other sensitive systems, applications, and data. User interactions are encrypted from the user's workstation or system to the portal, across the Internet or via direct circuits. The Registered User Portal, via the Common Communication Gateway, also supports IRS extranets, such as the exchange of bulk files of information with the IRS and the Virtual Private Network (both inbound and outbound) by registered and authorized external entities
Requirement	A formalization of a need that is the statement of a capability or condition that a system, subsystem, or system component must have or meet to satisfy a contract, standard, or specification.

Term	Definition
Requirements Traceability Verification Matrix	A tool that documents requirements and establishes the traceability relationships between the requirements to be tested and their associated test cases and test results.
Return Review Program	The Return Review Program is a new integrated system that adds to the IRS's capability to detect, resolve, and prevent criminal and civil tax noncompliance and fraud.
Security Controls Assessment (SCA)	An SCA is conducted in the IRS production environment and consists of activities designed to ensure that the system's security safeguards are in place and functioning as intended.
*****2********	*************************2************************************ *************************2************************************ *************************2************************************ *************************2************************************ *************************2************************************ ************2*************
Sponsoring Entity	A sponsoring entity is an entity that will perform the due diligence, withholding, and reporting obligations of one or more sponsored investment entities or controlled foreign corporations.
Systems Acceptability Test (SAT)	A SAT verifies that the system satisfies software application requirements.
Withholding Agent	A withholding agent is a U.S. or foreign person that has control, receipt, custody, disposal, or payment of any item of income of a foreign person that is subject to withholding. A withholding agent may be an individual, corporation, partnership, trust, association, or any other entity, including any foreign intermediary, foreign partnership, or U.S. branch of certain foreign banks and insurance companies.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF TECHNOLOGY OFFICER

September 8, 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR_AUDIT

FROM: Terence V. Milholland /s/ Terence V. Milholland
Chief Technology Officer

SUBJECT: While the Foreign Financial Institution Registration System Deployed on Time, Improved Controls Are Needed (Audit 201420013) (e-trak #2014-58575)

Thank you for the opportunity to review your draft audit report and to discuss earlier draft report observations with the audit team. We appreciate TIGTA noting the timely delivery of the FATCA FI Registration System in your report.

With regard to your recommendations, we disagree with TIGTA's conclusions in the areas of performance measures, electronic signature, security-specific requirements, security access controls, ****2*****, and assurance that a standard suite of integrated, automated tools is implemented to manage future FATCA system requirements, test cases, and bidirectional traceability.

Performance Measures

Business performance measures for the FATCA FI Registration System are not the responsibility of the Chief Technology Officer. The Commissioner, Large Business and International, has developed business performance measures for the FATCA FI Registration System. The Chief Technology Officer will incorporate these measures into the Exhibit 300 for inclusion in the FY 2016 budget submission.

Security-Specific Requirements

Throughout the development lifecycle of the FATCA FI Registration System the appropriate system-specific security testing was conducted, as sanctioned by the Information Technology (IT) Cyber Security organization and governed by the IRS *Information Technology (IT) Security, Policy and Guidance*, IRM 10.8.1. As required by IRM 10.8.1.4.15.2 SA-3 *System Development Life Cycle (SDLC)*, FATCA FI Registration System was developed and tested via the IRS - approved SDLC method- the IRS Enterprise Life Cycle (ELC).

During Release 1.1 Drop 1, the FATCA FI Registration System went through Security Accreditation and Authorization (SA&A) and completely tested those security controls necessary to achieve an Interim Authority to Operate. During Release 1.1 Drop 2, the FATCA FI Registration System went through an ED-SCA (Event-Driven Security Control Audit) to capture

and fully test those features and functions not previously tested during the initial SA&A. An Authority to Operate (ATO) was issued in November 2013, prior to the go-live date of December 9, 2013. In addition, throughout the Development Lifecycle, test cases relating to specific areas that tie back to security requirements, such as those governing the Access Code and FATCA ID generation, were fully tested and documented within the FATCA FI Registration System Requisite Pro repository.

As IRS followed the standard practice necessary to obtain Cybersecurity authorization to operate the FATCA FI Registration System, and as TIGTA did not find any specific examples related to FATCA FI Registration System where security testing was deficient, we do not agree with this recommendation.

Use of Electronic Signature

During the course of the audit, IRS discussed with TIGTA that there were no requirements for e- Signature given to IT by the business. The Chief Technology Officer timely delivered the system per business requirements.

Security Access Controls

TIGTA asserts that contractors have maintained all information regarding the source of design and implementation of security in a proprietary fashion such that the IRS has no access to or knowledge of such information. This is both inaccurate and misleading and leads to the inaccurate conclusion that there is potential security vulnerability in the design of the FRS based on such proprietary knowledge.

A secondary issue with the recommendation is that TIGTA holds the FATCA PMO responsible for fully documenting the authentication and access control capabilities for ***2***, a tool used by the application. IRS disagrees that the FATCA FI Registration System documentation should contain detailed design information for ***2***. ***2*** is a common use service within IRS that is leveraged by many applications including the FATCA FI Registration System. IRS fully tested all access controls that were integrated with ***2*** to ensure the roles-based accesses were working as designed. These tests are fully documented within the Requisite Pro repository, and traced to requirements and results.

**********2**********

The version of **********2*********used to create the access controls and authentication for the external users of the Financial Institution Registration System was the most current version available at the time. As part of Information Technology's normal infrastructure review process, we will consider a newer version of the Framework, if approved for use on IRS systems.

Standard Suite of Integrated Tools

We disagree that the Chief Technology Officer should specifically ensure that a standard suite of integrated, automated tools is implemented to manage future FATCA system requirements, test cases, and bidirectional traceability. FATCA FI Registration System completely documented system requirements and traceability using the existing suite of IRS approved tools. This recommendation has already been addressed in other audit reports, and IRS is responding to this recommendation at the Enterprise level.

We are committed to continuously improving IRS information technology systems and processes. We value your continued support, and the assistance and guidance your team provides. Our corrective action plan for the recommendations is attached. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Lisa Starr, Program Oversight Manager Coordination Manager, at (240) 613-4219.

Attachment

RECOMMENDATION #1: The Chief Technology Officer should ensure that the IRS Information Technology organization and the LB&I Division coordinate to timely develop and implement adequate business performance measures to quantify net benefits for information technology investments in support of the FATCA.

CORRECTIVE ACTION #1: The Commissioner, Large Business and International, is responsible for the business measures for the FATCA FI Registration System and has developed these measures. The Chief Technology Officer will incorporate these measures in the OMB Exhibit 300 for the IRS's FY 2016 budget submission.

IMPLEMENTATION DATE: January 25, 2015

RESPONSIBLE OFFICIAL: Deputy Commissioner (International), Large Business and International

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES). These Corrective Actions are monitored on a monthly basis until completion.

RECOMMENDATION #2: The Chief Technology Officer should ensure that system-specific security requirements are traced to test cases, and test cases to test results to ensure the completeness of Financial Institution Registration System security testing. This will also provide assurance that adequate system-specific security will be in place throughout the lifecycle of the FRS.

CORRECTIVE ACTION #2: The IRS disagrees with this recommendation. There were no specific findings from this audit related to any specific test cases as documented within the Financial Institution Registration System Requisite Pro repository that were presented to the IRS as examples of a deficiency. Instead, TIGTA presented the recommendation based on a one-time initiative taken by the CADE2 project wherein every NIST Security Control had been traced in some manner to some type of testing and included in the CADE2 security documentation. This is not a standard practice within IRS.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #3: The Chief Technology Officer should ensure that the FATCA IT PMO determines whether the particular technology and set of procedures that comprise the signing process are as reliable as is appropriate for the intended purpose.

CORRECTIVE ACTION #3: No business requirements existed to provide an e-Signature capability for the FATCA FI Registration System. The Chief Technology Officer delivered the system per business requirements. TIGTA was provided with the legal analysis undertaken by the Associate Chief Counsel (International) on whether an electronic signature was needed.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #4: The Commissioner, LB&I Division, should ensure that the LB&I Division completes a thorough risk analysis and cost-benefit analysis to better assess the likelihood and cost of not implementing enforceable electronic signatures for the FRS.

CORRECTIVE ACTION #4: LB&I has provided TIGTA with a report that outlined the decision on Part Four of the FATCA registration system regarding the signature. In addition, we are completing a risk assessment to document the decision.

IMPLEMENTATION DATE: October 25, 2014

RESPONSIBLE OFFICIAL: Deputy Commissioner (International), Large Business and International Division

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES). These Corrective Actions are monitored on a monthly basis until completion.

RECOMMENDATION #5: The Chief Technology Officer should ensure that the developer provides design and implementation documentation for the system security access controls in sufficient detail to permit analysis and testing of the controls.

CORRECTIVE ACTION #5: The IRS disagrees with this recommendation. The application is fully documented in an approved Design Specification Report (DSR). ***2***is appropriately referenced as part of the design, but a detailed design for this tool is not required as part of the application DSR.

Additionally, in a previous response to a draft version of this Audit Report, TIGTA was requested to remove all reference to "the contractor" as it related to "the developer" and any inferences that the FATCA FI Registration System was developed solely by an outside organization. The Financial Institution Registration System was designed and developed by a fully integrated team of IRS and Contractor personnel managed by IRS leadership.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #6: The Chief Technology Officer should mitigate the risks associated with using an **********2**********.

CORRECTIVE ACTION #6: The IRS disagrees with this recommendation. IRS followed the process established at the time. The version of **********2**********2**********. As part of our normal infrastructure review, a later version of the Framework will be considered.

IMPLEMENTATION DATE: N/A

RESPONSIBILE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #7: The Chief Technology Officer should ensure that a standard suite of integrated, automated tools is implemented to manage future FATCA system requirements, test cases, and bidirectional traceability.

CORRECTIVE ACTION #7: The IRS disagrees with this recommendation. The Financial Institution Registration System was developed using the most current set of integrated, automated tools available, which are still the current standard. At such time when newer tools become available, the Financial Institution Registration System will migrate to those along with the rest of the Information Technology organization.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A