# *Annual Assessment of the Internal Revenue Service Information Technology Program*

**September 30, 2013**

**Reference Number: 2013-20-126**



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

**ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE INFORMATION TECHNOLOGY PROGRAM**

# Highlights

**Final Report issued on September30, 2013**

Highlights of Reference Number: 2013-20-126 to the Internal Revenue Service Chief Technology Officer.

## IMPACT ON TAXPAYERS

The IRS relies extensively on its computer systems to carry out the responsibilities of administering our Nation's tax laws. As such, it must ensure that its computer systems are effectively secured to protect sensitive financial and taxpayer data. In addition, successful modernization of IRS systems and the development and implementation of new information technology applications are necessary to meet evolving business needs and to enhance services provided to the American taxpayer. The IRS also needs to ensure that it leverages viable technological advances as it modernizes its major business systems and improves its overall operational environment. This includes ensuring that information technology solutions are cost-effective and support mandatory Federal requirements and electronic tax administration goals.

## WHY TIGTA DID THE AUDIT

This audit is included in our Fiscal Year 2013 Annual Audit Plan under the major management challenge of Modernization; however, it also addresses other challenge areas (*e.g.*, *S*ecurity for Taxpayer Data and Employees and Implementing the Affordable Care Act and Other Tax Law Changes). TIGTA annually assesses and reports on an evaluation of the adequacy and security of IRS information technology, as required by the IRS Restructuring and Reform Act of 1998.

## WHAT TIGTA FOUND

Since last year's assessment report, the IRS has made progress on improving information security. As a result, the Government Accountability Office made a determination to downgrade information security from a material weakness to a significant deficiency. Even still, TIGTA's reviews identified weaknesses in system access controls, audit trails, and remediation of security weaknesses.

In addition, the IRS took important steps to correct system performance issues of the Modernized e-File system to deliver a successful filing season. However, TIGTA continues to believe that the IRS's Modernization Program remains a major risk. TIGTA identified several systems development issues that should be addressed to further strengthen and support the Modernization Program. For example, our review of the Customer Account Data Engine 2 database determined that existing data quality issues prevented the downstream interfaces from being implemented. Further, the development and implementation of new systems for the Affordable Care Act present major information technology management challenges. As a result, TIGTA plans to continue its strategic oversight of this area.

Achieving program efficiencies and cost savings is an important area for the IRS. In October 2012, the IRS achieved Information Technology Infrastructure Library® Maturity Level 3 to help achieve greater efficiency delivering information technology services. While the IRS has made progress on improving program effectiveness and reducing costs, TIGTA's recent audit work involving data center consolidation, the Aircard and BlackBerry® smartphone program, and hardware and software management identified several opportunities for the IRS to achieve additional cost savings.

## WHAT TIGTA RECOMMENDED

Because this was an assessment report of the IRS's Information Technology Program through Fiscal Year 2013, TIGTA did not make any recommendations. However, TIGTA provided recommendations to the IRS in the audit reports referenced throughout this report.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 30, 2013

**MEMORANDUM FOR** CHIEF TECHNOLOGY OFFICER

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

**SUBJECT:** Final Audit Report – Annual Assessment of the Internal Revenue Service Information Technology Program (Audit # 201320019)

The overall objective of this review was to assess the progress of the Internal Revenue Services's (IRS) Information Technology Program, including modernization, security, and operations. This review is required by the IRS Restructuring and Reform Act of 1998.[1] This audit is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2013 Annual Audit Plan under the major management challenge of Modernization; however, it also addresses other challenge areas (*e.g.*, Security for Taxpayer Data and Employees and Implementing the Affordable Care Act and Other Tax Law Changes).

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

[1] Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C.,31 U.S.C., 38 U.S.C., and 49 U.S.C.).

# *Table of Contents*

# Abbreviations

| | |
|---|---|
| ACA | Affordable Care Act |
| ACIO | Associate Chief Information Officer |
| BYOD | Bring Your Own Device |
| CADE | Customer Account Data Engine |
| FATCA | Foreign Account Tax Compliance Act |
| FISMA | Federal Information Security Management Act |
| FRS | Foreign Financial Institution Registration System |
| GAO | Government Accountability Office |
| IFS | Integrated Financial System |
| IFSV | Income and Family Size Verification |
| IRS | Internal Revenue Service |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| KISAM-AM | Knowledge, Incident/Problem, Service Asset Management – Asset Manager |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| RRA 98 | Restructuring and Reform Act of 1998 |
| TIGTA | Treasury Inspector General for Tax Administration |

# Background

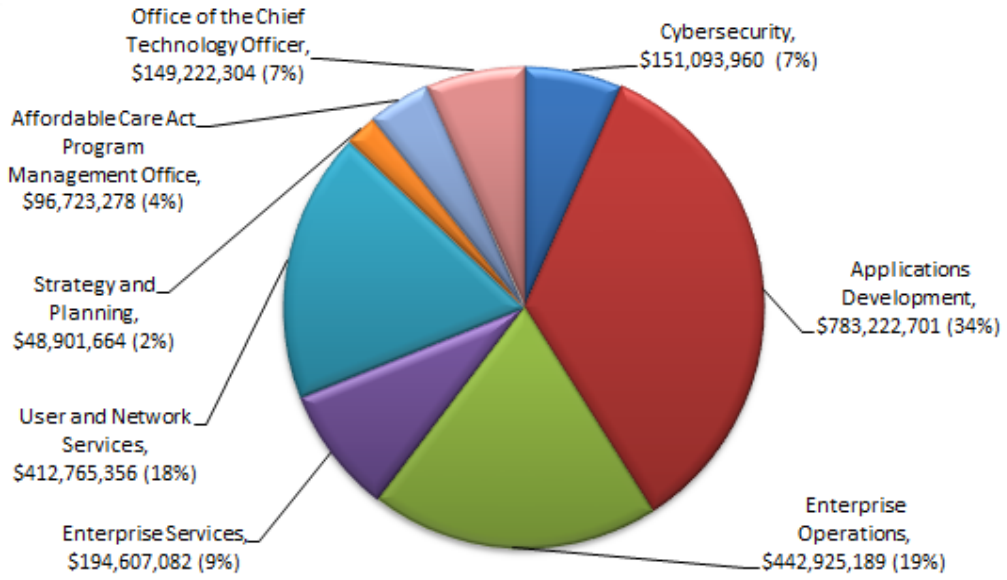
The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998 (RRA 98)[1] requires the Treasury Inspector General for Tax Administration (TIGTA) to annually evaluate the adequacy and security of the IRS Information Technology Program. This report provides our assessment of the IRS's Information Technology Program and operations for Fiscal Year 2013.

The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In Fiscal Years 2011 and 2012, the IRS collected about $2.4 trillion and $2.5 trillion, respectively, in Federal tax payments, processed hundreds of millions of tax and information returns, and paid about $416 billion and about $373 billion, respectively, in refunds to taxpayers. Further, the size and complexity of the IRS add unique operational challenges. The IRS employs more than 95,000 people in its Washington, D.C., headquarters and more than 650 offices in all 50 states and U.S. territories and in some U.S. embassies and consulates. The IRS relies extensively on computerized systems to support its financial and mission-related operations.

According to March 2013 budget information provided by the Associate Chief Information Officer (ACIO), Strategy and Planning, the IRS Information Technology (IT) organization's Fiscal Year 2013 budget was approximately $2.3 billion, which is up slightly from last year's budget of $2.2 billion. Figure 1 provides a breakdown of the Fiscal Year 2013 budget by ACIO organization. Figure 2 provides a breakdown of the Fiscal Year 2013 budget by funding source.

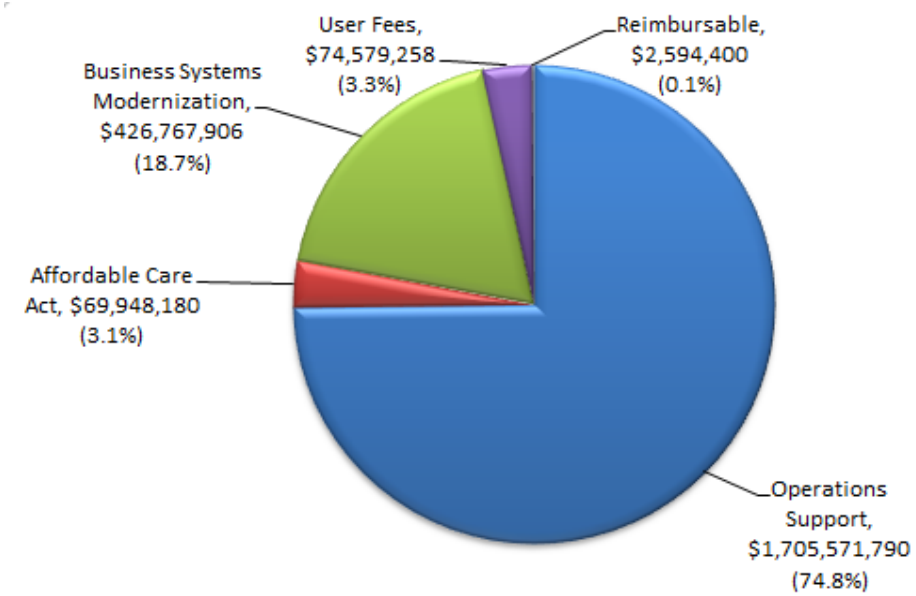
[1] Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

## Figure 1: IRS Information Technology Organization Fiscal Year 2013 Budget (by ACIO organization)




*Source: Our analysis of the IRS IT organization budget data as of March 31, 2013, provided by the ACIO, Strategy and Planning, Financial Management Services.*

## Figure 2: IRS Information Technology Organization Fiscal Year 2013 Budget (by Funding Source)




*Source: Our analysis of the IRS IT organization budget data as of March 31, 2013, provided by the ACIO, Strategy and Planning, Financial Management Services.*

The ACIO offices were restructured during Calendar Year 2013. Applications Development is now Enterprise Applications Development and will focus its efforts on systems development and maintenance, requirements analysis and development, and the delivery of multiple projects. The Enterprise Program Management Office will perform project management responsibilities for several systems development projects including the Customer Account Data Engine (CADE) 2, Return Review Program, Electronic Fraud Detection System, and Modernized e-File. In addition to the organizational restructuring, the IRS IT organization experienced turnover in some of its executive positions. For example, Enterprise Applications Development, Enterprise Services, and the Affordable Care Act (ACA)[2] Program Management Office have new executive leadership.

As of August 2013, the IRS's IT organization employed 7,303 individuals, of which 7,145 work in eight different ACIO offices:

- Enterprise Applications Development is responsible for building, testing, delivering, and maintaining integrated information applications systems, or software solutions, to support modernized systems and the production environment.
- Enterprise Program Management Office is responsible for solution architecture and program-level life cycle processes for solution development.
- Cybersecurity is responsible for ensuring IRS compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
- Enterprise Operations provides efficient, cost-effective, and highly reliable computing (server and mainframe) services for all IRS business entities and taxpayers.
- Enterprise Services enables business transformation through integrated solutions, services, and standards.
- Strategy and Planning is responsible for developing a comprehensive, integrated financial management program and strategic plan that support the programs and goals of the IT organization and for developing and implementing a capital planning and policy investment methodology and business case development.
- User and Network Services supplies and maintains all deskside (including telephone) technology, provides workstation software standardization and security management, inventories data processing equipment, conducts annual certifications of assets, provides

[2] Patient Protection and Affordable Care Act (Affordable Care Act), Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered section of the U.S. Code), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.

the Information Technology Service Desk as the single point of contact for reporting an information technology issue, and equips the Volunteer Income Tax Assistance program.

- ACA Program Management Office is responsible for managing the strategic planning, development, and implementation of new information systems in support of business requirements with regard to the ACA (our Nation's healthcare reform initiative).

The remaining 158 employees work in the Management Services business unit or support the Office of the Chief Technology Officer. The Management Services business unit partners with IRS IT leadership to define and implement human capital policies and guidance to ensure that employees are supported in the fashion necessary to deliver outstanding service. The Office of the Chief Technology Officer includes the Chief Technology Officer, two Deputy Chief Information Officers, and their staff. A Deputy Chief Information Officer serves as principal advisor to the Chief Technology Officer and provides executive direction and focus in helping the organization increase its effectiveness in delivering information technology services and solutions that align to the IRS's business priorities. Figure 3 presents the number of information technology employees in each business unit.

***Figure 3: Number of Information Technology Organization Employees by Business Unit (in descending order by number of employees)***

| Information Technology Business Unit | Number of Employees |
|---|---|
| Enterprise Applications Development | 1,978 |
| Enterprise Operations | 1,836 |
| User and Network Services | 1,660 |
| Enterprise Services | 645 |
| Cybersecurity | 370 |
| Strategy and Planning | 294 |
| Affordable Care Act – Program Management Office | 292 |
| Management Services | 144 |
| Enterprise Program Management Office | 70 |
| Office of the Chief Technology Officer | 14 |
| **Total** | 7,303 |

*Source: Treasury Integrated Management Information System as of August 2013.*

The compilation of information for this report was conducted at TIGTA offices in Austin, Texas; Chicago, Illinois; and Memphis, Tennessee, during the period May through September 2013. The information presented is derived from TIGTA audit reports issued between October 1, 2012, and September 27, 2013. We also reviewed relevant Government Accountability Office (GAO)[3] reports, congressional testimony, and IRS-issued documents relating to IRS information technology plans and issues. These previous audits and our analyses were conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and preform 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. A listing of the audit reports used in this assessment is presented in Appendix IV.

[3] See Appendix VI for a glossary of terms.

# Results of Review

## Assessment of Information Security in Information Technology Programs, Operations, and Systems Development

For Fiscal Year 2013, TIGTA designated Security for Taxpayer Data and Employees as the IRS's number one management and performance challenge. The IRS faces the daunting task of securing its computer systems against the growing threat of cyberattacks. Effective information systems security becomes essential to ensure that data are protected against inadvertent or deliberate misuse, improper disclosure, or destruction and that computer operations supporting tax administration are secured against disruption or compromise.

Protecting the confidentiality of this sensitive information is paramount. Otherwise, taxpayers could be exposed to loss of privacy and to financial loss and damages resulting from identity theft or other financial crimes. According to an Office of Management and Budget (OMB) report[4] to Congress, threats to Federal information—whether from insider threat (*e.g.*, mistakes, as well as fraudulent or malevolent acts by employees or contractors working within an organization), criminal elements, or nation states—continue to grow in number and sophistication, creating risks to the reliable functioning of our Government.

The number of cyber incidents affecting Federal Government agencies increased approximately five percent in Fiscal Year 2012, when agencies reported 48,842 cyber incidents to the U.S. Computer Emergency Readiness Team as presented in Figure 4. The Department of the Treasury reported 3,829 cyber incidents to the U.S. Computer Emergency Readiness Team in Fiscal Year 2012, as shown in Figure 5.

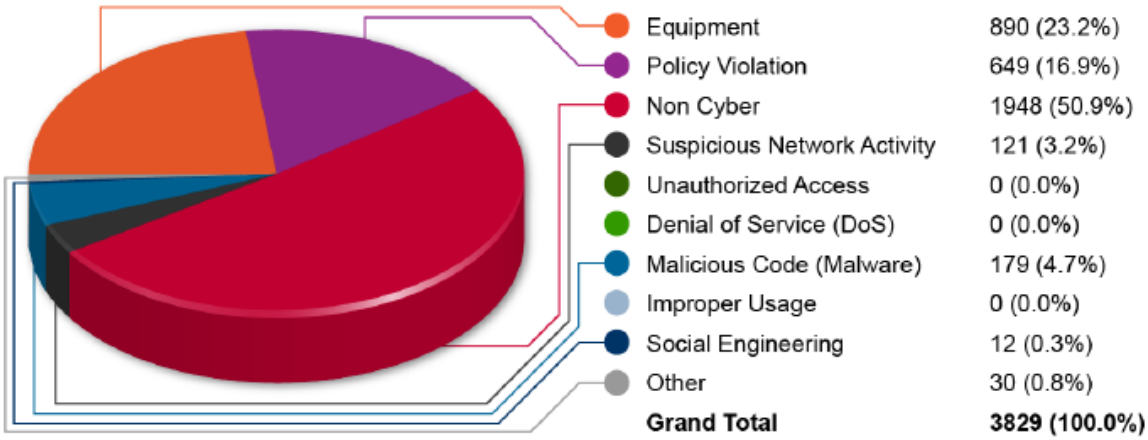
[4] OMB, *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* (March 2013). Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946-2961 (2002) (codified as amended in 44 U.S.C. §§ 3541–3549).

## Figure 4: Cyber Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies in Fiscal Year 2012

| Incident Category | Number of Incidents | Percentage of Total Incidents |
|---|---|---|
| **Non-Cyber** (Personally Identifiable Information spillage or mishandling for hardcopy or printed material) | 13,685 | 28.0% |
| **Policy Violations** (mishandling of data in storage or transit) | 9,194 | 18.8% |
| **Malicious Code** (malware) | 8,847 | 18.1% |
| **Equipment** (lost or stolen equipment) | 8,057 | 16.5% |
| **Suspicious Network Activity** | 2,918 | 6.0% |
| **Social Engineering** (fraudulent websites or attempts to entice users to provide sensitive information) | 2,459 | 5.0% |
| **Improper Usage** (rule of behavior violations) | 690 | 1.4% |
| **Unauthorized Access** (unprivileged users gain control of system or resource) | 347 | 0.7% |
| **Denial of Service** (successful Denial of Service attacks) | 27 | 0.05% |
| **Other** (low frequency incidents, such as unconfirmed third-party notifications, failed attacks, or incident with unknown causes) | 2,618 | 5.4% |
| **Total** | 48,842 | 100.0% |

*Source: The OMB's Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002, dated March 2013.* Percentages do not add to 100 percent due to rounding.

## Figure 5: Cyber Incidents Reported to the U.S. Computer Emergency Readiness Team by the Department of the Treasury in Fiscal Year 2012




*Source: The OMB's Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002, dated March 2013.*

The Office of Cybersecurity within the IRS IT organization is responsible for protecting taxpayer information and the IRS's electronic systems, services, and data from internal and external cybersecurity threats by implementing world-class security practices in planning, implementation, risk management, and operations. In September 2012, the IRS issued an updated version of the Information Technology Program Plan.[5] The plan addresses current information technology security issues and communicates to the IRS community the security initiatives to resolve the Information Security Material Weaknesses,[6] comply with Federal security guidelines, and reduce security risk.

The plan uses the 13 information security elements contained in National Institute of Standards and Technology (NIST) Special Publication 800-100[7] as the framework for the IRS Information Security Program. Under each program element, there is a brief description of its scope, the current environment, and an encapsulation of ongoing security initiatives. The initiatives represent the actions that serve as a roadmap and a basis for benchmarking performance. The document captures what the IRS is doing to continuously improve its security posture.

Since Security for Taxpayer Data and Employees is the highest management and performance challenge, we performed audits to assess the IRS's efforts to protect its information systems and taxpayer data. Some of these audits focused solely on what the IRS was doing to mitigate its information security risks. We also had audits whose objectives were primarily focused on management of systems development or information technology operations/projects but included security subobjectives. Therefore, some of the audits discussed below appear in two sections of this report.

## The IRS determined that information security should no longer be designated as a material weakness but as a significant deficiency

In Calendar Year 1997, the IRS designated information security as a material weakness. The information security material weakness compromises the accuracy and availability of the IRS financial information and places sensitive information regarding IRS operations and taxpayers at risk. In our 2012 annual assessment report,[8] the IRS stated that it closed or completed corrective actions for eight of the nine information security material weakness components and planned to close the remaining component by January 2014. During Fiscal Year 2013, the IRS revised its plans to close the remaining component by September 2014.

In November 2012, the GAO reported[9] that during Fiscal Year 2012, the IRS continued to make important progress in addressing numerous deficiencies in its information security controls over

[5] The IRS issued the first plan in September 2009.
[6] Formerly called computer security material weaknesses.
[7] NIST, NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers* (Oct. 2006).
[8] TIGTA, Ref. No. 2012-20-120, *Annual Assessment of the Internal Revenue Service Information Technology Program* p. 19 (Sept. 2012).
[9] GAO, GAO-13-120, *IRS's Fiscal Years 2012 and 2011 Financial Statements* Highlights page (Nov. 9, 2012).

its financial reporting systems. As a result, GAO considers information security, previously reported as a long-standing material weakness, to be a significant deficiency that continues to warrant the attention of those charged with governance of the IRS.

In addition to the GAO's determination to downgrade information security to a significant deficiency, the IRS provided a briefing and documents to TIGTA in August 2013 that detailed its other efforts and accomplishments to support the downgrade determination, which included:

- The IT organization's work and its progress on the Information Security Material Weakness remediation plan; GAO's top nine concerns, which include specific financial systems, security controls, and reliability on the IRS's monitoring of internal controls; review of external systems that provide data in support to the IRS's financial statements; and the annual Federal Information Security Management Act (FISMA)[10] assessment on security metrics.
- The Chief Financial Officer's work on interim OMB Circular A-123[11] testing to evaluate internal controls effectiveness over financial reporting, annual assurance statements, and IRS materiality determinations to better understand financial process workflows, systemic and operational risks, mitigation steps, monitoring, and controls.

Unlike previous years, the IRS did not request that TIGTA initiate a review to validate its efforts to support the downgrade determination. As a result, we are not in a position to concur or disagree with the determination. However, the information provided appears to be very comprehensive and detailed to support the downgrade.

In March 2013, the GAO reported[12] that despite the progress made by the IRS, the GAO still found access control deficiencies that reduced security over systems:

- Controls for identifying and authenticating users were inconsistently implemented.
- Inconsistent use of data encryption limited protection of sensitive information.
- Visitor physical access cards to restricted areas at one computing center provided unauthorized access to other restricted areas within the center, and regular reviews of individuals with an ongoing need to access restricted areas at one of the three computing centers were not being conducted monthly to ensure that such access was still appropriate.

[10] Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946-2961 (2002) (codified as amended in 44 U.S.C. §§ 3541-3549)
[11] OMB, OMB Circular No. A-123 (Revised), *Management's Responsibility for Internal Control* (Dec. 2004)
[12] GAO, GAO-13-350, *IRS Has Improved Controls but Needs to Resolve Weaknesses* pp. 11-13, 15, and 18 (March 15, 2013).

The GAO report continued by stating that a key reason for the information security weaknesses in the IRS's financial and tax-processing systems was that, although the IRS has developed and documented a comprehensive agencywide information security program, it had not effectively implemented certain elements of its information security program. For example (not all inclusive):

- Inconsistent system configurations resulted in preventable vulnerabilities. Eight of 19 servers reviewed lacked a security setting to enforce standard configuration updates, resulting in weaker controls for these servers.
- The agency's automated change management process could be circumvented because individuals had privileges that allowed them to make changes to mainframe applications.
- The IRS did not always apply patches to its systems in a timely manner. For example, a database supporting tax account processing had not been patched for several months despite the issuance of critical patches, and another database used for operations support was missing key patches. IRS officials stated that these situations resulted from restrictions on making changes to systems during the tax filing season. Other servers were also not patched due to system performance problems.
- The IRS's audit and monitoring policies and procedures did not comprehensively address users accessing files used by one processing environment from a different environment.
- The IRS's security standards for systems that support tax processing and financial management contained information that was several years out of date, which had resulted in less secure system configurations.

The GAO also reported that the IRS had a process in place for evaluating and tracking remedial actions, but it did not always effectively validate that corrective actions had been taken or whether the actions addressed the weakness. The Internal Revenue Manual requires that the IRS track the status of resolution of all weaknesses and verify that each weakness has been corrected before closing it. During the GAO audit period, March 2012 through March 2013, the IRS informed the GAO that it had addressed 58 of the 118 previous GAO information system security recommendations that remained unresolved at the end of the prior audit. However, the GAO determined that 13 (about 22 percent) of the 58 had actually not yet been fully resolved.[13] The GAO previously made a recommendation in March 2007 to the IRS for it to revise its verification process to ensure that actions are fully implemented.[14]

During a similar review to determine whether closed corrective actions to security weaknesses and findings reported by TIGTA have been fully implemented, validated, and documented as

[13] GAO, GAO-13-350, *IRS Has Improved Controls but Needs to Resolve Weaknesses* p. 22 (March 15, 2013).
[14] GAO, GAO-07-364, *Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service* p. 23 (March 30, 2007).

implemented,[15] we found that eight (42 percent) of the 19 planned corrective actions had not been fully implemented and should not have been closed. These planned corrective actions involved systems containing taxpayer data. For the eight planned corrective actions, we found the following internal control deficiencies.

- For five planned corrective actions, the supporting documentation did not fully support the closed corrective action. In the remaining three planned corrective actions, we were not provided any documentation to support the closure of the corrective action.
- For four planned corrective actions, the update and closure form did not include the appropriate executive approval.
- For all eight planned corrective actions, the office responsible for monitoring internal control weaknesses did not audit the corrective actions to ensure implementation and proper closure.

Our audit report provided six recommendations to address these issues.

The Federal Government has a duty to secure Federal information and information systems and protect against threats (*e.g.*, unauthorized access to systems or data) posed by security weaknesses. The FISMA requires agencies to provide information security protections commensurate with risks and their potential harms to Federal information. We completed our mandatory review of the FISMA[16] and found that the IRS generally complied with nine of 11 requirements on its information security programs and practices. Based on our and the GAO's recent reports, the IRS should improve its efforts to promptly resolve findings and document the actions taken to close the corrective actions.

## ***Weaknesses in security of operations programs, Internet access, and new technologies***

Information security services and products are essential elements of an organization's information security program. The selection of services and products is an integral part of the design, development, and maintenance of an information technology security infrastructure that ensures confidentiality, integrity, and availability of mission-critical information. Information security services and product acquisition encompasses the selection of services and products that are used as operational or technical security controls for the IRS's information technology systems. The following are the audits that reported information security issues.

***Trusted Internet Connections*:** This initiative is intended to improve cybersecurity and the security of Federal information systems. The primary goals are (1) to consolidate and secure

[15] See Appendix IV, Ref. No. 2013-20-117.
[16] See Appendix IV, Ref. No. 2013-20-128.

Federal agency external connections using a common set of security controls and (2) to improve the Federal Government's incident response capability.

During our review of the IRS's implementation of this initiative,[17] we found that in February 2013 the Department of Homeland Security conducted a Cybersecurity Capability Validation assessment of two of the three IRS Trusted Internet Connections and reported that each met 68 (92 percent) of the 74 capabilities required. Although the IRS has made good progress implementing the requirements for this initiative, our review revealed areas where improvements could strengthen security.

- The IRS was not capturing audit logs of administrator activity on servers, firewalls, or routers. Audit logs containing information on activities by administrators on Trusted Internet Connection devices provide a means to establish individual accountability. Without an effective system for the capture and review of administrator activity, accountability for actions taken on equipment cannot be established and unauthorized activity may go undetected.
- A Data Loss Prevention system designed to detect potential data breach transmissions and prevent them by monitoring, detecting, and blocking sensitive data while **in use** (endpoint actions), **in motion** (network traffic), and **at rest** (data storage) was not in place.
- The IRS does not have a sufficient number of operational employees with appropriate security clearances for handling classified information.
- The IRS does not have a Sensitive Compartmented Information Facility[18] at any of its three Trusted Internet Connection locations as required. A Sensitive Compartmented Information Facility is a secured area within a building that is used to process sensitive compartmented information.
- Although the IRS has generally configured firewalls and routers securely, we found instances where firewalls or routers were not configured in compliance with required baseline configuration settings.
- The IRS has eight servers running outdated versions of the operating system. Outdated operating systems increase the risk of attacks that exploit known vulnerabilities, resulting in unauthorized access or loss of IRS data.

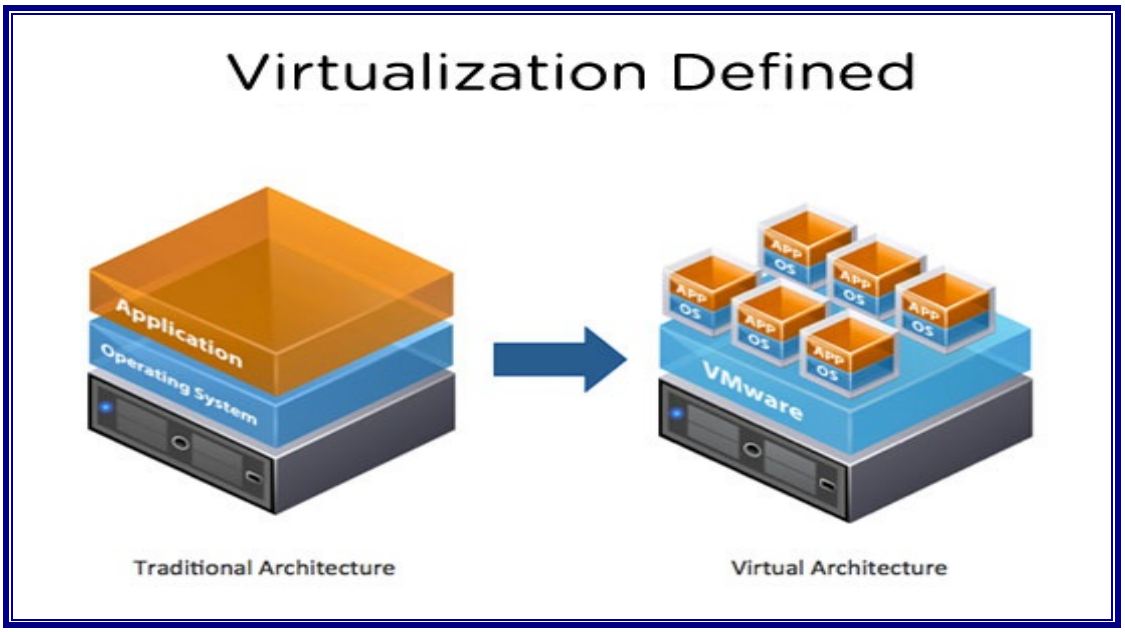
Our audit report provided six recommendations to address these issues.

[17] See Appendix IV, Ref. No. 2013-20-107.
[18] Office of the Director of National Intelligence, Intelligence Community Directive Number 705, *Sensitive Compartmented Information Facilities* (May 26, 2010), established the uniform physical and technical requirements with which facilities must comply in order to be accredited as a Sensitive Compartmented Information Facility.

***Treasury Enhanced Security Initiatives*:** This project was implemented to enable the IRS to comply with the OMB's mandate[18] to continuously monitor security settings on computer workstations and identify and address security settings that have been altered. We found[19] that the project, which includes the continuous monitoring tool for workstation security, will address several computer security weaknesses on employee workstations. Our audit report did not include any security recommendations.

***Virtualized Environment*:** Server virtualization is a technology that allows several "virtual" servers to run on one physical host server (hereafter referred to as "host"), as illustrated in Figure 6. The technology helps organizations utilize their existing hardware infrastructure more effectively.

**Figure 6: Illustration of Server Virtualization**




*Source:* TIGTA, Ref. No. 2013-20-106, *Automated Monitoring Is Needed for the Virtual Infrastructure to Ensure Secure Configurations* p. 1 (Sept. 2013).

Our review of the security over the IRS's virtualized environment[20] found that the IRS developed a comprehensive policy that establishes the minimum security controls to prevent unauthorized access to IRS information systems hosted in its virtualization environment. The IRS has been

[18] OMB, OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems* (March 22, 2007).
[19] See Appendix IV, Ref. No. 2013-20-016.
[20] See Appendix IV, Ref. No. 2013-20-106.

successful in its continual efforts to expand its virtual server environment. As a result, the IRS improved server efficiency and realized significant cost savings. However, we found that:

- Security configuration settings on virtual hosts were not in accordance with IRS policy and the hosts were not timely patched to address known security vulnerabilities.
- Twelve (43 percent) of 28 required security controls on 16 hosts we tested were failed by three or more hosts. In addition, 10 (63 percent) of the 16 hosts were missing a total of 48 security patches.
- Audit logs capturing administrator activity on certain hosts and servers were not being collected and reviewed as required. Without the proper capture and review of administrator activity, accountability for actions taken on hosts cannot be established and unauthorized activity may go undetected. Moreover, the IRS could have a security breach in the virtual environment and not be aware of it.

Our audit report provided three recommendations to address these issues.

***eAuthentication*:** RRA 98 requires the IRS to allow taxpayers to access tax account information online. The objective of the IRS eAuthentication Project is to design and build a common service to proof and register individuals and to provide and validate credentials for ongoing system access using the Internet.

During our review,[21] we determined that eAuthentication Release 1 has limited audit reporting functionality. While actions taken by users within the eAuthentication application are identified by user identification, these actions are not associated to a user's actual name and therefore cannot be associated to a specific taxpayer. In addition, the user information captured by the application may contain Personally Identifiable Information and therefore must be encrypted when it is stored on the server. The IRS does not have a mechanism to make the encrypted data readable, but it does have a tool that can log auditable events for each taxpayer transaction that does track the individual with his or her Social Security Number. These transactions are available for designated security and audit individuals but not generally available for management review.

For eAuthentication Release 2, the project team plans to use a suite of products to meet the reporting requirements. This capability should enable the project team to provide stakeholders access to more useful reports for both customer usage reporting and process effectiveness purposes. Without adequate reporting functionality, the IRS is only able to see minimal details about taxpayers using the eAuthentication application. The expanded reporting functionality should provide the IRS with application-specific reports, taxpayer account reports, and system infrastructure reports. Our audit report provided one recommendation to address this issue.

[21] See Appendix IV, Ref. No. 2013-20-127.

***Bring Your Own Device (BYOD) Pilot Project*:** BYOD is a popular trend in mobile computing that allows users to access network resources on their personal mobile devices, such as smartphones. The IRS is currently piloting a limited BYOD effort[22] that allows BYOD participants access to e-mail, calendaring, and some web-based internal IRS applications, but technical limitations prevent users from interfacing with many IRS internal systems. One drawback of a BYOD program is that BYOD devices are subject to distinctive threats and often need additional protection because their nature generally places them at higher exposure to threats than other devices, *e.g.*, desktop and laptop devices used only within the organization's facilities and on the organization's networks.[23]

During our review of the IRS's BYOD Pilot Project,[24] we found that the IRS considered and implemented security measures when it implemented its BYOD pilot; however, increased attention is still needed to address security concerns related to the participants in the pilot.

- Because the BYOD pilot takes place in the production environment, standard security controls should apply. The IRS is unable to fully implement Federal and IRS security guidance with respect to BYOD devices. Thus, we believe BYOD devices should only be allowed to access e-mail functions and should not be allowed to access other IRS network resources.
- The IRS allows devices based on the Android® operating system to participate in the BYOD pilot, even though these devices are more subject to malware than the Apple® devices tested in earlier phases.
- Access audit trails are not retained or reviewed in compliance with IRS policy. If audit trails are not available or are not reviewed, unauthorized accesses may occur and not be detected.
- BYOD participants are not receiving periodic refresher training specific to BYOD threats and recommended security practices. Without periodic training, the IRS has no assurance that users are knowledgeable about elevated loss and theft rates of smartphones, how to identify potentially dangerous applications, and other mobile device security issues.

Our audit report provided four recommendations to address these issues.

[22] The IRS currently refers to its BYOD pilot as a "technology demonstrator," which is meant to distinguish BYOD as a provisional initiative or prototype, thus differentiating it from formal pilots or large-scale information technology initiatives for which the IRS uses a well-established investment decision and enterprise life cycle methodology. The word "pilot" is used in the report in a general sense for ease of understanding.
[23] NIST, NIST Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013).
[24] See Appendix IV, Ref. No. 2013-20-108.

## Security and systems development

According to a March 2013 GAO report,[25] the IRS applies information technology to help achieve its missions and provide information and services to the public, but extensive reliance on computerized information also creates challenges in securing that information from various threats. Information security is especially important for government agencies, where maintaining the public's trust is essential. As a component of overall system security, security controls should be addressed when developing a new system (*e.g.*, during the design and requirements development phases) or revising an existing system to mitigate information security risks.

The GAO describes these controls as general controls (security management, access controls, configuration management, segregation of duties, and contingency planning), business process application controls (input, processing, output, master file, interface, and data management system controls), and user controls (controls performed by people interacting with information systems). Without proper safeguards, computer systems are more vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. During this reporting period, information security control weaknesses were identified in several of our systems development audits.

***Integrated Financial System (IFS)*:** The IRS's core financial system annually accounts for approximately $12 billion in operational funds. During our review,[26] we found that updates for the system were completed as planned to address compliance for specific information technology security controls. For example, one update provided data encryption and eliminated security weaknesses in the Citrix® and Windows® 2000 environments no longer supported by the vendor. However, improvements are needed to better ensure that remaining system security weaknesses are addressed. We reported that:

- Users have access to Personally Identifiable Information without a business need. In addition, 110 users have access to the 1099 and W-2 data for some IRS employees and vendors without reasonable access control checks in place. Such controls would identify or prevent a user viewing another IRS employee's tax information.
- The data encryption tool complies with Federal guidance, but it is not yet certified for validation.
- The system does not yet provide for multifactor authentication.

Our audit report provided four recommendations to address these issues.

[25] GAO, GAO-13-350, *IRS Has Improved Controls but Needs to Resolve Weaknesses* pp. 3, 4, and 6 (March 15, 2013).
[26] See Appendix IV, Ref. No. 2013-20-030.

***Income and Family Size Verification (IFSV) Project*:** The IFSV Project is one of six core ACA Program projects being implemented in October 2013. It will support open enrollment by verifying income and family size for individuals requesting eligibility for the Advanced Premium Tax Credit for health insurance. During our review,[27] we found that, within a new iterative system development approach, the IRS had developed a security plan intended to protect taxpayer data and also incorporated FISMA and NIST guidelines. We did not make any recommendations directly related to information security controls.

***Premium Tax Credit Project*:** Provisions of the ACA include a refundable credit, referred to as the Premium Tax Credit, for eligible individuals to assist with paying health insurance premiums. In addition, the IRS's implementation plan for ACA Exchange provisions includes providing information that will support eligibility and enrollment functions. Like the IFSV Project, the Premium Tax Credit Project is managed under the IRS ACA Program. The project includes all processes related to the development of the Premium Tax Credit Computation Engine in support of the implementation of Advanced Premium Tax Credit capabilities. During our observation of security testing,[28] Cybersecurity management ensured that tests were conducted in accordance with the NIST requirements and Internal Revenue Manual guidelines. However, the configuration baselines and settings for specific controls were not adequately tested. Because Cybersecurity did not stipulate specific corrective actions for failed tests and known risks associated with the component misconfiguration, we could not verify that known risks associated with component misconfigurations have been consistently addressed for the project.

We reported that change management guidelines were also not consistently followed to withdraw approved baseline security requirements. Specifically, the change request and impact assessment prepared to withdraw the security requirements only included one of the seven baseline requirements removed. If change management guidelines are not properly followed, management may not be able to determine the potential impact of changed requirements on the security controls for the Premium Tax Credit Computation Engine, which could negatively affect functionality or delay deployment of the Premium Tax Credit Project. Our audit report provided two recommendations to address these issues.

***Knowledge, Incident/Problem, Service Asset Management – Asset Manager (KISAM-AM)*:** The KISAM-AM is the sole authoritative source and official inventory record for all information technology assets within the IRS [with the exception of information technology software assets (to include software and software licenses)]. We conducted tests to ensure that sufficient system controls were in place to protect access to the KISAM system data.[29] Our tests determined that the KISAM-AM application, database, and operating system complied with the IRS's password

[27] See Appendix IV, Ref. No. 2013-23-034.
[28] See Appendix IV, Ref. No. 2013-23-119.
[29] See Appendix IV, Ref. No. 2013-20-089.

management requirements. However, our review of the switch user log (audit log) identified three individuals who accessed the KISAM system database using a system account and without a need to know. These three individuals are not database administrators and should not have access to the database system account or the password for the account. This suggests that a security weakness exists within the KISAM-AM system infrastructure, and we cannot be assured that the data within the KISAM-AM system is protected from accidental or malicious altering. Our audit report provided a recommendation to address this issue.

***Foreign Financial Institution Registration System (FRS)*:** Development and implementation of the FRS is underway to support requirements of the Foreign Account Tax Compliance Act (FATCA).[30] If successful, the FRS would help to significantly improve taxpayer compliance internationally and thus enhance IRS tax administration under the FATCA provisions. Through the FRS, Foreign Financial Institutions will register and provide offshore account information reporting to the IRS. Our audit[31] found that security controls need improvement to ensure long-term success for this new international system. Specifically, the IRS needs to ensure that system test plans are completed so that all security requirements, controls, and test cases are identified, traced, and tested. Without improvements in risk mitigation controls during development of this new system, the IRS may not be able to adequately determine whether:

- The Security Controls Assessment Test Plan included adequate security controls prior to deployment of the FRS.
- System security controls aligned with NIST guidance, IRS requirements and testing manuals, and other applicable standards.
- The Security Controls Assessment Test Plan contained test cases for all the system security requirements.
- The test cases were mapped to the security controls.

Our audit report provided one recommendation to address this issue.

***CADE 2 database*:** The CADE 2 program implements a single data-centric solution that provides daily processing of taxpayer accounts. The first phase is Transition State 1, which establishes the target CADE 2 data model and database and uses the data to provide individual taxpayer account information to select systems. The Transition State 1 solution will also implement required security controls and begin to address identified security weaknesses.

Our review of security controls in the system development activities for the CADE 2 database[32] found that the lack of security systems integration prevents transaction-level tracking of employee access to the CADE 2 database. The CADE 2 – Corporate Files Online/Individual

[30] Pub. L. No. 111-147, Subtitle A, 124 Stat 71, 96-116 (2010)(codified in scattered sections of 26 U.S.C.).
[31] See Appendix IV, Ref. No. 2013-20-118.
[32] See Appendix IV, Ref. No. 2013-20-125.

Master Files Online systems interface uses two security systems to provide user authentication and access control and auditing functionality.

We attempted to trace a transaction from a Corporate Files Online/Individual Master Files Online system data call to the CADE 2 database and were unable to follow the transaction once it passed through the Data Access Service system account. Not having transaction-level tracking of employee access to the CADE 2 database can allow unauthorized access to taxpayer data to go undetected by audit logs. Our audit report provided one recommendation to address this issue.

## Privacy

Within the Federal Government, privacy is defined as an individual's expectation that his or her personal information collected for official Government business will be protected from unauthorized use and access. During our review[33] of the IRS's implementation of the privacy provisions of the E-Government Act of 2002,[34] we found that the IRS implemented the Privacy Impact Assessment Management System in December 2011 to automate the process of completing Privacy Impact Assessments in a more efficient and less time-consuming way. We determined that the Privacy Compliance office analysts effectively conducted in-depth quality reviews of completed Privacy Impact Assessments submitted by system and program owners. Further, the Privacy and Information Protection office complied with the updated privacy reporting requirements by preparing and submitting required reports to the Department of the Treasury.

Despite its commitment toward privacy and improvements from our prior review, the IRS continues to face challenges in meeting legislative privacy requirements. Specifically, we found that Privacy Impact Assessments:

- Had not been completed or updated for all systems or customer surveys where taxpayer or employee information have been collected and maintained.
- Had not been posted to the IRS's public website.
- May not have been completed and submitted for internal SharePoint collaboration sites.

Our report provided 11 recommendations to address the privacy issues.

To summarize, although the IRS may have closed many of its information security weaknesses identified in the past, we and the GAO continue to identify similar or new security weaknesses in our recent audits of information technology initiatives and operations. For example, improper security configuration control settings were found during the Premium Tax Credit, Treasury Internet Connections initiative, and Virtualized Environment audits. Issues with capturing and reviewing audit trail logs were found during the Treasury Internet Connections initiative,

[33] See Appendix IV, Ref. No. 2013-20-023.
[34] Pub. L. No. 107-347, § 208, 116 Stat. 2899 (2002).

Virtualized Environment, BYOD, and CADE 2 audits. These findings, along with continued cyberattacks against Government systems, bring us to conclude that the IRS needs to continue efforts to reduce its security vulnerabilities.

## Systems Development Projects to Support Modernization, Tax Legislation Changes, and Tax Compliance Initiatives

The Business Systems Modernization Program (hereafter referred to as the Modernization Program) is a major undertaking and involves a complex effort to modernize IRS technology and related business processes. When the program stood up, estimates were that this initiative would last up to 15 years. Now in its 15th year and with IRS budget information from March 2013 indicating a budget of over $426 million, the Modernization Program continues to make improvements in electronic tax administration with projects like the Modernized e-File and CADE 2.

The IRS's modernization efforts also include modernizing taxpayer applications that allow taxpayers to communicate with the IRS through the Internet, developing a shared infrastructure and common business service solutions usable across multiple modernization projects, and ensuring that systems solutions meet business needs and effectively integrate modernization projects and programs. Building on last year's organizational shift incorporating modernization into the overall portfolio, the IRS's IT organization renamed the Modernization Program Management Office and Applications Development organization to the Enterprise Program Management Office and Enterprise Applications Development, respectively. Successful modernization of IRS systems and the development and implementation of new information technology applications is necessary to meet evolving business needs and ensure the long-term viability of IRS tax processing systems.

In February 2013, the GAO reported that it removed the Modernization Program from its High Risk List.[35] The GAO removed this program because:

- Progress was made in addressing significant weaknesses in information technology and financial management capabilities.
- The IRS delivered the initial phase of its cornerstone tax processing project and began the daily processing and posting of individual taxpayer accounts in January 2012. This enhanced tax administration and improved service by enabling faster refunds for more taxpayers, allowing more timely account updates, and providing faster issuance of taxpayer notices.

[35] GAO, GAO-13-359T, *GAO's High Risk Series – An Update*, p.2 (Feb. 2013).

- The IRS has put in place close to 80 percent of the practices needed for an effective investment management process, including all of the processes needed for effective project oversight.
- The IRS had embarked on an effort to improve its software development practices using the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model Integration, which calls for disciplined software development and acquisition practices that are considered industry best practices. In September 2012, the IRS's application development organization reached Capability Maturity Model Integration Maturity Level 3, a high achievement by industry standards.

Although the GAO removed the Modernization Program from its High Risk List, we believe the program remains a high risk and major management challenge for the IRS because of the needs for improvements in information technology practices and performance. Some of these areas of improvement are discussed below.

To help meet its business needs, the IRS IT organization developed the Integrated Release Plan. This document is an evolving business planning tool that merges information about the technology roadmap, release/capacity management, and budget. According to the IRS's IT organization, the objectives of the Integrated Release Plan include:

- Supporting continuous engagement with the non–information technology side of the IRS.
- Improving alignment of information technology investments, service, and delivery with IRS strategic goals.
- Facilitating enterprisewide "early warning" of risks and issues on essential projects.
- Enhancing situational awareness and enabling the IT organization to manage risks, resource contention, and tradeoff decisions.

## The Modernized e-File system helps deliver the filing season

The Modernized e-File system is the IRS electronic filing system that enables real-time processing of tax returns while improving error detection, standardizing business rules, and expediting acknowledgements to taxpayers. It is a critical component to meet the needs of taxpayers, reduce taxpayer burden, and broaden the use of electronic interactions. The IRS modified the scope for Modernized e-File Release 8 to focus on correcting the performance issues identified during Release 7 and delayed the implementation of new business taxpayer forms to Release 9.

During last year's review of the Modernized e-File system,[36] we recommended that the IRS defer the retirement of the Legacy e-File system. During this year's review,[37] we found that the IRS took important steps before the 2013 Filing Season to correct the system performance issues that occurred during the 2012 Filing Season. The IRS increased the Release 8 test requirement for the Performance Evaluation Testing Environment database by implementing a copy of the Modernized e-File system production database. This production-sized database contained 23.1 million records, up from the 6.6 million records required for Release 7 testing. By doing so, the IRS leveraged data from the production-sized database to help it obtain the required amount of data needed to execute sustained performance testing. The IRS also implemented enhancements to improve the delivery of files to downstream systems and increased the capacity of the portal to guard against a decrease in overall performance.

### *Development of a new Return Review Program system is necessary to mitigate fraud risks affecting the IRS's environment for electronic tax administration*

The IRS is developing a new Return Review Program system to implement its emerging business model for a coordinated criminal and civil tax noncompliance system. Once developed and implemented, the new system will significantly enhance the IRS's capabilities to prevent, detect, and resolve tax refund fraud, including identity theft. The IRS's current system used to detect fraud is the Electronic Fraud Detection System. At the time of our review, the IRS had determined that the Electronic Fraud Detection System, which was implemented in 1994, is outdated and would be inefficient to maintain, upgrade, or operate beyond Calendar Year 2015. Successful implementation of the new Return Review Program system would increase the dollar amount of fraudulent tax refunds identified annually.

During our review of the Return Review Program,[38] we found that the roles for program-level governance were not yet established and that the key role of system integrator was not documented or clearly communicated. From January to December 2012, prototype activities were conducted to validate that technology product solutions integrated successfully. However, Return Review Program Prototype Management Plans, critical systems development products, were not completed or approved by major stakeholders before significant resources were committed. Uncertainty about the systems development path for the Return Review Program and the absence of Enterprise Life Cycle guidance for prototypes hindered initial systems development efforts. Further, alternative commercial software products were not fully considered prior to selecting technology solutions for the Return Review Program system. Our

[36] TIGTA, Ref. No. 2012-20-121, *Despite Steps Taken to Increase Electronic Returns, Unresolved Modernized E-File System Risks Will Delay the Retirement of the Legacy e-File System and Implementation of Business Forms* (Sept. 2012).
[37] See Appendix IV, Ref. No. 2013-20-029.
[38] See Appendix IV, Ref. No. 2013-20-063.

report provided six recommendations to address our findings on initial development activities for the Return Review Program system.

The National Taxpayer Advocate's Annual Objectives Report to Congress[39] recently cited concerns about the implementation of the Return Review Program system. The report stated:

> *...the IRS is now forced to consider non-deployment or a limited deployment of RRP* [Return Review Program]. *On January 15, 2013, the Information Technology division reported that it did not have enough resources available to bring RRP online by the January 1, 2015, deadline. Even with the additional resources, the IRS would still need another year (until January 1, 2016) to complete the system.*
>
> *Not deploying the RRP as intended could impose significant harm and cost on both the IRS and the public. An unexpected failure of the EFDS system* [Electronic Fraud Detection System] *would force the IRS to decide whether to stop issuing refunds until the system could be repaired, or issue billions of dollars in potentially fraudulent refunds without screening. In addition, as EFDS becomes harder to update and maintain, it could erroneously stop an increasing number of valid refunds. The lack of automation to handle administrative adjustments and actions is straining the IRS's limited resources as fraud and identity theft grow and staffing declines.*

## The FATCA aims to improve international compliance

The FATCA is an important development in the U.S. efforts to improve tax compliance involving foreign financial assets and offshore accounts.[40] Changes required by the FATCA will: (1) combat tax evasion by U.S. persons holding investments in offshore accounts, (2) expand the IRS's global presence, (3) pursue international tax and financial crimes, (4) fill a gap in the IRS's information reporting system, and (5) generate additional enforcement revenue. The Department of the Treasury issued the final FATCA regulations on January 28, 2013.

During our review,[41] we found that the IRS is developing the FRS within its new Enterprise Life Cycle Iterative Path systems development and testing process. The initial system release was substantially developed and nearing deployment when the IRS terminated the effort in November 2012. Following new Department of the Treasury regulations, changes with intergovernmental agreements, and new processes needed to implement the FATCA, the IRS was unable to fully utilize the initial system. Subsequently, the IRS modified and expanded the scope of the system requirements. The major redesign and initiation of a new development effort

[39] National Taxpayer Advocate, *Fiscal Year 2014 Objectives Report to Congress* (June 2013).
[40] The FATCA legislation was enacted as part of the Hiring Incentives to Restore Employment Act; Pub. L. No. 111-147, 124 Stat. 71 (2010).
[41] See Appendix IV, Ref. No. 2013-20-118.

was necessary because the IRS did not sufficiently develop requirements for the initial FRS as needed for new system development. We identified a potential inefficient use of resources of $2.2 million based on the IRS exceeding its original cost estimate of $14.4 million to develop and deploy the FRS.

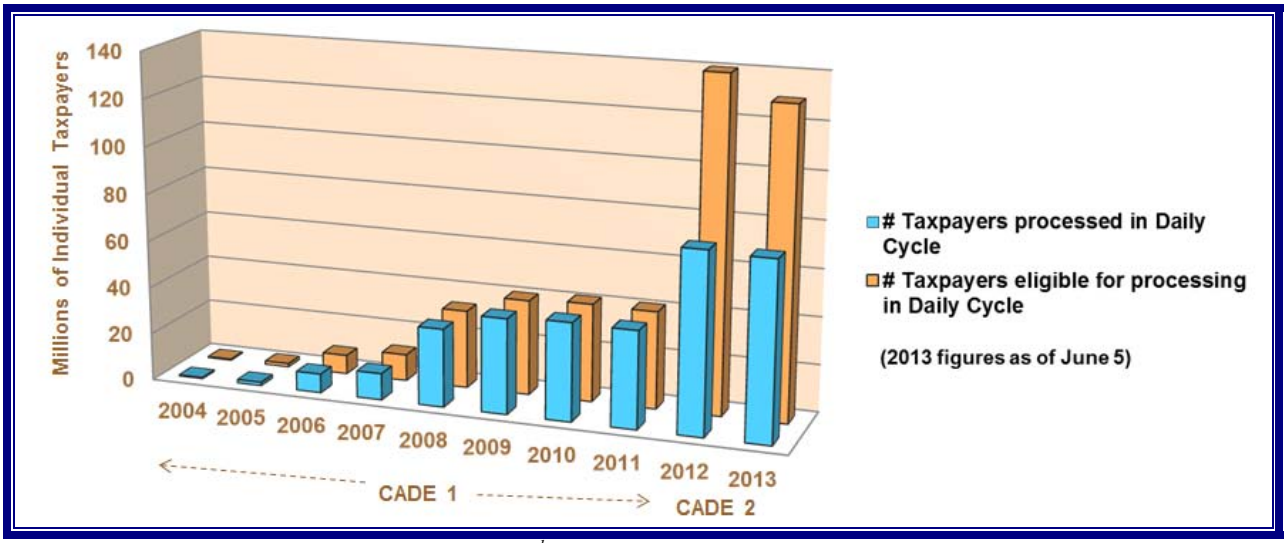
Further, while the IRS has taken steps to improve management controls for this major information technology investment, additional improvements are needed to ensure consistent risk mitigation within program management processes, testing practices, and system requirements management. Our report provided six recommendations to address these issues.

## CADE 2 system

The CADE 2 program is one of the top information technology modernization projects in the IRS. The CADE 2 mission is to provide state-of-the-art individual taxpayer account processing and data-centric technologies to improve service to taxpayers and enhance tax administration. CADE 2 will replace the current Individual Master File account settlement system with a relational database processing system and become a key component in the IRS's enterprisewide, data-centric information technology strategy.

Transition State 1 has two major implementation pieces: Daily Processing and Database Implementation. Daily Processing, which uses the Individual Master File and not the CADE 2 database, went into production in January 2012. Figure 8 shows the difference in daily processing from CADE to CADE 2.

### Figure 8: Comparison of CADE and CADE 2 Daily Processing




*Source: IRS IT organization, Fiscal Year 2013 3rd Quarter IT Investment Report Version 2.2, dated June 30, 2013.*

The March 2013 Information Technology Business Value Chart reported that as of March 28, 2013, CADE 2 Transition State 1 Daily Processing posted over 72.65 million returns

and issued 66.54 million refunds totaling in excess of $174.43 billion. With the CADE 2 Transition State 1 Daily Processing cycle, the IRS can process returns faster and IRS customer service representatives can more quickly access and update taxpayer records to resolve discrepancies.

Database Implementation, while not fully implemented, developed a relational database to store individual taxpayer account data migrated from Individual Master File tape files on a daily basis. In March 2012, the IRS initialized version 2.1 of the CADE 2 database with 270 million individual taxpayer accounts and more than a billion tax modules. The IRS completed a second database initialization in October 2012 and kept the database current and in sync with the Individual Master File data through December 2012.

During our review[42] of the database deployment, we found that the CADE 2 database cross-functional triage team effectively managed and resolved more than 1,000 data defects. However, our review determined that the downstream system interfaces were not implemented because of data quality issues that exist with the CADE 2 database. The interfaces were also not implemented by the June 2013 revised date, which had a revised estimated cost of $83 million.

In addition, the CADE 2 database's lack of accuracy, completeness, and availability prevents it from serving as the trusted source for the downstream systems. We also determined that the solution architecture of the CADE 2 database interfaces does not meet the IRS's business needs because it does not meet performance expectations and creates resource contention situations between servicing online transactions and query operations. Our report provided four recommendations to address these issues.

## Implementation of New Systems for the Patient Protection and Affordable Care Act Provisions

The ACA contains an extensive array of tax law changes that will present a continuing source of challenges for the IRS in the coming years. While the Department of Health and Human Services has the lead role in the policy provisions of the ACA, the IRS administers the law's numerous tax provisions. The IRS estimates that at least 42 provisions will either add to or amend the tax code and at least eight will require the IRS to build new processes that do not exist within the current tax administration system. In addition, the IRS must create new or revise existing tax forms, instructions, and publications; revise internal operating procedures; and reprogram major computer systems used for processing tax returns.

Results from our audits illustrate the need for continued oversight of the IRS's administration of many of these tax-related provisions. In addition, during our July 2013 congressional

[42] See Appendix IV, Ref. No. 2013-20-097.

testimony,[43] we raised the following three concerns regarding implementation of the ACA provisions:

- The protection of Federal tax data provided to the Exchanges.
- New fraud prevention or existing fraud detection systems may not be operational in sufficient time to mitigate ACA fraud risks.
- Final integration testing for IRS and Department of Health and Human Services systems may not be completed before the start of the enrollment period (October 2013).

Several key ACA provisions will become effective in Fiscal Year 2014, making both Fiscal Year 2014 and Calendar Year 2015 significant periods for ACA oversight. Because of the extensive changes to numerous tax code provisions, our concerns related to the development and implementation of new ACA systems, and the extensive coordination required between all of the stakeholders to effectively administer the ACA, we have implemented a multiyear oversight strategy that includes audits, evaluations, and investigative resources to assess the IRS's implementation of the ACA. This strategy includes coordination with other agencies, such as the Department of Health and Human Services Office of the Inspector General. Our system development reviews of the IFSV and Advanced Premium Tax Credits Project identified deficiencies that should be addressed to ensure long-term success of the IRS's efforts to develop and implement new information technology systems within its ACA Program.

## IFSV Project

The IFSV Project is a core project of the ACA Program and will support open enrollment beginning in October 2013. The IFSV Project is important to the functionality and success of the ACA Program because it is responsible for developing a solution that will verify income and family size, based on tax return data, for determining an individual's eligibility for the Advanced Premium Tax Credit for health insurance.

By the end of August 2012, the IFSV Project had completed all six systems development components, each delivering a piece of approved functionality.[44] While cost data specific to the IFSV Project were not readily available during our audit, the IRS is generally managing systems development risk areas with the implementation of the new Iterative Path within the Enterprise Life Cycle. However, process improvements are needed to better ensure that (1) the IFSV Project team adheres to configuration management guidelines when baselined requirements are changed and (2) the ACA Program Configuration Control Board emergency meeting processes are effectively communicated. Further, an integrated suite of automated tools could improve

[43] *ACA – Information Technology Readiness and Data Security: Joint Hearing Before the Committees on Oversight and Government Reform and Homeland Security*, 113th Cong. (July 17, 2013) (statement of Alan R. Duncan, Assistant Inspector General for Audit, TIGTA).
[44] See Appendix IV, Ref. No. 2013-23-034.

requirements management and testing for the IFSV Project. Our report provided three recommendations to address these issues.

### Premium Tax Credit Program

Beginning in January 2014, eligible taxpayers who purchase health insurance through an Exchange may qualify for and request a refundable tax credit, the Premium Tax Credit, to assist with paying their health insurance premium. The Premium Tax Credit will be claimed on the taxpayer's Federal tax return at the end of each coverage year. Because it is a refundable credit, taxpayers who have little or no income tax liability can still benefit. The Premium Tax Credit can also be paid in advance to a taxpayer's health insurance provider to help cover the cost of premiums. This credit is referred to as the Advanced Premium Tax Credit.

Our review found that the IRS had completed development and testing for the Premium Tax Credit Computation Engine needed to calculate the Advanced Premium Tax Credit and the Remainder Benchmark Household Contribution.[45] The IRS has also developed a process to verify the accuracy of the Premium Tax Credit Computation Engine calculations. However, improvements are needed to ensure the long-term success of the Premium Tax Credit Project by adhering to important systems development controls for configuration and change management, interagency testing, and fraud detection and mitigation. Our report provided seven recommendations to address these issues.

## Updates for the Integrated Financial System to Support Internal Revenue Service Operations

In November 2004, the IRS replaced the Automated Financial System with the IFS. The system was implemented as a major project under the Modernization Program, but in November 2005 the IFS was reclassified as Operations and Maintenance funding. For Fiscal Years 2012 and 2013, the IRS requested nearly $37.5 million to upgrade the IFS. The IRS recently 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. At the time of our review,[46] the IRS planned to complete deployment of these system updates in November 2012.

During our audit of the IFS, we found that the IRS did not comply with Internal Revenue Manual guidance requiring that test cases be developed to support requirements testing and that the expected results from testing should be compared to the actual results to determine if requirements were sufficiently tested. Additionally, our audit found that the IRS did not maintain evidence to validate the actual test results. IFS management did not ensure that testers

[45] See Appendix IV, Ref. No. 2013-23-119.
[46] See Appendix IV, Ref. No. 2013-20-030.

consistently followed Internal Revenue Manual guidelines to obtain and maintain objective evidence, such as screen prints, to verify that requirements were sufficiently tested. When expected results are not fully presented in test cases, or documents used to verify actual test results are not available, the IRS cannot verify the adequacy of its system testing activities. This increases the risks of adverse impact on the functionality of the IFS. Our report provided six recommendations to address these issues.

## Information Technology Service Management Disciplines to Achieve Program Efficiencies and Savings Were Implemented; However, Additional Cost Savings Can Be Realized

The IRS IT organization plays an important role in helping the IRS meet its tax administration responsibilities each year. It is not only responsible for the efficient and secure processing and transfer of taxpayer data, but it also supports the needs of over 95,000 employees who rely on equipment and system availability. The IRS needs to ensure that it leverages viable technological advances as it improves its overall operational environment.

Attaining Information Technology Infrastructure Library (ITIL®) maturity is a critical milestone for the IRS in developing a world-class information technology infrastructure that will create greater efficiency and productivity in supporting taxpayers and meeting the IRS's mission. The ITIL is a set of practices for information technology service management. The ITIL focuses on the five key service management principles pertaining to service strategy, design, transition, operation, and continual improvement. The IRS reported that the IT organization had achieved ITIL Maturity Level 3 in October 2012.

Achieving program efficiencies and cost savings is an important area for the IRS, especially when considering that its Fiscal Year 2012 budget was reduced over $300 million from Fiscal Year 2011. As a result of its reduced budget, the IRS reduced its administrative costs, offered early outs and buyouts, and made difficult decisions affecting taxpayer services and enforcement operations. While the IRS has made progress improving program effectiveness and reducing costs, this area continues to remain a challenge for the IRS. Our recent audit work illustrates the IRS's accomplishments and opportunities to achieve cost savings in information technology areas including data center consolidation, hardware management, and software management. Several of our reviews resulted in the reporting of outcome measures. See Appendix V for a list of outcome measures we reported in Fiscal Year 2013.

### Data Center Consolidation Initiative

In February 2010, the OMB established the Federal Data Center Consolidation Initiative as a Governmentwide initiative designed to reduce the energy and real estate footprint of Federal data centers while increasing efficiency, strengthening the overall Government security posture, and promoting green information technology by reducing the total number of Federal data centers.

The IRS has exceeded its yearly goals in the first two years for reducing data center space and improving the energy efficiency of its data centers. However, management of the project needs to be improved to ensure that the IRS meets its remaining Data Center Consolidation Initiative goals by the end of Fiscal Year 2015. Two years of the IRS's five-year Data Center Consolidation Initiative have elapsed without a clear plan for how the overall data center space reduction goals will be accomplished. During our review,[47] the IRS decided to close the Enterprise Computing Center in Detroit, with an estimated savings of approximately $15 million per year. Our report provided eight recommendations to address these issues.

## Aircard and BlackBerry® Smartphone Program

Our audit identified that the processes for assigning and monitoring the use of aircards and BlackBerry smartphones are not adequate.[48] We found that assignment of these devices is generally based on job series classifications without adequately ensuring that a business need exists. For example, management did not always consider the frequency an employee actually works outside an IRS office prior to assigning devices. We also found that managerial approvals were not always obtained when employees who were not in a profiled job series were assigned these devices. We identified 2,560 devices without documented management approval, costing the IRS more than $950,000 in Fiscal Year 2011, or potentially about $4.8 million over five years.

In addition, processes for monitoring aircard and BlackBerry smartphone use do not ensure that the IRS is not paying for unused or underused equipment. Established processes to notify employees when aircards were not used for 90 calendar days were not being followed, and there was no formal process to monitor BlackBerry smartphone use for similar periods of inactivity. We identified periods of inactivity during Fiscal Year 2011 for aircards and BlackBerry smartphones ranging from three to 12 months; however, the IRS still incurred monthly access fees totaling approximately $1.1 million for these devices. Our report provided six recommendations to address these issues.

## Information technology hardware maintenance contracts

Our review identified several weaknesses in the oversight of selected information technology hardware maintenance contracts.[49] Specifically, we found instances where contracting personnel were not always effectively monitoring the contracts. We also identified an instance where the IRS did not receive contract deliverables in accordance with the contract's requirements or submit written modifications when necessary to update an existing contract. These scenarios could potentially cause the IRS to unnecessarily pay for maintenance on assets that have been retired and no longer need this service. When contracts are not properly administered, the IRS

[47] See Appendix IV, Ref. No. 2013-20-013.
[48] See Appendix IV, Ref. No. 2013-10-010.
[49] See Appendix IV, Ref. No. 2013-22-094.

may not receive the desired outcome or the best return on its investment. Our report provided two recommendations to address these issues.

### Treasury Enhanced Security Initiatives Project

In addition to the information security deficiencies discussed in an earlier section of this report, we found that the IRS appropriately acquired the project's multiple software components and the project team completed key documentation during the development process, ensuring that critical issues were identified and addressed.[50] However, the project experienced several delays, and the project's oversight board did not take required actions to manage the delays or associated costs. At the time of our review, the IRS was scheduled to deploy the security tools in December 2010 but now plans to complete the deployment in May 2013. As a result, we identified a potential outcome measure of $1,151,939 in inefficient use of resources on contractor support services for the Treasury Enhanced Security Initiatives Project from its original December 2010 planned deployment of the Symantec Risk Automation Suite component through April 2012. Our audit report provided three recommendations to address these issues.

## The Internal Revenue Service Needs to Strengthen Its Hardware and Software Management Processes

As previously mentioned, the IRS achieved a significant milestone in October 2012 when an independent research company affirmed that the IRS IT organization had achieved ITIL Maturity Level 3. Maturity Level 3 is when the organization is in a proactive, rather than reactive, stage and has a set of defined, documented, established, and integrated processes; it focuses on the customer and appropriate level of service support provided by information technology operations. IRS information technology services have successfully completed the ITIL process called Service Transition, which incorporates asset management. Attaining this maturity is critical for the IRS in developing a world-class information technology infrastructure that will create greater efficiency and productivity in supporting taxpayers and meeting the IRS's mission. Although the IRS IT organization achieved this major milestone, it needs to work to correct the deficiencies identified during our reviews of information technology asset management system and software licensing.

### Improvements to hardware asset management are needed to ensure complete and accurate inventory data

In August and September 2011, the User and Network Services organization replaced its former inventory system, Information Technology Asset Management System, with the KISAM system. The User and Network Services organization recognizes the KISAM-AM module as the sole authoritative source and official inventory record for all information technology assets within the

[50] See Appendix IV, Ref. No. 2013-20-016.

IRS [with the exception of information technology software assets (to include software and software licenses)].

Although the IRS successfully migrated inventory data between the legacy inventory system and the KISAM-AM, our review identified that the procedures established to ensure the accuracy of information technology asset records within the KISAM-AM were not being followed.[51] Our review also identified several conditions demonstrating the IT organization's inability to maintain effective controls over its information technology assets. For example, IRS offices did not always properly conduct the reconciliation of information technology assets and resolve those asset records identified as needing updating or correcting. In addition, offices were not taking sufficient steps to recover assets placed in a temporary "missing" status, and the reports used by the offices to track down missing assets did not provide disposal information. An inaccurate and incomplete inventory system decreases data integrity and exposes the IRS to the loss or theft of its assets. Our report provided eight recommendations to address these issues.

### Improvements to software asset management are needed to ensure resources are used efficiently

During our audit of desktop and laptop software licensing,[52] we found that the IRS does not have enterprisewide or local software license management policies and procedures, an enterprisewide license management structure, or roles and responsibilities for the organizational entities that conduct software license management. In addition, the lack of an enterprisewide inventory with comprehensive data on all software and software licensing impedes the ability of the IRS to more thoroughly analyze the relationships among its software license agreements and vendors to more cost-effectively buy software licenses and maintenance.

Until the IRS implements an effective program to manage software licenses, the IRS is incurring increased risks in managing software licenses. These risks include: 1) not complying with licensing agreements that could result in embarrassment, legal problems, and financial liability; 2) not using licenses in the most cost-effective manner; and 3) not effectively using licensing data to reduce software purchase and software maintenance costs. Our report provided six recommendations to address these issues.

## There Has Been a Lack of Progress in Providing Taxpayer Access to Account Information via the Internet

RRA 98 required the IRS to develop procedures to allow taxpayers filing returns electronically to review their account online by December 31, 2006; the IRS did not meet this requirement. The objective of the IRS eAuthentication Project is to design and build a common service to proof and register individuals and to provide and validate credentials for ongoing system access using

[51] See Appendix IV, Ref. No. 2013-20-089.
[52] See Appendix IV, Ref. No. 2013-20-025.

the Internet. The IRS stated that the Get Transcript application is set to launch in January 2014, which will provide the first step toward expanding transcript access online.

Our review of the IRS's development and implementation of an effective eAuthentication solution for taxpayers to access their tax information[53] found that applications were created to increase online taxpayer functionality; however, these applications do not meet the criteria of RRA 98. The IRS has not made adequate progress in allowing taxpayers to access tax accounts. Currently, taxpayers cannot review account information electronically.

We believe that IRS leadership did not prioritize the applications that meet the requirements of RRA 98. Rather, the IRS devoted resources to the development and implementation of several applications that do not meet the intent of RRA 98. For example, in August 2012, the IRS deployed the eTranscripts for Banks application, which allowed a small number of taxpayers to securely verify their identities with the IRS and participate in the eTranscripts for Banks program. However, the application does not meet the intent of RRA 98 because it only allows taxpayers to request that their tax account and tax return transcripts be sent to their lending institution electronically versus a hardcopy request. It does not provide the ability to view, print, or perform any other functions. In March 2013, the IRS deployed the Where's My Amended Return?[54] application, but it did not directly meet the requirements of account review. However, both applications provided ancillary benefits to taxpayers. Besides not developing applications that meet the RRA 98 requirements, we found the following problems.

- The IRS eAuthentication project team did not perform complete capacity testing on eAuthentication Release 1 for several reasons (*e.*g., instability of the IRS information technology infrastructure and concerns over the security of data in the testing environment). Without capacity testing, the IRS does not know how many users can access eAuthentication at once before it fails and cannot verify whether eAuthentication will function as intended.
- Actual cost information is not readily available for the project because the project office has no formal system to obtain actual costs. The project manager uses a less formal approach (*e.g.*, calling people or manually tracking expenses) to obtain actual cost information. Due to the informal nature of the process used, the cost information obtained and ultimately reported to Cybersecurity executive management are estimates and may be inaccurate and unreliable. Executive management should be given the best information possible when making key resource decisions.

Our audit report provided three recommendations to address these issues.

[53] See Appendix IV, Ref. No. 2013-20-127.
[54] Allows taxpayers to track the status of an amended return.

## Potential Savings for New Bring Your Own Device Pilot

Businesses and Government agencies are receptive to BYOD programs because they have the potential to provide cost savings, increase productivity, and improve employee satisfaction. Employees tend to like the BYOD program because it allows them to use their own preferred device and, if they are required to have a cell phone for work, carry only one device. Cost savings can be realized if the organization's cell phone ownership, service, and/or support are reduced or discontinued as a result of a BYOD program. Additionally, achieving benefits is contingent on implementation details and workforce acceptance.

The driving force behind the BYOD program at the IRS has been the investigation of mobile technology that provides business value to employees and increases employee productivity and satisfaction. Starting in September 2010, the IRS began a phased approach to implement a BYOD program. In June 2012, the IRS started its third phase, a true BYOD program, enabling it to connect up to 1,000 devices.

Our audit of the IRS's BYOD Pilot Project[55] found that the IRS took several noteworthy actions to implement its BYOD pilot, including taking a phased approach and considering security. However, although it has spent more than $900,000 on mobility efforts to date, the IRS has not developed a complete cost-benefit analysis to fully justify the implementation of the BYOD concept within the IRS.

While the IRS prepared a simple cost analysis that compared the estimated cost of a BYOD program to the cost of the IRS's existing BlackBerry and cell phone programs prior to starting the BYOD pilot, the analysis was not updated with complete information on assumptions and costs. Consequently, as the pilot expanded, IRS managers relied on the original assumptions and cost projections in the analysis, which did not provide a sufficient basis for informed decisionmaking. BYOD could provide significant benefits; however, these benefits are just conjecture until the IRS conducts a thorough cost-benefit analysis. Our audit report provided one recommendation to address this issue.

[55] See Appendix IV, Ref. No. 2013-20-108.

## Appendix I

# Detailed Objective, Scope, and Methodology

Our overall objective was to assess the progress of the IRS's Information Technology Program, including modernization, security, and operations for Fiscal Year 2013. This review was required by the RRA 98. To accomplish our objective, we:

I. Obtained information on the IRS budget and staffing to provide context on the size of the IRS IT organization.

II. Assessed systems security and privacy issues. We determined which are at high risk in delivering IRS program objectives and protecting tax administration data.

   A. Obtained and reviewed TIGTA's Systems Security Directorate audit reports issued during Fiscal Year 2013. During the review, we analyzed and prepared an overall assessment of security and privacy issues.

   B. Identified and summarized other relevant TIGTA and/or external oversight assessments dealing with security and privacy (*e.g.*, assessments performed by the GAO and the National Taxpayer Advocate).

III. Assessed systems modernization and applications development issues. We determined which are at high risk in delivering IRS program objectives and protecting tax administration data.

   A. Obtained and reviewed TIGTA's Systems Modernization and Applications Development Directorate audit reports issued during Fiscal Year 2013. During the review, we analyzed and prepared an overall assessment of modernization and applications development issues.

   B. Identified and summarized other relevant TIGTA and/or external oversight assessments dealing with modernization and applications development (*e.g.*, assessments performed by the GAO and the National Taxpayer Advocate).

IV. Assessed systems operations issues. We determined which are at high risk in delivering IRS program objectives and protecting tax administration data.

   A. Obtained and reviewed TIGTA's Systems Operations Directorate audit reports issued during Fiscal Year 2013. During the review, we analyzed and prepared an overall assessment of systems operations issues.

B. Identified and summarized other relevant TIGTA and/or external oversight assessments dealing with operations (*e.g.*, assessments performed by the GAO and the National Taxpayer Advocate).

## ***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 did not evaluate internal controls as part of this review because doing so was not necessary to satisfy our review objective.

## Appendix II

# Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Gwen McGowan, Director, Systems Modernization and Applications Development
Kent Sagara, Director, Systems Security
Danny Verneuille, Director, Systems Operations
Diana Tengesdal, Audit Manager
Sarah Shelton, Lead Auditor
Charlene Elliston, Senior Auditor
Louis Lee, Senior Auditor
Larry Reimer, Senior Auditor
Tina Wong, Senior Auditor

## Appendix III

# Report Distribution List

Acting Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Office of the Deputy Commissioner for Services and Enforcement SE
Chief, Agency-Wide Shared Services OS:A
Commissioner, Wage and Investment Division SE:W
Deputy Chief Information Officer for Operations OS:CTO
Deputy Chief Information Officer for Strategy and Modernization OS:CTO
Deputy Commissioner, Services and Operations SE:W
Associate Chief Information Officer, Affordable Care Act – Program Management Office OS:CTO:ACA
Associate Chief Information Officer, Applications Development OS:CTO:AD
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Associate Chief Information Officer, Information Technology – Program Management Office OS:CTO:MP
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
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, Business Planning and Risk Management OS:CTO:SP:RM

## Appendix IV

# List of Treasury Inspector General for Tax Administration Reports Reviewed

| Number | Reference Number | Audit Report Title | Report Issuance Date |
|---|---|---|---|
| 1 | 2013-10-010 | *Inadequate Aircard and BlackBerry Smartphone Assignment and Monitoring Processes Result in Millions of Dollars in Unnecessary Access Fees* | January 11, 2013 |
| 2 | 2013-20-013 | *The Data Center Consolidation Initiative Has Made Significant Progress, but Program Management Should Be Improved to Ensure That Goals Are Achieved* | June 10, 2013 |
| 3 | 2013-20-016 | *Significant Delays Hindered Efforts to Provide Continuous Monitoring of Security Settings on Computer Workstations* | January 24, 2013 |
| 4 | 2013-20-023 | *Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process* | February 27, 2013 |
| 5 | 2013-20-025 | *Desktop and Laptop Software License Management Is Not Being Adequately Performed* | June 25, 2013 |
| 6 | 2013-20-030 | *Integrated Financial System Updates Are Improving System Security, but Remaining Weaknesses Should Be Addressed* | March 28, 2013 |
| 7 | 2013-23-034 | *Affordable Care Act: The Income and Family Size Verification Project: Improvements Could Strengthen the Internal Revenue Service's New Development Process* | March 29, 2013 |
| 8 | 2013-20-039 | *Enhancements Made to the Modernized e-File System in Release 8 Should Improve System Performance for the 2013 Filing Season* | April 22, 2013 |
| 9 | 2013-20-063 | *Improvements Are Needed to Ensure Successful Development and System Integration for the Return Review Program* | July 26, 2013 |

| Number | Reference Number | Audit Report Title | Report Issuance Date |
|---|---|---|---|
| 10 | 2013-20-089 | *Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss* | September 16, 2013 |
| 11 | 2013-20-125 | *Customer Account Data Engine 2 Database Deployment Is Experiencing Delays and Increased Costs* | September 23, 2013 |
| 12 | 2013-20-106 | *Automated Monitoring Is Needed for the Virtual Infrastructure to Ensure Secure Configurations* | September 18, 2013 |
| 13 | 2013-20-107 | *Full Compliance With Trusted Internet Connection Requirements Is Progressing; However, Improvements Would Strengthen Security* | September 17, 2013 |
| 14 | 2013-20-108 | *Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot* | September 24, 2013 |
| 15 | 2013-20-117 | *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* | September 27, 2013 |
| 16 | 2013-20-118 | *Foreign Account Tax Compliance Act: Improvements Are Needed to Strengthen Systems Development Controls for the Foreign Financial Institution Registration System* | September 27, 2013 |
| 17 | 2013-22-094 | *Increased Oversight of Information Technology Hardware Maintenance Contracts Is Necessary to Ensure Against Paying for Unnecessary Services* | September 24, 2013 |
| 18 | 2013-23-119 | *Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project* | September 27, 2013 |
| 19 | 2013-20-127 | *While Efforts Are Ongoing to Deploy a Secure Mechanism to Verify Taxpayer Identities, the Public Still Cannot Access Their Tax Account Information Via the Internet* | September 25, 2013 |
| 20 | 2013-20-128 | *Fiscal Year 2013 FISMA Unclassified Systems* | September 27, 2013 |

## Appendix V

# Outcome Measures Reported in Fiscal Year 2013

| Audit Report Title | Type of Measure | Amount |
|---|---|---|
| *Inadequate Aircard and BlackBerry Smartphone Assignment and Monitoring Processes Result in Millions of Dollars in Unnecessary Access Fees* | Cost Savings – Funds Put to Better Use | $5.9 million over 5 years |
| *The Data Center Consolidation Initiative Has Made Significant Progress, but Program Management Should Be Improved to Ensure That Goals Are Achieved* | Cost Savings – Funds Put to Better Use | $60 million over 4 years |
| *Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss* | Reliability of Information | 60,548 assets |
| | Protection of Resources | 106 assets totaling $6,857,798 |
| *Foreign Account Tax Compliance Act: Improvements Are Needed to Strengthen Systems Development Controls for the Foreign Financial Institution Registration System* | Inefficient Use of Resources | $2.2 million |

## Appendix VI

# Glossary of Terms

| Term | Definition |
|---|---|
| Advanced Premium Tax Credit | Paid in advance to a taxpayer's insurance company to help cover the cost of premiums. |
| Affordable Care Act (ACA) | In March 2010, the President signed into law the Patient Protection and Affordable Care Act to provide more Americans with access to affordable health care by January 1, 2014. |
| Asset Manager | KISAM module that tracks both information technology and non–information technology equipment used throughout the IRS. |
| Auditable Events | Actions taken on IRS systems that shall be captured and recorded for subsequent audit review based on the impact level of the system (high, moderate, or low) as determined by the guidelines in the NIST Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*. Internal Revenue Manual 10.8.3 contains lists of auditable events applicable to the systems categorized as high, moderate, or low based on the NIST standards. |
| Baseline Configuration | A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time and that can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. |
| Best Practices | Proven activities or processes that have been successfully used by multiple organizations. |
| Capacity Test | Test used to determine how many users and/or transactions a given system will support and still meet performance goals. |
| Change Management | The transition of a changed or new product through development to deployment into the current production environment with minimum disruption to users. This can occur in a number of ways, including, but not limited to: (1) implementation of a change to a product baseline, (2) establishing a new product baseline, and (3) a change to a Service Level Agreement. |

| Term | Definition |
|---|---|
| Change Request | The method for requesting approval to change a baselined product or other controlled item. |
| Citrix Environment | Provides an environment for use on server and desktop virtualization and cloud computing technologies. |
| Configuration Control Board | Serves as the change approval authority for baselined products. |
| Configuration Settings | The set of parameters that can be changed in hardware, software, and/or firmware that affect the security posture and/or functionality of the information system. |
| Consolidation | An approach to reducing data center space that involves moving servers to a few selected data centers or moving small data centers to larger centers. |
| Corporate Files Online | This system provides online transactional access to Individual and Business Master File data, Information Return Program data, and various other related data collections. These files are accessed via IRS-developed Customer Information Control System command codes. |
| Customer Account Data Engine 2 | An IRS application that will replace the existing Individual Master File and CADE applications. The CADE 2 is designed to provide state-of-the-art individual taxpayer account processing and technologies to improve service to taxpayers and enhance IRS tax administration. |
| Database Administrator | An individual that performs all activities related to maintaining a correctly performing and secure database environment. Responsibilities include design, implementation, and maintenance of the database system. |
| Encryption | The process of making data unreadable by other humans or computers for the purpose of preventing others from gaining access to its contents. |
| Enterprise Life Cycle | A structured business systems development methodology that requires the preparation of specific work products during different phases of the development process. |
| Federal Information Security Management Act (FISMA) | A statute that requires agencies to assess risks to information systems and provide information security protections commensurate with the risks. The FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the OMB. (Title III, P.L. 107-347.) |

| Term | Definition |
|---|---|
| Filing Season | The period from January through mid-April when most individual income tax returns are filed. |
| Fiscal Year | A 12-consecutive-month period ending on the last day of any month. The Federal Government's fiscal year begins on October 1 and ends on September 30. |
| Form 1099 | The 1099 series is used to report various types of income received throughout the year other than the wages paid. |
| Form W-2 | A form used to report an employee's wages paid and taxes withheld for the year. |
| Governance | A set of processes, guidelines, and policies that guide and affect the direction of an organization's behavior or assets. |
| Government Accountability Office | The audit, evaluation, and investigative arm of Congress that provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. |
| Green Information Technology | Optimal use of information and communication technology for managing the environmental sustainability of enterprise operations as well as that of their products, services, and resources, throughout their life cycles. |
| Health and Human Services | The U.S. Government's principal agency for protecting the health of all Americans and providing essential human services. |
| Impact Assessment | Evaluation of a change request to determine its impact on a project's schedule, cost, other dependent projects, and upstream and downstream systems. |
| Income and Family Size Verification | Will verify income and family size for individuals requesting eligibility for an Advanced Premium Tax Credit for health insurance. |
| Individual Master Files Online | This system provides online transactional access to Individual Master File data. See entry for Corporate Files Online. |
| Information Technology Infrastructure Library | Provides guidelines for the use and management of software and licenses. The ITIL® is a widely accepted set of concepts and practices for information technology service management derived from user and vendor experts in both the private and public sectors. It focuses on key service management principles pertaining to service strategy, design, transition, operation, and continual improvement, with each principle being covered in a separate ITIL core publication. Software asset management is a key process described within the service transition core publication. |

| Term | Definition |
|---|---|
| | The ITIL also has a separate publication entitled Best Practice Software Asset Management that covers software asset and license management best practices in more depth than the core publication. ITIL best practices recommend 1) the development of software license management policies and procedures and roles and responsibilities; 2) a centralized, enterprisewide management structure for software asset management; 3) the use of software license management tools; and 4) the creation and maintenance of accurate enterprisewide inventories of software licenses. |
| Infrastructure | The fundamental structure of a system or organization. The basic, fundamental architecture of any system (electronic, mechanical, social, political, *etc*.) determines how it functions and how flexible it is to meet future requirements. |
| Interface | A point at which independent systems interact. |
| Knowledge Incident/Problem Service Asset Management System | An IRS application that maintains the complete inventory of information technology and non–information technology assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications and shares information with the Enterprise Service Desk. |
| Legacy e-File System | The current IRS electronic filing system that is being replaced by the Modernized e-File system. |
| Material Weakness | A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis. Materiality represents the magnitude of an omission or misstatement of an item in a financial report that, when considered in light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item. |
| Missing | KISAM-AM asset assignment status of lost, stolen, or temporarily missing assets until a determination is made. |
| Modification | Any formal change to the terms and conditions of a contract, delivery order, or task order, either within or outside the scope of the original agreement. |

| Term | Definition |
|---|---|
| Multifactor Authentication | 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. |
| 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. |
| Portal | A point of entry into a network system that includes a search engine or a collection of links to other sites, usually arranged by topic. |
| Requirement | A formalization of a need and 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. |
| Retired | KISAM-AM asset assignment status of removed from active inventory and no longer used. This assignment is used in conjunction with disposal codes. |
| Risk | A potential event that could have an unwanted impact on the cost, schedule, business, or technical performance of an information technology program, project, or organization. |
| Security Controls Assessment Test Plan | Security controls assessments are conducted in the IRS production environment and consist of activities designed to ensure that the system's security safeguards are in place and functioning as intended. |
| Significant Deficiency | An instance of weak or missing controls that are of sufficient importance to be reported to the next level of management. |
| Software License Agreement | The legal contract between the owner and purchaser of a piece of software that establishes the purchaser's rights. A software license agreement provides details and limitations on where, how, how often, and when the software can be installed and used and provides restrictions that are imposed on the software. The agreement includes the licensing model used for defining and measuring the use of the software. For example, a common simple license model could be based on how many people can use the software and how many systems the software may be installed on. Software companies also make special license agreements for large business and Government entities that may be different from those provided to the general consumer. |

| Term | Definition |
|---|---|
| Stakeholders | An individual or organization that is materially affected by the outcome of the system. Examples of project stakeholders include the customer, the user group, the project manager, the development team, and the testers. |
| Symantec Risk Automation Suite | Tool with capabilities that relate directly to the objectives of the NIST Secure Content Automation Protocol, a method for using specific standards to enable automated and integrated vulnerability management and measurement and policy compliance evaluation. Provides continuous and automated information technology risk metrics. |
| 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. |
| Validation | Verification that something is correct or conforms to a certain standard. |
| Virtualization | An approach that helps to accomplish data center consolidation. It involves moving applications and data on several physical servers onto a single virtual server. |
| Windows 2000 | Provides an environment for use on both client and server computers. |