TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Integrated Financial System Updates Are Improving System Security, but Remaining Weaknesses Should Be Addressed

March 28, 2013

Reference Number: 2013-20-030

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.

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

INTEGRATED FINANCIAL SYSTEM UPDATES ARE IMPROVING SYSTEM SECURITY, BUT REMAINING WEAKNESSES SHOULD BE ADDRESSED

Highlights

Final Report issued on March 28, 2013

Highlights of Reference Number: 2013-20-030 to the Internal Revenue Service Chief Financial Officer and Chief Technology Officer.

IMPACT ON TAXPAYERS

The Integrated Financial System (IFS) is the IRS's core financial system and annually assists the IRS in accounting for approximately $12 billion in operational funds.

The IFS was implemented as a major project under the IRS's Business Systems Modernization Program, but in November 2005 the system was reclassified as Operations and Maintenance funding. For Fiscal Years 2012 and 2013, the IRS requested nearly $37.5 million to upgrade the IFS. Recently, the IRS initiated approximately $10.5 million in system updates for the IFS that include: 1) encryption of graphical user interface traffic, 2) update of the platform with functional enhancements, and 3) support of a Department of the Treasury mandate for all Federal agencies. The IRS planned to complete deployment of these system updates in November 2012.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS has adequately planned for recent updates of the IFS to support long-term goals and to mitigate risks in accordance with the Department of the Treasury, IRS, and other systems development guidelines. TIGTA evaluated key management controls and processes, project funding, and system security risks.

WHAT TIGTA FOUND

In July 2012, the IRS implemented the System Application and Products Secure Network Connection, providing for data encryption and eliminating security weaknesses in the Citrix and IFS Windows 2000 environments. With successful implementation of System Application and Products Enterprise Central Component 6.0, the IRS expects that the IFS will be in compliance with current Federal laws and accounting standards and will address the security weakness related to Oracle database software.

As planned, IFS updates address compliance for specific information technology security controls. However, improvements are needed to better ensure that: 1) remaining IFS security weaknesses are adequately addressed and 2) system requirements testing consistently complies with established IRS guidelines.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer work with the Chief Financial Officer to: 1) apply existing or implement additional access controls to ensure that IFS users are restricted to IRS employee sensitive data on a "need to know" basis; 2) implement control checks to prevent IFS users from accessing unauthorized IRS employee accounts or prepare a risk-based decision and accept the risk; 3) implement two-factor authentication in a future release and identify a form of multifactor authentication for IFS system administrators; 4) ensure that all applicable system requirements for IFS test cases include expected results; and 5) ensure that all IFS testers obtain and maintain documentation to verify test case results.

In its response, the IRS agreed with our recommendations. The IRS plans to restrict access to sensitive employee data to only those users with a "need to know" basis; evaluate the identified low risk to determine if a risk-based decision is needed; implement the new version of the Secure Network Connection module once its certification is completed in late 2013; ensure that the IFS is included in the current program-level mitigation strategy to implement two-factor authentication; and link its Rational Quality Manager to its requirements repository so that requirements test management can be properly documented.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

March 28, 2013

MEMORANDUM FOR CHIEF FINANCIAL OFFICER
CHIEF TECHNOLOGY OFFICER

Michael E McKenney

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Integrated Financial System Updates Are Improving System Security, but Remaining Weaknesses Should Be Addressed (Audit 201220013)

This report presents the results of our review of updates to the Integrated Financial System. The overall objective of this review was to determine whether the Internal Revenue Service (IRS) has adequately planned for Integrated Financial System updates to support long-term goals and to mitigate risks in accordance with the Department of the Treasury, IRS, and other systems development guidelines. This audit was included in the Treasury Inspector General for Tax Administration Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Modernization of the IRS.

Management's complete response to the draft report is included as Appendix V in the attached PowerPoint presentation.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), if you have questions.

Attachment

PDF

201320030-Final
Report.pdf

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Integrated Financial System Updates Are Improving System Security, but Remaining Weaknesses Should Be Addressed

March 28, 2013

Reference Number: 2013-20-030

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.

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

Table of Contents

Abbreviations

Abbreviation	Description
CFO	Chief Financial Officer
CTO	Chief Technology Officer
ECC	Enterprise Central Component
FIPS	Federal Information Processing Standards
IFS	Integrated Financial System
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
RBD	Risk-Based Decision
SAP	Systems Applications and Products
SNC	Secure Network Connection
SSN	Social Security Number
SSP	System Security Plan

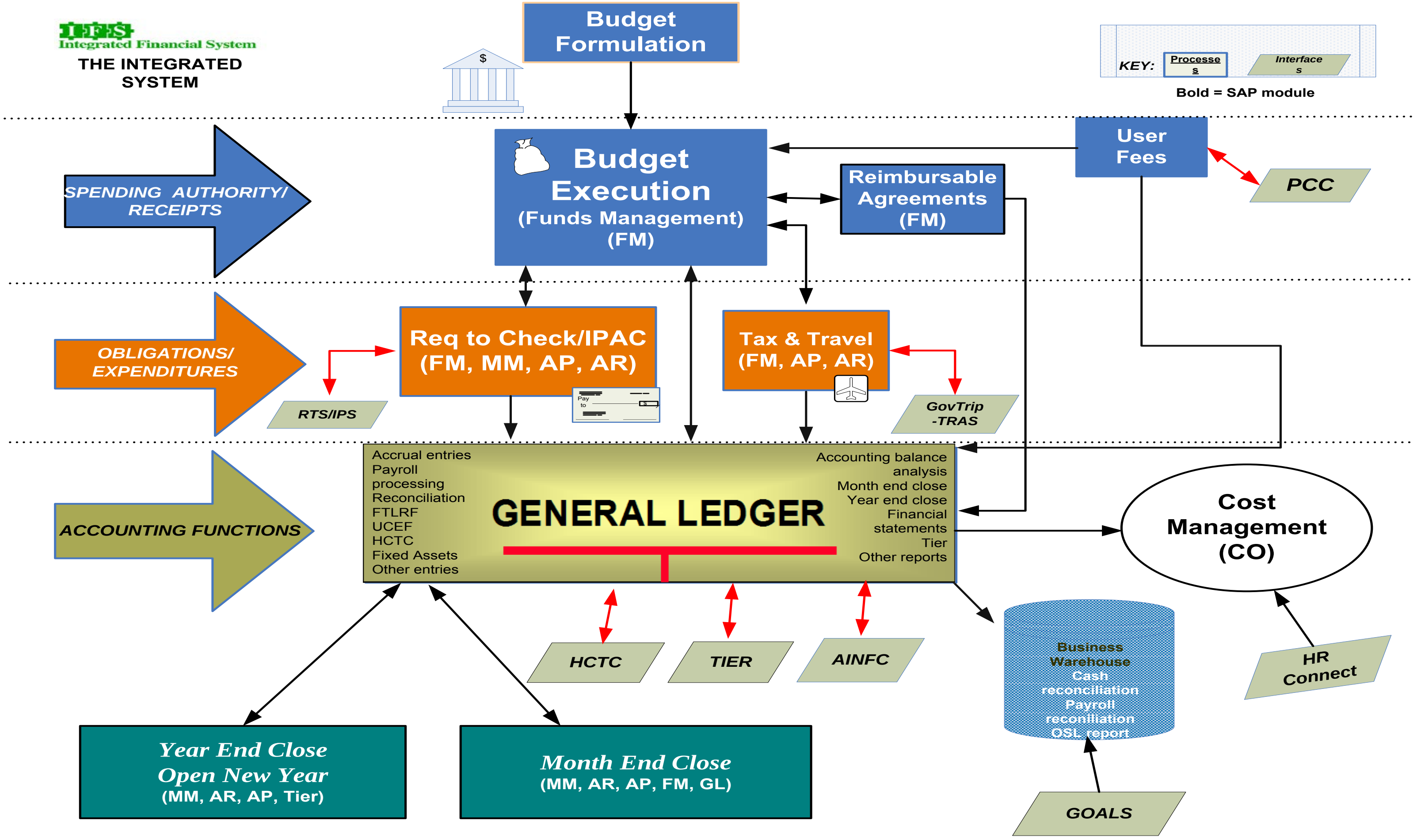
Background

- In November 2004, the Internal Revenue Service (IRS) replaced the Automated Financial System with the Integrated Financial System (IFS). The IFS is the IRS's core financial system and annually accounts for approximately $12 billion in operational funds.
- The IFS was implemented as a major project under the Business Systems Modernization Program and supports the IRS's administrative financial operations.
- In November 2005, the IFS was reclassified as Operations and Maintenance funding.
- The IFS has 24 custom interfaces with systems belonging to the IRS, Department of the Treasury, and General Services Administration. The IFS Data Transfer Service uses these interfaces to transport data files in and out of the IFS.

- The IFS provides processes and reports (Figure 1) for the following:
  - General ledger, accounts receivables, and accounts payable (Financial Accounting module).
  - Budget execution (Funds Management module).
  - Cost accounting (Controlling module).
  - Purchasing (Materials Management and Purchasing module).
  - Budget formulation (Business Warehouse module).
- IFS management stated that the system does not process or report on the IRS's tax revenues and refunds.[1]

[1] The IFS provides some tax processing functionality for Health Coverage Tax Credit payments.

Figure 1: Overview of IFS Processes



Source: Office of the Chief Financial Officer. AINFC = Automated Interface National Finance Center; AP = Accounts Payable; AR = Accounts Receivable; FM = Funds Management; FTLRF = Federal Tax Lien Revolving Fund; GL = General Ledger; GOALS = Government On-Line Accounting Link System; HCTC = Health Coverage Tax Credit; HR = Human Resources; IPAC = Intra-Governmental Payment and Collection; IPS = Integrated Procurement System; MM = Materials Management; OSL = Obligation Subsidiary Ledger; PCC = Paper-Check Conversion; RTS = Request Tracking System; SAP = Systems Applications and Products; TRAS = Travel Reimbursement & Accounting System; and TIER = Treasury Information Executive Reporting; UCEF [sic] = UCFE = Unemployment Compensation for Federal Employees.

- The Office of the Chief Financial Officer (CFO) and the Information Technology organization, Applications Development Office, share dual responsibility over IFS operations.

- The IFS uses a version of software that is more than 10 years old. Beginning in Fiscal Year 2011, the vendor ceased providing new changes to accommodate new legislative or Federal accounting requirements.

- The vendor provided only customer-specific support, charging maintenance to keep the outdated version operational. Thus, the IRS is paying a premium to maintain the IFS and, if successful, the updates will allow the IRS to reduce maintenance costs.

- During Fiscal Year 2011, the IRS established an extended agreement with the vendor to provide necessary maintenance support through January 2013.

- ❑ For Fiscal Years 2012 and 2013, the IRS requested nearly $37.5 million to fully upgrade the IFS software.
- ❑ The proposed IFS upgrade was not fully funded; however, the IRS received approximately $10.5 million for specific IFS updates.
- ❑ These IFS updates include:
  - ❑ Systems Applications and Products (SAP) Netweaver Single Sign-On Secure Network Connection (SNC) to encrypt graphical user interface traffic.
  - ❑ SAP 4.6C to Enterprise Central Component (ECC) 6.0 establishing the current technology platform with functional enhancements.
  - ❑ The Internet Payment Platform, a Department of the Treasury mandate for all Federal agencies, to be implemented in conjunction with SAP ECC 6.0.
- ❑ The IRS is considering additional IFS modifications, which were part of the $37.5 million full system upgrade request, if funding is approved. This would include budget formulation and reimbursable systems modules and integrating the IFS with the Integrated Procurement System.

Audit Objective

- ❑ Determine whether the IRS has adequately planned for IFS updates to support long-term goals and to mitigate risks in accordance with the Department of the Treasury, IRS, and other systems development guidelines.
  - ❑ Determine whether the IFS Project Management Office has established key management controls and processes in accordance with systems development guidelines.
  - ❑ Determine whether project funding for the IFS update is current, accurate, and complete.
  - ❑ Determine if the IFS includes adequate security controls to address system security risks prior to deployment of the updates.

Results of Review

- IFS Updates Address Compliance and Specific Security Weaknesses (see slide 11).
- Remaining IFS Security Issues Should Be Addressed (see slides 12 through 21).
- Systems Requirements Testing Processes Did Not Consistently Comply With Guidelines (see slides 22 through 26).

IFS Updates Address Compliance and Specific Security Weaknesses

- ❑ The IFS updates management team established the Project Tailoring Plans and issued systems development plans covering key processes.

- ❑ Funding amounts were documented for each of the IFS updates.

- ❑ In July 2012, the IRS implemented the SAP SNC, providing for data encryption and eliminating security weaknesses in the Citrix and IFS Windows 2000 environments no longer supported by the vendor.

- ❑ The IRS reported a cost savings of approximately $1 million per year for technical support resulting from eliminating the Citrix servers.

- ❑ With successful implementation of SAP ECC 6.0, the IRS stated that the IFS will be in compliance with current Federal laws and accounting standards and will address the security weakness related to Oracle database software that is no longer supported by the vendor.

Remaining IFS Security Issues Should Be Addressed

IFS users have access to Personally Identifiable Information (PII) without a business need

- ❑ The Office of Management and Budget and the Internal Revenue Manual (IRM) 10.5.1. require that unique identifiers be used in place of Social Security Numbers (SSN) on systems, where possible, to prevent unnecessary disclosure of PII.
- ❑ The IRM also requires that individuals with access to sensitive data, including SSNs and PII, have a “need to know” based upon the performance of their job duties and receive managerial authorization for system access.

- IFS screens display SSNs in clear text, along with associated PII. Approximately 320 IFS users access the system using SSNs to perform vendor and document analysis as part of their IFS duties.
  - Further, currently there are approximately eight IFS users who have access to this information, even though it is not part of their IFS duties.
  - In May 2012, the CFO and the Chief Technology Officer (CTO) drafted a Risk-Based Decision (RBD) and Plan of Action and Milestones to address this weakness and are awaiting stakeholders' comments.
  - Based on discussions, the IRS proposed a short-term solution to review and remove users who do not have a "need to know" by March 2013, after deployment of the IFS update.
  - The IRS also proposed a long-term solution that will require changes to the IFS screens by limiting the number of authorized users and masking of the SSNs; however, this solution will require additional time beyond March 2013 and additional funding.

- In addition, 110 IFS users have access to the 1099 and W-2 system data[2] for some IRS employees and vendors, but reasonable access control checks are not in place, such as those that would identify or prevent a user viewing another IRS employee's tax information. Specific types of employee tax information include long-term travel and tuition assistance payments.
  - IFS management stated that the potential for inappropriate use is low as the data do not include taxable earnings; therefore, no corrective actions were taken. We maintain that any inappropriate access is unacceptable.
  - Following audit discussions, the CFO initiated plans to look at the business process impacts of implementing changes after the IFS update deployment. Until this analysis can be conducted, the CFO has accepted the risk and plans to establish an RBD.

[2] The 1099 system includes information from various versions of Forms 1099 used to report types of income such as interest, dividends, and miscellaneous income. The W-2 system includes information from Forms W-2, *Wage and Tax Statement*.

- The loss, theft, or unauthorized disclosure of PII places individuals at risk for identity theft and invasion of privacy. The proper protection of PII helps maintain system integrity and the IRS's reputation for privacy protection, which are critical for the IRS to perform its mission.

- **Management Action:** After we advised the CFO staff that there were an unknown number of IFS users with access to PII, they performed an analysis to determine which users should not have access to PII.

Recommendations

- ❑ ***Recommendation 1:*** The CTO should work with the CFO to implement access controls necessary to ensure that IFS users are adequately restricted from IRS employee sensitive data, including SSNs and PII, until the planned long-term solution can be implemented.
  - ❑ ***Management's Response:*** The IRS agreed with this recommendation. The IRS will review IFS access to IRS employee sensitive data, including SSNs and PII, and restrict access to only those users with a "need to know."
- ❑ ***Recommendation 2:*** The CTO should work with the CFO to either implement access control checks to prevent IFS users from accessing unauthorized IRS employee accounts or to appropriately document this risk.
  - ❑ ***Management's Response:*** The IRS agreed with this recommendation. The IRS will conduct an analysis and remove users who do not have a "need to know" and evaluate the identified low risk to determine if an RBD is needed.

SAP SNC is FIPS 140-2 compliant but not yet certified for validation

- The Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, specifies security requirements when cryptographic modules are used within a security system protecting sensitive information.
- The National Institute of Standards and Technology (NIST) recommends and IRM 10.8.1. requires that the IRS use only cryptographic modules that have been validated in accordance with FIPS 140-2 or later.
- Protection of a cryptographic module within a security system is critical to maintain the confidentiality and integrity of the information protected by the modules.
- On March 19, 2012, the Office of the CFO and the Information Technology organization (formally known as Modernization and Information Technology Services) both signed an RBD stating that implementation of the SAP SNC solution would strengthen the system's internal controls.

- On June 16, 2012, the IRS deployed the SAP SNC solution, replacing the outdated Citrix software, for the IFS. However, IFS management informed us that the new solution is FIPS 140-2 compliant but not yet certified for validation.

- During development and testing of the new SAP software, the Office of the CFO received a waiver from the Enterprise Architecture Office to operate the IFS, but production deployment was contingent upon obtaining the certification.

- IFS management stated that the cryptographic module will be FIPS 140-2 certified with the next version of the IFS, approximately late in 2013, after deployment of the IFS update.

- If requirements are not followed, the IFS will not comply with NIST and IRS standards to adequately protect and reduce serious risk that includes unauthorized access or loss of sensitive data.

Recommendation

- ***Recommendation 3:*** The CTO should work with the CFO to update and document the status in the System Security Plan (SSP) as FIPS 140-2 certified with the next version of the IFS in Fiscal Year 2013.

  - ***Management's Response:*** The IRS agreed with this recommendation. SAP and NIST test centers have notified the IRS that the FIPS 140-2 certification of the SNC module will be completed in late 2013. Once certification is completed, the IFS will implement the new version of the SNC.

The IFS does not yet provide for multifactor authentication

- The NIST recommends user identities be authenticated through the use of passwords, tokens, biometrics, or a combination thereof. Based upon this criteria, multifactor authentication for systems administration access is required for the IFS.

- The IFS SSP states that the IFS relies on the Modernization and Information Technology Services General Support System-18 for identification and authentication. However, General Support System-18 does not support multifactor authentication of system administrators.

- The IRS has recognized that deployment of two-factor authentication is a program-level control weakness and plans to implement two-factor authentication as part of an enterprise solution.

- If the IRS does not provide multifactor authentication for IFS system administrators, this could result in the reliance on outdated, insecure password authentication for network and local authentication used to protect sensitive data, including SSNs and PII.

Recommendation

- ***Recommendation 4:*** The CTO should work with the CFO to implement two-factor authentication and, in the short term, identify compensating authentication controls for IFS system administrators.
  - ***Management's Response:*** The IRS agreed with this recommendation. The CTO will ensure that the IFS is included in the current program-level mitigation strategy to implement two-factor authentication and identify a form of multifactor authentication for IFS system administrators.

Systems Requirements Testing Processes Did Not Consistently Comply With Guidelines

Not all test cases included expected results

- IRM 2.6.1 requires that test cases should be developed to support requirements testing. Test cases should include requirements being tested and the expected results.

- During testing for IFS system updates, the expected results in the test cases should be compared to the actual results observed by the tester to determine whether the requirements were sufficiently tested.

- We judgmentally sampled[3] and reviewed 10 of the 363 total IFS system update requirements to determine whether test cases were properly developed in accordance with IRM 2.6.1. We selected seven functional and three security requirements to represent the different types of IFS requirements.

[3] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population. Judgmental sampling was used because we did not intend to project our results.

- The 10 sampled requirements related to four test cases. The test cases did not always include the expected results, and one test case only included expected results for one of 15 test steps.
- IFS management informed us that the expected results for the four test cases included a spreadsheet of budget figures that was too large to attach to the test cases.
- As a result, IFS testers needed to obtain information outside the approved test cases to verify that the requirements were tested.
- When expected results are not fully presented in test cases, the risk of accepting inadequate test results increases, which could adversely affect IFS functionality.

Recommendation

- ***Recommendation 5:*** The CTO should work with the CFO to ensure that all applicable IFS test cases include expected results to validate that systems requirements were sufficiently tested.
  - ***Management's Response:*** The IRS agreed with this recommendation. The Enterprise System Test group will implement standard processes and tools for Systems Acceptance Testing in accordance with soon-to-be issued IRM changes. The Enterprise System Test group is working to link its Rational Quality Manager to the RequisitePro requirements repository so that full requirements test management can be adequately and accurately documented.

Testers did not always obtain documentation to validate the actual test results

- IRM 2.6.1. requires that testers obtain and maintain evidence to validate the actual test results, which could include computer screen prints, input and output data files, and system logs.

- The testers did not always obtain and maintain documentation for four of 10 sampled requirements to validate the actual test results.

- IFS management did not ensure that testers consistently followed IRM guidelines to obtain and maintain objective evidence, such as screen prints, to verify that requirements were sufficiently tested.

- If the documents used to verify actual test results are not available, then the IRS cannot verify the adequacy of its systems testing activities. This increases the risks of adverse impact on the functionality of the IFS.

Recommendation

- ***Recommendation 6:*** The CTO should work with the CFO to ensure that all IFS testers obtain and maintain documentation to verify actual test case results.

  - ***Management's Response:*** The IRS agreed with this recommendation. The EST group will implement standard processes and tools for SAT testing in accordance with soon-to-be-issued IRM changes. EST is working to link its RQM to the RequisitePro requirements repository so that full requirements test management can be adequately and accurately documented.

Detailed Objective, Scope, and Methodology

- **Overall Objective:** Determined whether the IRS had adequately planned for IFS updates to support long-term goals and to mitigate risks in accordance with Department of the Treasury, IRS, and other systems development guidelines.
- Determined whether the IFS Project Management Office had established key management controls and processes in accordance with Department of the Treasury, IRS, and other systems development guidelines. We considered the following program and project controls for the IFS:
  - Applicable guidance from Department of the Treasury, IRS, and SAP best practices.
  - Established plans with the Integrated Procurement System.
  - Integrated master schedules, work breakdown structures, and schedules.
  - Program and project charters.
  - Program and project management plans.
  - Risk and issue management plans.
  - Requirements management plans.

  - Configuration and change management plans.
  - Test management plans.
  - Human resources.
- Considered project funding for the IFS update by reviewing:
  - Estimated costs and benefits and supporting documentation.
  - Cost tracking mechanisms for IFS update.
  - Contract management practices including task order for the project.
- Reviewed security controls identified in the SSP.
  - Determined whether the IFS SSP includes adequate security controls for the system updates.
  - Determined whether all security and privacy requirements were adequate.
  - Determined whether all security risks were adequately addressed.

- This review was performed at the Office of the CFO and Information Technology organization in New Carrollton, Maryland, from July through October 2012.
- We conducted this performance audit in accordance with generally accepted government auditing standards, which 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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 the following internal controls were relevant to our audit objective: NIST Special Publication 800-53, the IRM, and related systems development guidelines applicable to the IFS.
- We evaluated these controls by conducting interviews with management and staff from both the Office of the CFO and the Information Technology organization and reviewing relevant policies and procedures for the IFS update.
- Documents reviewed included the IFS Project Management Plan, the IFS Application SSP, and other documents that provided evidence of whether the IRS has adequately planned for IFS updates to support long-term goals and to mitigate risks.

Appendix II

Major Contributors to This Report

- Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
- Gwendolyn McGowan, Director
- Suzanne Westcott, Audit Manager
- Louis Lee, Acting Audit Manager
- Cari Fogle, Senior Auditor
- Wallace Sims, Senior Auditor
- Trisa Brewer, Auditor

Report Distribution List

- ❑ Acting Commissioner C
- ❑ Office of the Commissioner – Attn: Chief of Staff C
- ❑ Deputy Commissioner for Operations Support OS
- ❑ Deputy Commissioner for Services and Enforcement SE
- ❑ Chief Financial Officer OS:CFO
- ❑ Deputy Chief Information Officer for Operations OS:CTO
- ❑ Associate Chief Information Officer, Applications Development OS:CTO:AD
- ❑ 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
- ❑ Director, Privacy, Governmental Liaison, and Disclosure OS:P
- ❑ Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Glossary of Terms

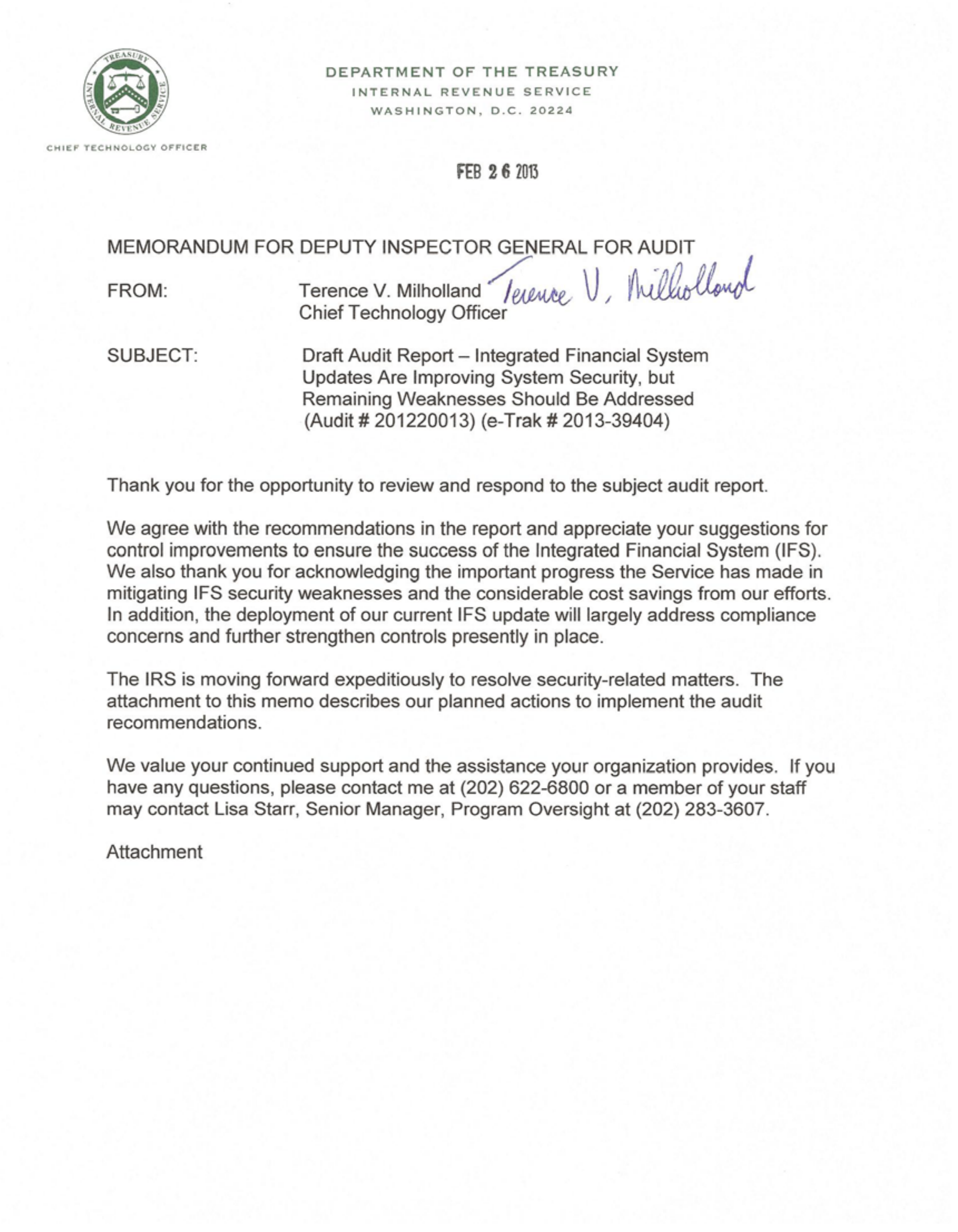
Term	Definition
Cryptographic	The art of writing or deciphering messages in code.
Encryption	The process of making data unreadable by other humans or computers for the purpose of preventing others from gaining access to its contents.
Federal Information Processing Standards	A set of standards that describe document processing, encryption algorithms, and other information technology standards for use within nonmilitary Government agencies and by Government contractors and vendors who work with the agencies.
General Support System-18	The system provides appropriately identified, authenticated, and authorized user access to tax administration business applications and provides those tax administration business applications access to data stores containing business records.
Integrated Procurement System	An Office of Management and Budget reported Financial Management System and a procurement system used to track obligations, create solicitations and awards, handle vendor files, and generate reports.
Interface	A point at which independent systems interact.
Multifactor Authentication	Multifactor authentication is achieved by combining two or three independent credentials: what the user knows (password/Personal Identification Number), what the user has (security token security or smart card), and what the user is (biometric verification).
National Institute of Standards and Technology	A nonregulatory Federal agency within the Department of Commerce that is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.

Glossary of Terms

Term	Definition
Personally Identifiable Information	Information that can be used to uniquely identify, contact, or locate a single individual or that can be used with other sources to uniquely identify a single individual.
Plan of Action and Milestones	A management process that outlines weaknesses and delineates the tasks necessary to mitigate them.
Requirement	A formalization of a need and statement of a capability or condition that a system must have or meet to satisfy a contract, standard, or specification.
Risk-Based Decision	NIST 800-53 and IRM 10.8.1 guidance allows Designated Approving Authorities to tailor security control baselines for their systems using a cost-effective, risk-based approach.
Test Case	A test case is created to specify and document the conditions to be tested and to validate that system functions meet requirements as translated into documented functional design. A test case also tests outside the normal or expected functions in order to find defects.
Two-Factor Authentication	Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. This type of authentication method also meets the definition of multifactor authentication.
Validation	Verification that something is correct or conforms to a certain standard.

Management's Response to the Draft Report

Management's complete response to the draft report is included beginning on the next page.



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

CHIEF TECHNOLOGY OFFICER

FEB 26 2013

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Draft Audit Report – Integrated Financial System Updates Are Improving System Security, but Remaining Weaknesses Should Be Addressed (Audit # 201220013) (e-Trak # 2013-39404)

Thank you for the opportunity to review and respond to the subject audit report.

We agree with the recommendations in the report and appreciate your suggestions for control improvements to ensure the success of the Integrated Financial System (IFS). We also thank you for acknowledging the important progress the Service has made in mitigating IFS security weaknesses and the considerable cost savings from our efforts. In addition, the deployment of our current IFS update will largely address compliance concerns and further strengthen controls presently in place.

The IRS is moving forward expeditiously to resolve security-related matters. The attachment to this memo describes our planned actions to implement the audit recommendations.

We value your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 622-6800 or a member of your staff may contact Lisa Starr, Senior Manager, Program Oversight at (202) 283-3607.

Attachment

Draft Audit Report – Integrated Financial System Updates Are Improving System Security, but Remaining Weaknesses Should Be Addressed (Audit # 201220013) (e-trak # 2013-39404)

RECOMMENDATION #1: The CTO should work with the CFO to implement access controls necessary to ensure IFS users are adequately restricted from IRS employee sensitive data, including SSNs and PII, until the planned long-term solution can be implemented.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. We will review Integrated Financial System (IFS) access to IRS employee sensitive data, including Social Security Numbers (SSNs) and Personally Identifiable Information (PII) and restrict access to only those users with a "need to know."

IMPLEMENTATION DATE: April 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Applications Development

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

RECOMMENDATION #2: The CTO should work with the CFO to either implement access control checks to prevent IFS users from accessing unauthorized IRS employee accounts or appropriately document this risk.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. We will conduct an analysis and remove users that do not have a "need to know," and evaluate the identified low risk to determine if a Risk Based Decision (RBD) is needed.

IMPLEMENTATION DATE: April 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Applications Development

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

RECOMMENDATION #3: The CTO should work with the CFO to update and document the status in the System Security Plan (SSP) as FIPS 140-2 certified with the next version of the IFS in Fiscal Year 2013.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. SAP and

National Institute of Standards and Technology (NIST) test centers have notified the IRS that the Federal Information Processing Standard (FIPS) 140-2 certification of the Secure Network Communication (SNC) module will be completed in late 2013. Once certification is completed, IFS will implement the new version of SNC.

IMPLEMENTATION DATE: January 1, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Applications Development

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

RECOMMENDATION #4: The CTO should work with the CFO to implement two-factor authentication and, in the short term, identify compensating authentication controls for IFS system administrators.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. The CTO will ensure IFS is included in the current program level mitigation strategy to implement two-factor authentication and identify a form of multi-factor authentication for IFS system administrators.

IMPLEMENTATION DATE: July 1, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Applications Development

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

RECOMMENDATION #5: The CTO should work with the CFO to ensure that all applicable IFS test cases include expected results to validate systems requirements were sufficiently tested.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation. The Enterprise System Test (EST) group will implement standard processes and tools for Systems Acceptance Testing (SAT) in accordance with soon-to-be-issued Internal Revenue Manual (IRM) changes. EST is working to link its Rational Quality Manager (RQM) to the RequisitePro requirements repository so that full requirements test management can be adequately and accurately documented.

IMPLEMENTATION DATE: May 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Applications Development

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

RECOMMENDATION #6: The CTO should work with the CFO to ensure that all IFS testers obtain and maintain documentation to verify actual test case results.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. The EST group will implement standard processes and tools for SAT testing in accordance with soon-to-be-issued IRM changes. EST is working to link its RQM to the RequisitePro requirements repository so that full requirements test management can be adequately and accurately documented.

IMPLEMENTATION DATE: May 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Applications Development

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