TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the Internal Revenue Service Information Technology Program

September 30, 2015

Reference Number: 2015-20-094

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

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

HIGHLIGHTS

ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE INFORMATION TECHNOLOGY PROGRAM

Highlights

Final Report issued on September 30, 2015

Highlights of Reference Number: 2015-20-094 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

In Fiscal Year 2014, the IRS collected about $3.1 trillion in Federal tax payments, processed hundreds of millions of tax and information returns, and paid about $374 billion in refunds to taxpayers. In addition, the IRS employs almost 87,000 people in 551 facilities nationwide. The IRS relies extensively on computerized systems to support its financial and mission-related operations. Weaknesses within the IRS's Information Technology Program could result in computer operations that become compromised, disrupted, or outdated, which could adversely affect the IRS's ability to meet its mission of providing America's taxpayers with top-quality service by helping them understand and meet their tax responsibilities and enforcing the law with integrity and fairness to all.

WHY TIGTA DID THE AUDIT

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. Our overall objective was to assess the progress of the IRS's Information Technology Program including security, modernization, and operations for Fiscal Year 2015.

WHAT TIGTA FOUND

Cybersecurity remains a major challenge for the Federal Government, and the IRS continues to work toward securing tax information and maintaining taxpayer privacy. TIGTA identified weaknesses within the IRS's Cybersecurity program pertaining to continuous monitoring, configuration management, identity and access management, privacy impact assessments, external connections, and audit trails.

In addition, the IRS is developing a new system that uses data analytics to combat identity theft and tax fraud. During its pilot in Calendar Year 2014, the Return Review Program identified 10,348 identity theft cases totaling $43 million in refunds and an additional 350,000 potentially fraudulent returns that were not detected by the existing fraud detection system. However, the IRS has not planned for the retirement of its existing fraud detection system.

The IRS continues to develop or upgrade its systems to meet its obligation as the Nation's tax administrator. TIGTA identified concerns with Windows workstation and server upgrades, Integrated Enterprise Portal operations, and the Customer Account Data Engine 2 program.

Finally, the IRS made significant progress developing new systems supporting the Affordable Care Act. However, TIGTA identified issues with the Coverage Data Repository, the Affordable Care Act Verification Service, interagency testing, and the Final Integration Test program.

WHAT TIGTA RECOMMENDED

Because this report was an assessment report of the IRS's Information Technology Program based on TIGTA audit reports issued during Fiscal Year 2015, TIGTA did not make any recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 30, 2015

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael E McK

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Annual Assessment of the Internal Revenue Service Information Technology Program (Audit #201520010)

This report presents the results of our review of the Internal Revenue Service's (IRS) Information Technology Program including security, modernization, and operations. This review is required by the IRS Restructuring and Reform Act of 1998.[1] This audit is included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenges of Modernization, Security for Taxpayer Data and IRS Employees, Implementing the Affordable Care Act and Other Tax Law Changes, Fraudulent Claims and Improper Payments, and Achieving Program Efficiencies and Cost Savings.

Copies of this report are also being sent to the IRS managers affected by the report information. If you have any questions, please contact me or Danny Verneuille, Acting 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

Background...Page 1

Results of Review ....Page 6

Cybersecurity Remains a Major Challenge ....Page 6

Security and Privacy of Federal Tax Information..Page 7

Information Systems to Combat Identity Theft and Tax Fraud....................Page 14

Information Technology Infrastructure and Application Upgrades.............Page 17

Systems Development Supporting the Affordable Care Act ....Page 21

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ....Page 25

Appendix II – Major Contributors to This Report ....Page 27

Appendix III – Report Distribution List ....Page 28

Appendix IV – List of Treasury Inspector General for Tax Administration Reports Reviewed..Page 29

Appendix V – Outcome Measures Reported in Fiscal Year 2015................Page 31

Appendix VI – Glossary of Terms..Page 32

Abbreviations

ACA	Affordable Care Act
ACIO	Associate Chief Information Officer
CADE 2	Customer Account Data Engine 2
CMS	Centers for Medicare and Medicaid Services
CTO	Chief Technology Officer
EFDS	Electronic Fraud Detection System
ELC	Enterprise Life Cycle
ESAT	Enterprise Security Audit Trail
FISMA	Federal Information Security Modernization Act
FIT	Final Integration Test
FY	Fiscal Year
GAO	Government Accountability Office
IRS	Internal Revenue Service
IT	Information Technology
MOU	Memorandum of Understanding
PGLD	Privacy, Governmental Liaison, and Disclosure
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
RRP	Return Review Program
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized Access
USCERT	U.S. Computer Emergency Readiness Team

Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998[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 for Fiscal Year[2] (FY) 2015.

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. This includes ensuring that its computer systems are effectively secured to protect sensitive taxpayer data.

The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In FY 2014, the IRS collected about $3.1 trillion in Federal tax payments, processed hundreds of millions of tax and information returns, and paid about $374 billion in refunds to taxpayers. Further, the size and complexity of the IRS add unique operational challenges. The IRS employs almost 87,000 people in 551 offices located throughout the country. The IRS relies extensively on computerized systems to support its financial and mission-related operations. As such, it must ensure that its computer systems are effectively secured to protect sensitive financial and taxpayer data and are operating as intended. 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.

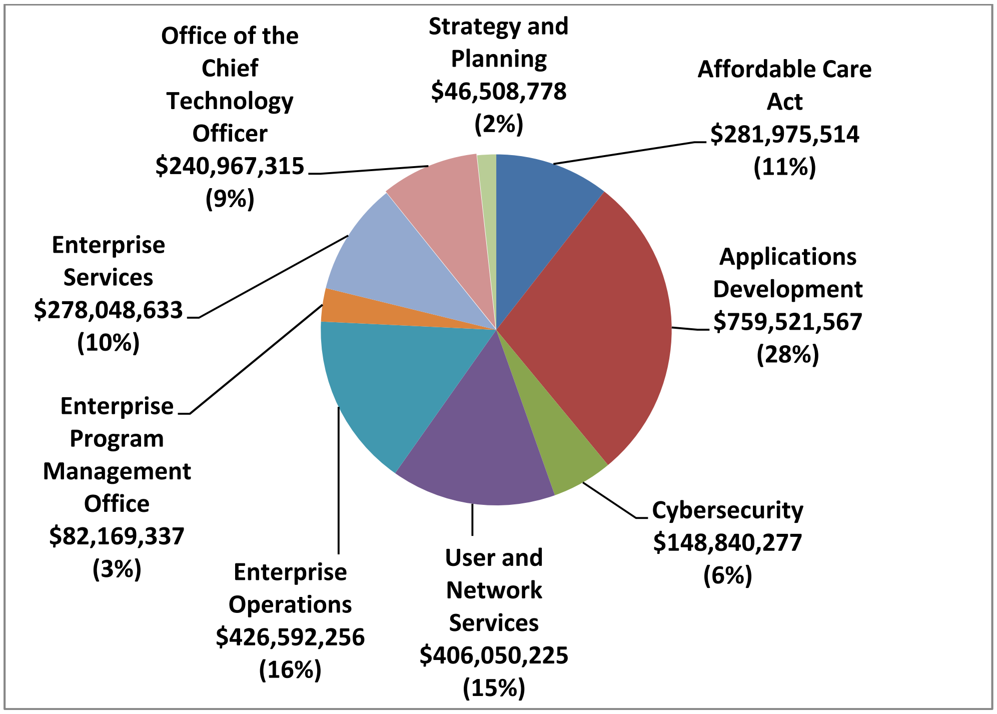
The growth of the Internet over the past decade has changed consumer expectations as they become increasingly more accustomed to using the web for anything from ordering telephone service to conducting transactions with financial institutions using traditional online and mobile devices. According to the IRS Strategic Plan (FYs 2014–2017), customers show a preference for Internet-based service before trying other service channels such as telephones, paper, or in person. The primary focus for the IRS over the past two decades has been to migrate taxpayers to electronic filing. In FY 2013, 83 percent of individual taxpayers chose to file electronically, a significant increase from 71.3 percent in FY 2010. In the same year, business returns were filed electronically at a rate of 36.7 percent, up from 27.5 percent in FY 2010. Outside of filing activities, taxpayers also use the Internet to download forms, view content, and check refund status. In FY 2012, the “Where’s My Refund?” application was used 132 million times. While these trends demonstrate substantial progress towards full online tax administration, there are

[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.).
[2] See Appendix VI for a glossary of terms.

distinct, unmet taxpayer needs that provide opportunities for the IRS to introduce more online self-service options. In 2011, an IRS study reported that taxpayers want to access online resources to complete transactional tasks and use digital services that provide self-service and assisted service from any location at any time. In addition to the opportunity to develop new online self-service tools, the IRS reports that there is an equally compelling case to refine web content and search capabilities that will lead to an overall improved user experience.

According to July 2015 budget information provided by the Associate Chief Information Officer (ACIO), Strategy and Planning, the IRS Information Technology (IT) organization's FY 2015 budget stayed flat at approximately $2.6 billion, up slightly from FY 2014's budget of approximately $2.5 billion. Figure 1 provides a breakdown of the FY 2015 budget by ACIO organization. Figure 2 provides a breakdown of the FY 2015 budget by funding source.

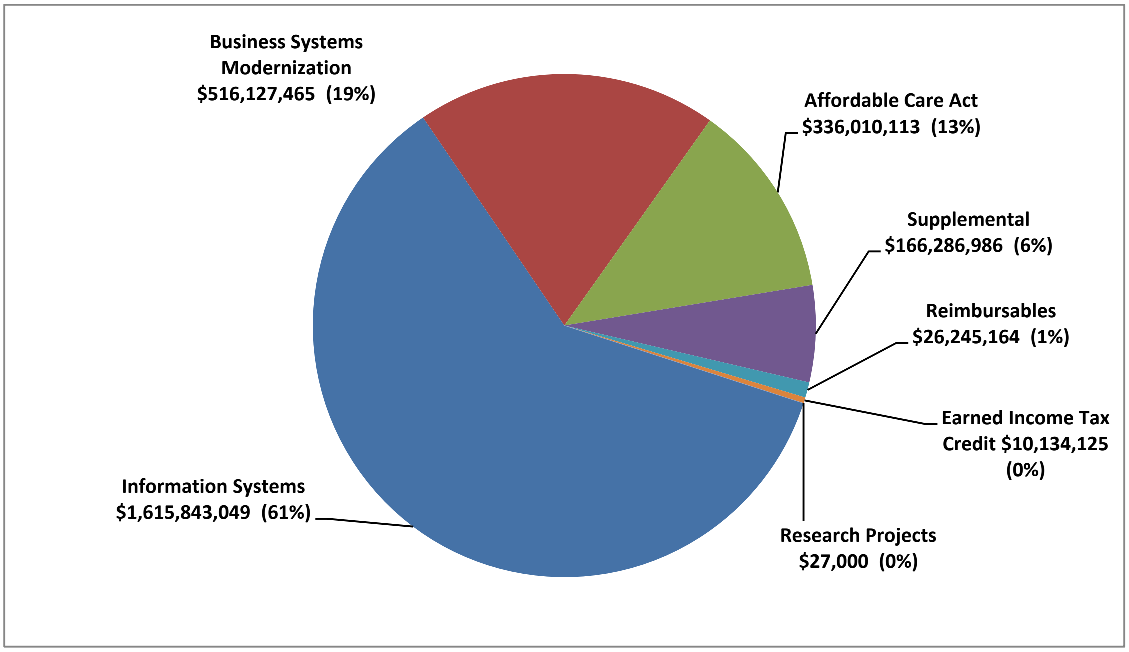
Figure 1: IRS IT Organization FY 2015 Total Available Funding (by ACIO Organization)[3]



Source: Our analysis of the IRS IT organization budget data as of July 2015, based on information provided by the ACIO, Strategy and Planning, Financial Management Services.

[3] The proportions of funding by ACIO areas or ACIOs with Business Systems Modernization funding are overstated because not all of these funds will be spent this year.

Figure 2: IRS IT Organization FY 2015 Total Available Funding (by Funding Source)[4]



Source: Our analysis of the IRS IT organization budget data as of July 2015, based on information provided by the ACIO, Strategy and Planning, Financial Management Services.

As of July 2015, the IRS IT organization has 7,042 employees, of which 6,916 work in the following seven ACIO offices:

- 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 the delivery of integrated solutions for several of the IRS's large-scaled programs. It plays a key role in establishing configuration management and release plans and implementing new information system functional capabilities.
- 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.

[4] The Business Systems Modernization account includes funds appropriated over three years and will not all be obligated during the current year.

- Enterprise Services is responsible for strengthening technology infrastructure across the enterprise.
- Strategy and Planning collaborates with IT organization leadership to provide policy, direction, and administration of essential programs, including strategy and capital planning, strategic planning and performance measurement, financial management services, vendor and contract management, requirements and demand management, and risk management.
- 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 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.

Figure 3 presents the number of IT organization employees in each business unit as of July 2015. At this time last year, the IRS IT organization employed 7,339 employees, nearly 300 more full-time personnel than this year.

Figure 3: Number of IT Organization Employees by Business Unit (in Descending Order by Number of Employees)

IT Organization Business Unit	Number of Employees
Applications Development	2,019
Enterprise Operations	1,839
User and Network Services	1,534
Enterprise Services	676
Cybersecurity	344
Strategy and Planning	256
Enterprise Program Management Office	248
Management Services	115
Office of the Chief Technology Officer	11
Total	7,042

Source: Treasury Integrated Management Information System as of July 2015.

The remaining 126 employees work in the Management Services business unit or support the Office of the Chief Technology Officer (CTO). The Management Services business unit partners with IRS IT organization leadership to define and implement human capital policies and guidance to ensure that employees are supported in the fashion necessary to deliver outstanding service. IRS IT organization leadership also partners with the Privacy, Governmental Liaison, and Disclosure (PGLD) organization to ensure that data loss incidents involving taxpayer information are investigated, analyzed, and resolved. The Office of the CTO includes the CTO, two Deputy Chief Information Officers, and their staff. A Deputy Chief Information Officer serves as principal advisor to the CTO and provides executive direction and focus to help the organization increase its effectiveness in delivering information technology services and solutions that align to the IRS's business priorities.

The compilation of information for this report was conducted at the TIGTA office in Dallas, Texas, during the period June through September 2015. The information presented is derived from TIGTA audit reports issued between October 1, 2014, and September 30, 2015. We also reviewed relevant Government Accountability Office (GAO) reports and IRS-issued documents relating to IRS information technology plans and issues. These audits and our analyses were conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. 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 list of TIGTA audit reports used in this assessment is presented in Appendix IV.

Results of Review

During this annual review, we summarize information from IRS IT organization program efforts in systems security, modernization, and operations as required by the IRS Restructuring and Reform Act of 1998. Overall, the IRS needs to ensure that it leverages viable technological advances as it modernizes its major business systems and improves its overall operational and security environments. Otherwise, the IRS's computer operations could become compromised, disrupted, or outdated, which could adversely affect the IRS's ability to meet its mission of providing America's taxpayers with top-quality service by helping them understand and meet their tax responsibilities and enforcing the law with integrity and fairness to all.

Cybersecurity Remains a Major Challenge

For FY 2015, TIGTA designated Security for Taxpayer Data and Employees as the IRS's number one management and performance challenge for the fifth consecutive year. The IRS faces the daunting task of securing its computer systems against the growing threat of cyberattacks. Beyond the cyber threat, effective information systems security is 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.

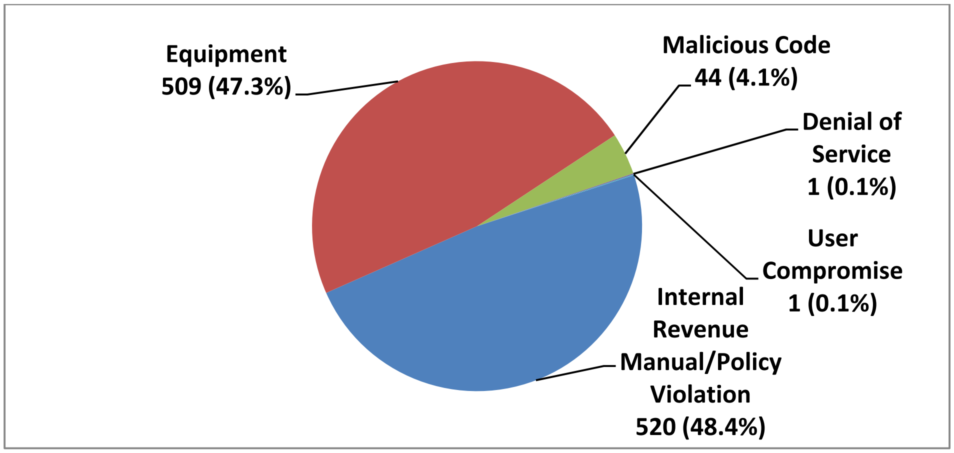
Protecting the confidentiality of this sensitive information is paramount. Otherwise, taxpayers could be exposed to loss of privacy and to financial loss and damages resulting from identity theft or other financial crimes. According to the FY 2014 Office of Management and Budget report to Congress,[5] 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.

Over the past several years, the IRS has steadily matured its approach to implementing information security—moving from a reactive to a proactive risk-based management approach. In addition, legislative and regulatory security requirements continue to evolve that directly affect the programs and associated initiatives undertaken by the IRS to mature and maintain an effective security program. In November 2014, the IRS updated its IT Security Program Plan in support of attaining its security objectives and communicating its security efforts across the IRS community. This plan serves as a roadmap and a basis for benchmarking information security performance towards the attainment of its security objectives.

[5] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act* (Feb. 27, 2015).

The number of cyber incidents affecting Federal Government agencies increased approximately 15 percent in FY 2014, when agencies reported nearly 70,000 cyber incidents to the U.S. Computer Emergency Readiness Team (USCERT). The USCERT receives computer security incident reports from the Federal Government, State and local governments, commercial enterprises, U.S. citizens, and international Computer Security Incident Response Teams. More specifically, from August 1, 2014, to July 31, 2015, the IRS shared with us that it reported 1,075 security incidents to the USCERT. Figure 4 shows the categories for each incident.

Figure 4: Number of Security Incidents the IRS Reported to the USCERT From August 1, 2014, to July 31, 2015



Source: IRS Cybersecurity Operations organization as of August 2015.

Security and Privacy of Federal Tax Information

The IRS is an attractive target to hackers due to its large amounts of tax data and negative connotations of being the Nation's tax administrators. Whether it pertains to defending its networks, detecting when incidents occur, or remediating those incidents, the IRS takes the protection of taxpayer privacy very seriously as will be demonstrated by our summary of audits throughout this assessment. As one example of the IRS's commitment to being accountable to taxpayers, during Calendar Year 2014, the IRS sent 20,947 letters to taxpayers informing them that their personal information was potentially disclosed, costing the IRS more than $149,000 in redeemed credit monitoring services. One single incident accounted for 18,782 of the letters sent to taxpayers and cost the IRS more than $139,000.

More recently, in May 2015, the IRS announced that criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts through its "Get Transcript" application. In August 2015, the agency disclosed a more extensive retroactive investigation into the matter showing that crooks compromised about 220,000 additional taxpayer accounts. The data included Social Security information, date of birth, and street address. These third parties gained sufficient information from an outside source before trying to access the IRS site, which allowed them to clear a multistep authentication process, including several personal verification questions that typically are known only by the taxpayer. IRS officials reported that criminals have used some of the stolen data to illegally claim tax refunds totaling about $39 million. The matter is under review by IRS Criminal Investigation. The following four audits highlight the risks associated with inadequate security protections.

Federal Information Security Modernization (FISMA) Act of 2014

The Office of Management and Budget relies on annual FISMA metrics to assess the implementation of agency information security capabilities and to measure overall program effectiveness in reducing risks. For Inspectors' General use in assessing Federal agency information security programs, the Department of Homeland Security issued the *Fiscal Year 2015 Inspector General Federal Information Security Management Act Reporting Metrics* on June 19, 2015, which contained 10 information security program areas for Inspectors General to assess.[6] TIGTA found that significant improvements were needed in the following three IRS program areas that failed to meet FISMA requirements overall.[7] These program areas were missing many performance attributes specified by the Department of Homeland Security to meet FISMA requirements.

- *Continuous Monitoring Management*

  The IRS Continuous Monitoring Management program is at a maturity level of one on a scale of one to five. The IRS is still in the process of implementing its Information Security Continuous Monitoring program required by the Office of Management and Budget to automate asset management and maintain secure configuration of these assets in real time. In July 2014, the Department of the Treasury decided to adopt a uniform approach across the Treasury and to use the toolset selected by the Department of Homeland Security to meet the program requirements. The Department of Homeland Security is in the process of procuring a standard set of cybersecurity tools and services for use by Federal agencies, expected to be completed in August 2015. This toolset will include sensors that perform automated searches for known cyber flaws and send the results to dashboards that inform system managers in real time of cyber risks that need remediation. When implemented, the Information Security Continuous Monitoring program is intended to provide security automation in 11 domains: Vulnerability Management, Patch Management, Event Management, Incident Management, Malware Detection, Asset Management, Configuration Management, Network Management, License Management, Information Management, and Software Assurance.

[6] The 10 information security program areas are: Continuous Monitoring Management, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, Plan of Action and Milestones, Remote Access Management, Contingency Planning, and Contractor Systems.
[7] See Appendix IV, number 9.

- *Configuration Management*

  The Configuration Management program did not meet a majority of the attributes specified by the Department of Homeland Security. Although the IRS has tools that discover assets, evaluate configuration policy, and scan the enterprise to detect vulnerabilities, these processes have not been fully implemented enterprise-wide and still rely on many tedious manual procedures. In addition, the IRS is still working to expand a standard automated process to deploy operating system patches enterprise-wide. Eventually, the IRS's Configuration Management program will benefit from the implementation of the Information Security Continuous Monitoring program, which intends to automate configuration management in real time for the universe of IRS assets.

- *Identity and Access Management*

  The Identity and Access Management program did not meet a majority of the attributes specified by the Department of Homeland Security, largely due to the IRS not achieving Governmentwide goals set for implementing logical (system) and physical access to facilities in compliance with Homeland Security Presidential Directive 12 requirements. Homeland Security Presidential Directive 12 requires Federal agencies to issue personal identity verification cards to employees and contractors for accessing agency systems and facilities. The IRS had not resolved existing challenges to achieving full compliance with the directive.

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program areas in compliance with FISMA requirements, taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure.

Privacy Impact Assessments (PIA)

Among the most basic of taxpayers' and employees' rights is an expectation that the IRS will protect the confidentiality of personal, financial, and employment information. A PIA is a process for examining the risks and ramifications of using information technology to collect, maintain, and disseminate information in identifiable form, such as Social Security Numbers, about members of the public and agency employees. In addition, the PIA identifies and is used to evaluate protections to mitigate the impact to privacy of collecting such information. A PIA is required to be performed and updated every three years or when a major system change creates new privacy risks. In November 2013, the Department of the Treasury issued guidance that expanded the scope of the PIAs to include questions on civil liberties. As a result, most PIAs are now referred to as the Privacy and Civil Liberties Impact Assessment. Within the IRS, the PGLD organization has overall responsibility for privacy issues. The Privacy Policy and Compliance office, within the PGLD organization, promotes the protection of individual privacy and integrates privacy into business practices, behaviors, and technology solutions. The specific group responsible for oversight of the PIA process is the Privacy Compliance and Assurance office. The PIA Management System supports the PIA program. To comply with applicable laws and regulations governing privacy, the IRS requires system owners to submit all new Privacy and Civil Liberties Impact Assessments through the PIA Management System.

The Internal Revenue Manual provides that Personally Identifiable Information be released to only those individuals having a need to know the information in the performance of their duties. The security principle of least privilege, which allows for only authorized accesses that are necessary to accomplish assigned tasks, should be implemented for managing access to shared network drives. During our audit,[8] TIGTA determined that the Privacy Compliance and Assurance office was unable to provide authorizations supporting access to the PIA Management System for 27 (93 percent) of 29 users with elevated privileges and changed the user roles and account statuses for 10 (34 percent) of the 29 users. In addition, after TIGTA brought it to its attention, the PGLD office removed 12 (29 percent) of 41 users' accesses to its shared drive because they no longer had a business need. In March 2015, the contractor for the PIA Management System added a new feature to disable user accounts.

During our independent testing, which included creating a fictitious Privacy and Civil Liberties Impact Assessment in a simulated process, TIGTA identified enhancements that could improve the assessment process. The enhancements included routing the assessment back to the manager for review and approval after changes are made to the Privacy and Civil Liberties Impact Assessment and requiring a negative response when no sensitive information is identified in the assessment prior to the disclosure review for redaction. The Privacy Compliance and Assurance office plans to implement all of our enhancements except requiring a negative response from the system owner. During our review, we also determined that the PGLD organization prepared eight documents for standard operating procedures. However, five of these documents have not been finalized nor incorporated in the new Internal Revenue Manual.

External connections

The IRS shares Federal tax information and other IRS records with many Federal, State, and local agencies as well as private agencies and contractors through system interconnections. The exchange of information may facilitate joint tax administration relationships, enable tax collection processes with financial institutions, or provide information needed for a variety of tax administration purposes. Interconnecting information technology systems can expose the participating organizations to risk. If the interconnection is not properly designed, security failures could compromise the connected systems as well as the data that they store, process, or transmit. It is critical, therefore, that both parties learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. It is also critical that they establish an agreement between themselves regarding the management, operation, and use of the interconnection and that they formally document this agreement. The agreement should be reviewed and approved by appropriate senior staff from each organization. The IRS must ensure that these system

[8] See Appendix IV, number 6.

interconnections are authorized by written agreements that specify the technical and security requirements for the interconnection before information is shared.[9] Both of the interconnected systems must meet IRS protection requirements in order to ensure that taxpayer and other sensitive data are secure.

The National Institute of Standards and Technology prescribes that two documents may be developed to govern the interconnection: a Memorandum of Understanding (MOU) or Agreement (or an equivalent document) and an Interconnection Security Agreement based on the relevant technical, security, and administrative issues. The MOU documents the terms and conditions for sharing data and information resources in a secure manner. The Interconnection Security Agreement is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. The IRS Information Technology Office of Cybersecurity is responsible for managing the IRS's Information Technology Security Program and ensuring the IRS's compliance with Federal statutory, legislative, and regulatory requirements. Within the Cybersecurity organization, the Security Assessment Services office provides oversight and guidance for the documentation of IRS interconnections in the MOUs and Interconnection Security Agreements.

At the time of our audit,[10] the Security Assessment Services office's inventory of interconnections consisted of 49 external partners. Despite the efforts from all participating individuals and offices on external interconnections, we found that 34 (69 percent) interconnections in use did not have proper authorization or security agreements, and the IRS does not have a method to identify and maintain an up-to-date inventory of its interconnections. We also found that the MOUs lacked consistency and uniformity. The Security Assessment Services office stated its focus has been on the Interconnection Security Agreements, and it has not given the MOUs as much priority. Rather, the Security Assessment Services office defers responsibility for the MOUs to the IRS business owners of the interconnected systems. When the MOUs do not meet IRS policies, the IRS may be unable to hold the external partner fully accountable for maintaining secure interconnections.

Although the IRS has established an office to provide oversight and guidance for the development of security agreements, that office is not responsible for managing or monitoring agreements for all external interconnections in use in the IRS environment. We believe the lack of a centralized inventory and an enterprise-level approach to ensure that all external interconnections are monitored has contributed to interconnections that are currently active but lack proper approvals and assurances that the interconnections meet current security

[9] Office of Management and Budget Circular A-130 (Revised), *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (Nov. 2000), states the requirement for Federal agencies to obtain written management authorization before connecting their information technology systems to other systems, based on an acceptable level of risk. It also requires that where a connection is authorized, controls must be established which are consistent with the rules of the system and in accordance with National Institute of Standards and Technology guidance.
[10] See Appendix IV, number 7.

requirements.

Audit trails and unauthorized access

Audit trails contain a record of events occurring on a computer from system and application processes as well as from user activity. In essence, audit trails should provide information as to what events occurred, when the events occurred, and who (or what) caused the events. This information can allow an organization to reconstruct events, monitor compliance with security policies, identify malicious activity or intrusion, and analyze user and system activity. Maintaining sufficient audit trails is critical to establishing accountability over users and their actions within information systems. Due to the sensitive nature of tax return information, the IRS is required by law to detect and monitor the unauthorized access and disclosure of taxpayer records. Without sufficient audit trails, the IRS may be unable to identify or substantiate noncompliant activity that puts taxpayer records at risk.

National Institute of Standards and Technology, Department of the Treasury, and IRS policies contain requirements for the capture, storage, transmission, review, and retention of audit trails. These policies require that audit trails be sufficient in detail to facilitate the reconstruction of events if unauthorized activity occurs or is suspected on IRS systems. To coordinate an enterprise solution for audit trail weaknesses, the IRS established the Enterprise Security Audit Trail (ESAT) Project Management Office within its Cybersecurity organization in March 2010. The ESAT office's mission is to resolve the IRS's systemic audit trail issues by managing all enterprise audit initiatives and overseeing the deployment of various audit trail solutions that meet the required standards for legacy and newly deployed systems. The ESAT office designated the Security Audit and Analysis System as the IRS's enterprise solution to collect audit trails from systems that store or process taxpayer information. Security Audit and Analysis System data can be accessed by those responsible for reviewing questionable activities and investigating potential unauthorized access (UNAX) violations.

TIGTA's Office of Investigations investigates an average of nearly 400 UNAX violations each year. Even so, the Office of Investigations has expressed concerns to IRS management with the large number of applications not yet sending audit trails to the Security Audit and Analysis System, which creates a UNAX detection gap. The Office of Investigations has informed IRS management that the majority of the 83 applications that the Office of Investigations has determined to be subject to UNAX risk do not yet transmit audit trails to the Security Audit and Analysis System. At the time of this audit, the Office of Investigations had evaluated 10 of 32 unique audit trails that are being sent to the Security Audit and Analysis System and determined that only four of the 10 were usable for UNAX investigations.

A completed audit plan is a key first step in the goal of having usable audit trails. Audit plans provide the framework that describes what type of audit trail data will be captured and how the data interface with other systems. However, the audit plan is just a plan, and having a completed audit plan does not mean the audit trails are being captured as intended. The Internal Revenue Manual states that new systems or applications that require audit plans shall not be deployed without an approved audit plan fully implemented and tested through the enterprise life cycle (ELC) process.

However, the majority of the new projects we reviewed[11] did not meet this standard. From October 2011 to November 2014, the ESAT office determined that 29 projects should complete audit plans. Of those 29, only eight had signed audit plans at the completion of the ELC process. Of those eight projects, only two also had an interface control document, which is needed to transmit to the Security Audit and Analysis System. This resulted in systems being put into production without fully functional audit trails.

Furthermore, we found that new projects that are related to legacy systems are not always held to the same standards as brand new systems in regards to contacting the ESAT office or developing audit plans during the ELC process. The FISMA Certification Program Office may allow legacy systems to exit and deploy new releases without completing audit plans. Currently, there is no formal control to ensure that project offices have contacted the ESAT office and actually obtained its input or had their projects assessed by the ESAT office. Consequently, the ESAT office expressed concern that project offices may just fill out the audit plan template with a minimal amount of information without being fully aware of the audit trail requirements they should be planning to have in place. Without the ESAT office's assessment of audit trail requirements early in the ELC process, new projects may deploy without proper audit trails required for UNAX investigations or other purposes.

In addition to the requirement for an audit plan, interface control documents are required for each application that must transmit audit trails to the Security Audit and Analysis System. This system collects, stores, and reports audit trail data for the investigation of potential instances of UNAX violations against IRS computer systems. The interface control document defines the mandatory fields and describes how the fields will be populated by the application. We reviewed the status of the interface control documents for the eight projects that had signed audit plans and an additional 13 projects that had substantially completed audit plans. Our analysis showed that for 15 of the 21 projects, the interface control document had not been started or was still in process. Consequently, many projects resulted in systems being put into production without fully functional audit trails. Some of these systems may have had separate application-level audit trails that were kept outside the Security Audit and Analysis System, but these audit trails would not have met the IRS's requirements for UNAX-compliant audit trails.

The ESAT office began documenting the audit trail deficiencies it identified in system audit plans and instructing system owners to create a Plan of Action and Milestones (POA&M) for tracking progress to correct them. The ESAT office also began to issue an audit notification memorandum to the system owners to highlight the need to correct the deficiencies or create POA&Ms within 60 calendar days. From May 2014 to January 2015, the ESAT office issued 10 audit notification memorandums. Of the 10 system owners who received the audit

[11] See Appendix IV, number 8.

notification memorandum, seven did not report deficiencies in the POA&M within the 60 calendar days. When audit trail deficiencies are not placed into the POA&Ms, the deficiencies are allowed to persist without visibility to higher level IRS management who monitor the status of IRS security weaknesses, which could lead to these deficiencies persisting indefinitely. Consequently, with audit trail deficiencies remaining unresolved, IRS management may be unable to identify or substantiate noncompliant activity or hold employees accountable to UNAX policies.

Overall, the IRS continues to make progress in implementing its enterprise solution to address its audit trail deficiencies. The ESAT office developed a strategic plan to correct the IRS's enterprise audit trail deficiencies and to help close the UNAX detection gap. However, the IRS needs to strengthen controls in its new systems development and deficiency remediation processes to improve the number and quality of its audit trails. Without fully operational audit trails, unauthorized accesses could be made within these systems and may not be detected.

Information Systems to Combat Identity Theft and Tax Fraud

Identity theft and tax refund fraud occurs when an identity thief uses a legitimate taxpayer's identifying information to file a fraudulent tax return and claim a refund. Undetected tax refund fraud, including identity theft, has a significant impact on tax administration. Tax fraud is a major challenge for the IRS. The IRS estimated it prevented $24.2 billion in fraudulent identity theft refunds in Filing Season 2013, but paid $5.8 billion later determined to be fraud. Because of the difficulties in knowing the amount of undetected fraud, the actual amount could differ from these point estimates. Implemented in 1994, the Electronic Fraud Detection System (EFDS) remains the IRS's primary frontline system for detecting fraudulent returns. The IRS reports that the long-term limitations of the EFDS include its inability to keep pace with increasing levels of fraud or to serve the organization's evolving compliance needs. In February 2009, the IRS chartered the initiation of a new program called the Return Review Program (RRP). The IRS plans to replace the EFDS with the RRP. The Wage and Investment Division is responsible for RRP requirements development, risk management, governance, project management, and deployment support. Criminal Investigation is responsible for supporting the RRP by identifying and developing schemes to refer and support high-impact criminal tax and related financial investigations.

The RRP

The RRP is a web-based automated system that uses leading edge technologies to enhance IRS capabilities to detect, resolve, and prevent criminal and civil noncompliance. The RRP models flagged potential identity theft fraud not detected by the EFDS models. During its pilot from April to November in 2014, the RRP identified 51,946 returns as potential identity theft cases. The IRS confirmed that 41,311 of the 51,946 returns were identity theft. Of the confirmed identity theft cases, the IRS determined that 10,348 (25 percent) cases, totaling $43 million in refunds, were not detected by the EFDS or other systems.

In addition, through July 2014, the RRP pilot identified approximately one million potentially fraudulent returns. Almost 350,000 of those potentially fraudulent returns were not detected by the EFDS. Figure 5 provides a breakdown of the confirmed fraudulent tax returns identified.

Figure 5: Confirmed Fraudulent Tax Returns Identified (March 2014 Through July 2014)

Tax Fraud Identified by System	Number of Confirmed Fraudulent Tax Returns	Refund Amount (in Millions)
Detected by RRP Models and Detected by EFDS Models	668,470	$9,154
Detected by RRP Models; Not Detected by EFDS Models	220,508	$1,001
Detected by RRP Linked Return Analysis; Not Detected by EFDS Models	128,490	$470

Source: *IRS RRP Predictive Analytics Performance Report Detection Summary.*

One reason the RRP detected more fraud is that the EFDS focuses on income, withholding, and prior year fraud examples, whereas the RRP uses data from a broader number of sources. Using the analytics capability in the RRP, the IRS can create predictive fraud and noncompliance detection models that will seek out subtle data patterns to determine reliability of return data, including the filer's identity. The RRP generates a scorecard for questionable returns, evaluating consistency and dependability. The RRP system is comprised of three major components:

Detection – This part of the system incorporates several existing models as well as new models. By using algorithms and business rules, the system detects errors on the tax return as the return is filed and routes the return to the correct treatment stream, thereby allowing the taxpayer to receive one notice with all the issues that must be resolved before the refund is released. The system also detects returns with potential fraud characteristics and routes those returns to the treatment stream, which allows Criminal Investigation to associate/link and analyze groups of returns to identify schemes for potential criminal prosecution.

Resolution – This part of the system contains existing treatment streams as well as new treatment streams. Returns are routed systemically to a treatment stream and opened into that treatment stream's inventory. In addition, initial contact letters are sent to the taxpayer.

Prevention – This part of the system allows the results of the resolution to be sent and updated into the detection models systemically. Both outreach and education inventory can be selected through the system to allow for early intervention to stop the noncompliance before the next filing season. It also allows for the analysis of additional fraud not identified by the detection models.

In contrast, EFDS processing minimally uses predictive analytics. For the 2014 Filing Season, the EFDS employed 15 models. In comparison, the RRP enables the IRS to employ 34 models in production. Additionally, the RRP generates 15 scores for each return to identify potential fraud, whereas the EFDS generates only one score per return. Based on the success of the 2014 RRP Identity Theft pilot, the IRS received approval for the 2015 Filing Season to expand the RRP Identity Theft pilot to run daily instead of weekly. Furthermore, tests showed that eight million returns can be loaded into the RRP per day, meeting stated capacity requirements.

In addition, patch management is an important element in mitigating the risks associated with known vulnerabilities. When vulnerabilities are discovered, the vendor may release an update to mitigate the risk. If the software update is not applied in a timely manner, an attacker may exploit a vulnerability not yet mitigated, enabling unauthorized access to an information system. We found system security vulnerabilities were not fully remediated in the RRP.[12] Three different vulnerability scans found issues on the RRP servers currently running because the IRS had not applied critical patches within the required time frames to servers and databases supporting the RRP system. The Internal Revenue Manual requires the IRS to implement patches for critical vulnerabilities within 72 hours, while patches for high vulnerabilities should be implemented within five business days. By not installing critical patches in a timely fashion, the IRS increases the risk that known vulnerabilities in its systems may be exploited.

A successful RRP system is critical to the IRS's mission because it will be the key automated component of the IRS's pre-refund initiative. The RRP system will implement the IRS's new business model for a coordinated criminal and civil tax noncompliance approach to prevent, detect, and resolve pre-refund tax fraud.

No termination date or retirement plan for the EFDS

The IRS is developing the RRP to replace the EFDS due to the older system's fundamental limitations in technology and design. However, the IRS has not set a termination date nor established a retirement plan for the EFDS. The EFDS is modified annually to accommodate legislative changes as well as other required database and application modifications. Making these changes effectively and efficiently requires expert knowledge of the database software products used by the EFDS project and its customers. Supporting this effort includes designing solutions, troubleshooting, and implementing best practices as well as documenting these efforts and their impact. This annual system modification effort is more time consuming, costly, and hands-on than a web-based solution, such as the RRP. As stated in the IRS's FY 2015 Congressional Budget Submission, the EFDS is vulnerable to structural failure and potentially the inability to detect up to $1.5 billion in fraudulent refunds each year that it is not replaced.

[12] See Appendix IV, number 5.

The EFDS is no longer capable of keeping pace with the levels of fraud and increasing business demands. Refundable credits are among the most popular targets for fraud. If the IRS does not efficiently transition to the RRP so that it can retire the EFDS, the estimated additional operation and maintenance costs of running the EFDS could cost taxpayers approximately $18.2 million per year.[13]

Information Technology Infrastructure and Application Upgrades

The IRS relies extensively on information systems to annually collect more than $3 trillion in taxes, distribute more than $370 billion in refunds, and carry out its mission of providing service to America's taxpayers in meeting their tax obligations. For FY 2014, the IRS expected to spend about $2.4 billion on information technology. Given the size and significance of the IRS's information technology investments and the challenges inherent in successfully delivering these complex systems, it is important that Congress be provided reliable cost, schedule, and scope information to assist with its oversight responsibilities.

Accordingly, the Senate Appropriations Committee directed the GAO to review the cost and schedule performance of the IRS's major information technology investments. The GAO reported that some investments experienced variances from initial cost, schedule, and scope plans that were not transparent in congressional reporting because the IRS has yet to address GAO's prior recommendations.[14] Specifically, the RRP previously discussed has so far exceeded planned costs by $86.5 million and has yet to deliver functionality that was scheduled for September 2012, and a key phase of the Customer Account Data Engine (CADE) 2 was developed 10 months late and at $183.6 million more than planned. In addition, the following information from four TIGTA audits highlights the risks associated with infrastructure and application upgrades and operations.

Windows workstation and server upgrades

Operating systems are critical software on computers that serve as a foundation to allow all other programs, software, and applications to run on the computers. Operating systems must be updated on a regular basis to patch security vulnerabilities and, if necessary, upgraded completely in order to fix crucial weaknesses or to address new threats to its functionality. The older an operating system gets, the more security vulnerabilities it has, and at some point, software companies such as Microsoft stop supporting the software with new patches, leaving the systems vulnerable to attack. Windows XP for workstations and Windows Server 2003 for servers are Microsoft operating systems that have reached their end of life. That means Microsoft made a business decision to stop supporting these operating systems effective April 2014 and July 2015, respectively, and encourage customers to upgrade to more current

[13] See Appendix IV, number 12.
[14] GAO, GAO-15-297, *Information Technology: Management Needs to Address Reporting of IRS Investments' Cost, Schedule, and Scope Information* (Feb. 2015).

versions of its operating systems. For organizations that do not upgrade their Windows computers by the end-of-life deadline, Microsoft offers support for these systems on a contracted fee basis.

The IRS was unable to upgrade all of its Windows workstations from Windows XP and all of its Windows servers from Windows Server 2003 by the Microsoft end-of-life deadlines.[15] We acknowledge that these Windows upgrade efforts were monumental and unprecedented for the IRS, particularly with the Windows XP upgrade due to its volume of approximately 110,000 workstations and geographical disbursement throughout the country. In addition, budgetary constraints at the start of the Windows XP upgrade effort in April 2011 forced the IRS to upgrade old computers rather than purchase new computers, which would have made the upgrade process easier due to the compatibility of new hardware with new operating systems. Furthermore, the IRS discovered nearly 6,000 applications being used by employees to do their jobs that required an assessment of each application to determine whether it would operate on Windows 7. So far, the IRS has spent almost $128 million over the past four years on its effort to upgrade Windows XP to the Windows 7 operating system and expects to spend an additional $11 million through the end of FY 2015, for a total project cost of $139 million.

This information technology project is unique at the IRS because the CTO made the decision to oversee the Windows 7 upgrade directly due to its complexity and magnitude. Information technology projects at the IRS are typically overseen by an executive steering committee. The primary objective of the executive steering committee is to ensure information technology infrastructure investment, program, and project objectives are met; risks are managed appropriately; and the expenditure of enterprise resources is fiscally sound. However, the CTO decided to bypass IRS ELC policy and important risk mitigation controls. No ELC documents or artifacts were created or signed after the initial project charter document, which was approved in April 2011. The IRS ELC policy outlines the repeatable processes and deliverables that IRS project managers are required to follow in order to mitigate risks when implementing information systems initiatives. Without the ELC or maintaining similar project documentation that provides version control and digital signatures, projects and initiatives run the risk of delays and less transparency and accountability, resulting in difficulty in assessing whether money could have been saved through alternative choices. Therefore, we concluded that management should have followed established policy by using the ELC process in the Windows 7 enterprise-wide upgrade effort. While the CTO's decision may have been made to ensure high-level emphasis and attention, the IRS was unable to show and prove that decisions were made after appropriate discussion and considerations of various factors.

[15] See Appendix IV, number 10.

The IRS is about halfway through upgrading its Windows 2003 servers to the 2008 release of the Windows Server operating system and is now preparing for the 2012 software upgrade. The IRS has not yet begun the upgrade to Windows Server 2012 and is in the initial planning stages for developing project budget estimates and other planning documents. Approximately 3,000 Windows 2003 servers continue to be delayed for upgrade. The IRS stated that it is not certain this number is correct because when many of these servers were deployed, inventory controls were not in place and it is not certain all of these servers are running the Windows 2003 version of the operating system.

Management informed us that they have upgraded approximately 4,100 Windows servers to the 2008 version, which is already seven years old. The IRS currently has no servers running the 2012 version in production and will not deploy any with the 2012 operating system until testing is complete. The server upgrade project team has completed no ELC documents because they are treating this effort as a refresh or upgrade—not a development project—as directed by Enterprise Operations organization management.

Similar to the Windows 7 effort, the Windows server upgrade lacks sufficient oversight and accountability, and delays in upgrading pose a realistic risk of weakening the IRS security posture. The IRS will begin paying a premium for extended service on an outdated server operating system that no longer receives critical security upgrades automatically from the vendor. As a result, we determined that the IRS has not adequately planned for the Windows server upgrade in terms of what it will cost, the potential security implications, and the amount of time necessary to complete the upgrade. Consequently, we have no assurance that this server update will be completed anytime soon. External hackers or malicious insiders need to locate only the one computer with security weaknesses to exploit, such as one with an outdated operating system, in order to steal data or further compromise other computers.

Integrated Enterprise Portal

The IRS strives to provide one-stop, web-based services for the general public, Federal agencies, and tax professionals from multiple channels. Prior to August 2012, there were three distinct IRS portals supporting the IRS user communities. One of the IRS's goals is to transform the technology platform for the three portals to one that is shared, which will lower its total cost of ownership. The modernized platform will also enable the IRS to provide enhanced online services to taxpayers. The Integrated Enterprise Portal serves as a preferred channel for interactions with the IRS, is currently the primary information source for taxpayers and tax professionals, and plays a central role in advancing taxpayer issue resolution, providing timely guidance and outreach, and improving service interactions for all taxpayers.

In May 2011, the IRS entered into a 10-year contract (five base years, five option years) with a third party for managed web portal services. The contract has an overall ceiling price of $320 million. The maximum aggregate dollar value of task orders awarded to the contractor cannot exceed the established contract ceiling. In the managed service contract, the contractor is to provide daily operational and maintenance services for the Integrated Enterprise Portal and the Employee User Portal. In our review, we identified instances in which the IRS did not always review, verify, and maintain appropriate invoice documentation prior to releasing payment for contractor services.[16] TIGTA's review of the three contractor invoices for January, February, and March 2014 showed 161 instances in which hours were billed for work performed by contractor employees outside the invoice period of performance. In addition, TIGTA found multiple contractor employees who billed more than 240 hours in a month that potentially resulted in $405,679 in additional labor costs.

CADE 2 Transition State 2

During this annual assessment cycle, TIGTA evaluated the IRS's approach and progress toward developing system requirements that will address the IRS financial material weakness with Transition State 2 of the CADE 2 system.[17] Since 1993, the GAO has reported a recurring financial material weakness in the IRS internal control over unpaid tax assessments. The Federal Financial Management Improvement Act of 1996[18] requires the IRS to complete a remediation plan to address material weaknesses that includes remedies (planned corrective actions), estimated and actual resources, and target dates to bring its financial systems into compliance.

Our system development audit considered key milestones and progress for the IRS financial material weakness effort to ensure effective management and direction, determined the status of the preliminary financial system requirements for the financial material weakness effort under CADE 2 Transition State 2, considered expected costs and benefits associated with the financial material weakness, and identified and reviewed the key risk mitigation controls related to CADE 2 if it is considered a Federal financial management system.

The IRS is currently planning activities for CADE 2 Transition State 2 to address the financial material weakness for individual taxpayer accounts. However, the review identified conditions, within four overall risks areas for this important initiative, for which additional controls are needed to ensure long-term success: 1) the IRS Remediation Plan does not include the Transition State 2 actions for addressing the financial material weakness; 2) the cost estimates specific to Transition State 2 activities for addressing the weakness are not in place; 3) a security strategy is needed to support Transition State 2 development as an authoritative source of data; and 4) the current system classification for the CADE 2 does not provide sufficient guidance for Transition State 2 activities to address the IRS financial material weakness.

[16] See Appendix IV, number 2.
[17] See Appendix IV, number 1.
[18] Pub. L. No. 104-208, 110 Stat. 3009.

Systems Development Supporting the Affordable Care Act

Among the ongoing challenges of technological advancement and system and software upgrades, the IRS must also address legislative changes that affect the tax code and its administration. In March 2010, the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act (collectively referred to as the Affordable Care Act (ACA))[19] were enacted. The ACA is intended to make health insurance more affordable and available to individuals. It contains comprehensive health insurance reforms for both individuals and employers and establishes a new health insurance marketplace (Exchanges) from which health insurance coverage can be purchased. The IRS administers the law's numerous tax provisions. The IRS estimates that the ACA includes approximately 50 tax provisions, and at least eight of the 50 provisions require the IRS to build new computer applications and business processes that do not exist within the current tax administration system. Beginning in January 2015, the IRS began receiving individual tax returns (and information returns from health insurance Exchanges, health insurance companies, and employers) that pertain to the Premium Tax Credit and to individual and employer shared responsibility coverage.

Coverage Data Repository

The IRS is developing the Coverage Data Repository to help implement the ACA, and it will be the IRS's sole authoritative source of all ACA data for health care–related functions and services. The Exchanges are intended to provide a place for Americans to shop for health insurance in a competitive environment. The term Exchanges refers to the Federal Exchange, the State Partnership Exchanges, and the State Exchanges. To enroll in health insurance coverage offered through an Exchange, individuals must complete an application and meet certain eligibility requirements defined by the ACA. During the 2015 Filing Season, the IRS received Exchange Periodic Data from the Exchanges, stored the data in the Coverage Data Repository, and used them to verify the accuracy of the Premium Tax Credits claimed by taxpayers. The IRS has identified the Coverage Data Repository as one of six core systems being developed to implement the ACA legislation, and it will be used by all IRS ACA systems to store and retrieve data. The IRS established the IT ACA Program Management Office to ensure a dedicated focus on fulfilling the ACA requirements. Specifically, the IT ACA Program Management Office is responsible for planning and managing information technology responsibilities related to ACA implementation and the myriad of legislative requirements.

The systems development review considered how risks for the Coverage Data Repository Project were being mitigated and whether established business and information technology requirements were being met. Risk areas evaluated included Coverage Data Repository testing processes,

[19] The Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections 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.

including interagency, release-level, and project-level functional testing controls as well as security and audit trail controls. The review found that the IRS did not receive all required Exchange Periodic Data submissions from the Exchanges as of January 20, 2015, the start of the 2015 Filing Season. Release-level testing was completed but not prior to initiating interagency testing with the Centers for Medicare and Medicaid Services (CMS). During project-level testing, system developers did not always demonstrate Coverage Data Repository functionality to business owners and did not maintain complete records verifying business participation in systems development processes. The Coverage Data Repository was deployed before responsible officials completely assessed security risks and authorized the system to operate. Further, application-specific plans were not yet in place to fully support the IRS's program and policy to mitigate risks for unauthorized access to taxpayers' records.[20]

ACA Verification Service

The ACA Program Management Office is developing numerous releases of ACA software to implement ACA provisions that take effect over several years. Under ACA Release 5.0, the ACA Program Management Office developed the ACA Verification Service to process new Forms 8962, *Premium Tax Credit (PTC)*, and 8965, *Health Coverage Exemptions*, filed by taxpayers during the 2015 Filing Season. The ACA Verification Service will also identify taxpayers who received an advance payment of the Premium Tax Credit but did not file the required Form 8962 with their tax return.

The System Test Plan is a requirement of the IRS ELC policy. The System Test Plan defines the scope, approach, and required activities that will be used to effectively test and assess the quality of a system, including the criteria that must be met to begin and end a test. The *ACA 5.0 Consolidated Project Level System Test Plan, Version 1.1*, dated April 1, 2014, states that each sprint includes all previously tested code and new code. During each sprint, the ACA Verification Service test team will execute test cases for the current build in parallel with regression test cases identified for the build. Before ending the project-level test, all defects must be resolved or appropriately dispositioned, and all test cases must be dispositioned and documented.

Project-level testing for the ACA Verification Service was originally scheduled to be completed by June 23, 2014. The backlog of test cases and defects and the time needed to complete changes to the program code to correct the critical defects identified during project-level testing prolonged project-level testing and pushed project-level testing into release-level testing.

Delays in code delivery delayed testing. For example, by December 27, 2013, the ACA Implementation and Testing organization reallocated 76 test cases from Sprint 1, Sprint 2, and Sprint 3 to Sprint 4 for test execution because the design for the Coverage Data Repository to ACA Verification Service interface was not finalized. The Implementation and Testing

[20] See Appendix IV, number 4.

organization expected a Sprint 7 build by midday June 16, 2014, to begin test execution. The development team experienced delays, and the Sprint 7 build was delivered that night. By then, an upgrade to an application server had begun and was completed on June 17, 2014. As a result, the Sprint 7 build delivered on the night of June 16, 2014, was incompatible with the application server upgrade, and the Implementation and Testing organization could not use it for its tests. These vulnerabilities could allow unauthorized connections, untrusted applications to gain privileges, and remote attackers to bypass intended access restrictions. Failure to correct such flaws increases the risk of successful data compromise, execution of arbitrary code, and attacks to disrupt computer operations.[21]

Interagency testing

The *CMS-IRS Interagency Test Plan* dated January 23, 2014, required the CMS and the IRS to complete independent testing of their respective systems prior to the start of CMS-IRS interagency testing. The IRS executed its internal ACA 4.0 release-level testing, which included Coverage Data Repository 2.0, and interagency testing with the Health and Human Services Data Services Hub at nearly the same time. Specifically, the IRS executed ACA 4.0 release-level testing from April 7, 2014, through September 24, 2014, while CMS-IRS interagency testing was executed from March 31, 2014, through September 30, 2014. However, this approach did not fully test and verify the IRS's internal ACA 4.0 release-level functionality prior to starting ACA 4.0 interagency testing with the Health and Human Services Data Services Hub. During our meetings with the ACA IT Implementation and Testing organization, the IRS agreed that ACA 4.0 release-level tests should have been completed before the start of ACA 4.0 interagency testing with the Health and Human Services Data Services Hub.

Because the IRS did not fully complete its internal ACA 4.0 release-level tests before the start of interagency testing as required by the *CMS-IRS Interagency Test Plan*, the IRS could not ensure that its internal ACA 4.0 systems were fully functioning as intended prior to starting CMS-IRS interagency testing. For example, the IRS did not know whether its Coverage Data Repository and Information Sharing and Reporting systems, which make up ACA 4.0, could successfully and properly work together as a complete ACA 4.0 release. This increases the risk that interagency testing between the IRS and the CMS may not have effectively determined whether planned functionality works as intended between the two agencies.

Final Integration Test

The Final Integration Test (FIT) is a critical part of the IRS's preparation for each filing season. Each year, the IRS incorporates system improvements and changes to the tax law into the tax processing system. The FIT is the final step of the application software testing effort designed to ensure that revisions to IRS computer applications interoperate correctly prior to the tax return filing season. While the overall responsibility for the FIT program lies with the IT

[21] See Appendix IV, number 11.

organization's Enterprise Systems Testing Division, the FIT program requires the participation and support of several other organizations including Applications Development, Enterprise Operations, the business units, and contractors. If tax processing systems are not properly integrated to deliver filing season functionality, taxpayers may be unable to timely file returns, receive refunds, or obtain timely, accurate customer service. The IRS is in the process of making significant changes to its tax processing system to implement legislative changes such as the ACA previously described. These changes will result in increased workload and challenges for the FIT program.

Each FIT performed consists of a series of tests designed to ensure that essential IRS applications will perform correctly when deployed. The FIT is performed from the perspective that all IRS applications are subsystems of the overall tax processing system. We found that the FIT program team effectively planned and prepared for the Processing Year 2015 FIT.[22] The team conducted and completed all required planning and preparation activities as well as took corrective actions on several of the previous TIGTA audit report recommendations. However, key systems and programs were not sufficiently developed and tested before delivery to the FIT environment. The FIT program received eight builds of the ACA 5.0 systems between November 3, 2014, and January 15, 2015. The final build was received by the FIT program less than one week before the start of the 2015 Filing Season. The Modernized e-File system was delivered to the FIT environment with programming errors. Some of these delivery events caused FIT program analysts to open several priority one helpdesk tickets.

[22] See Appendix IV, number 3.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the progress of the IRS's Information Technology Program including security, modernization, and operations for FY 2015. This review was required by the IRS Restructuring and Reform Act of 1998.[1] 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 Systems Security Directorate audit reports issued during FY 2015. During the review, we analyzed and prepared an overall assessment of the systems security and privacy issues.

   B. Identified and summarized relevant non–Systems Security Directorate and/or external oversight assessments dealing with security and privacy, *e.g.*, assessments performed by the GAO.

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

   A. Obtained and reviewed TIGTA Systems Development Directorate audit reports issued during FY 2015. During the review, we analyzed and prepared an overall assessment of the systems development issues.

   B. Identified and summarized relevant non–Systems Development Directorate and/or external oversight assessments dealing with modernization and systems development.

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

   A. Obtained and reviewed TIGTA Systems Operations Directorate audit reports issued during FY 2015. During the review, we analyzed and prepared an overall assessment of systems operations issues.

   B. Identified and summarized relevant non–Systems Operations Directorate and/or external oversight assessments dealing with systems operations.

[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.).

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

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Gwen McGowan, Director
Kent Sagara, Director
John Ledford, Acting Director
Joseph F. Cooney, Audit Manager
Jena Whitley, Lead Auditor
George Franklin, Senior Auditor
Bret Hunter, Senior Auditor
Ashley Weaver, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Chief, Agency-Wide Shared Services OS:A
Commissioner, Wage and Investment Division SE:W
Deputy Chief Information Officer for Operations OS:CTO
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, Enterprise – Program Management Office OS:CTO:EPMO
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 Program Evaluation and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

List of Treasury Inspector General for Tax Administration Reports Reviewed

Number	Report Reference Number	Audit Report Title	Report Issuance Date
1	2015-20-031	*Planning Decisions for Customer Account Data Engine 2 Transition State 2 Should Be Effectively Linked to Actions Needed to Address the Internal Revenue Service's Financial Material Weakness*	May 1, 2015
2	2015-20-033	*The Integrated Enterprise Portal Is Operating As Designed; However, Increased Contract Oversight Is Necessary*	May 5, 2015
3	2015-20-034	*Final Integration Test Planning and Preparation*	May 8, 2015
4	2015-23-041	*Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment*	June 2, 2015
5	2015-20-060	*The Return Review Program Enhances the Identification of Fraud; However, System Security Needs Improvement*	July 2, 2015
6	2015-20-079	*Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program*	Sept. 1, 2015
7	2015-20-087	*Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured*	Sept. 14, 2015

Number	Report Reference Number	Audit Report Title	Report Issuance Date
8	2015-20-088	*Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected*	Sept. 17, 2015
9	2015-20-092	*Treasury Inspector General for Tax Administration - Federal Information Security Modernization Act Report for Fiscal Year 2015*	Sept. 25, 2015
10	2015-20-073	*Inadequate Oversight and Bypassing Established Policy Contributed to Windows Upgrade Project Delays*	Sept. 28, 2015
11	2015-20-081	*Affordable Care Act Verification Service: Security and Testing Risks*	Sept. 28, 2015
12	2015-20-093	*Review of the Electronic Fraud Detection System*	Sept. 29, 2015

Appendix V

Outcome Measures Reported in Fiscal Year 2015

Audit Report Title	Type of Measure	Amount
The Integrated Enterprise Portal Is Operating As Designed; However, Increased Contract Oversight Is Necessary (Ref. No. 2015-20-033)	Cost Savings	$405,679
Review of the Electronic Fraud Detection System (Ref. No. 2015-20-093)	Funds Put to Better Use	$18.2 million

Appendix VI

Glossary of Terms

Term	Definition
Accountability	Ensuring that officials in an organization are answerable for their actions and that there is redress when duties and commitments are not met.
Affordable Care Act	The comprehensive health care reform law enacted in March 2010 and subsequently amended. The law was enacted in two parts. The Patient Protection and Affordable Care Act was signed into law on March 23, 2010, and was amended by the Health Care and Education Reconciliation Act on March 30, 2010.[1] The ACA refers to the final amended version of the law.
Affordable Care Act Verification Service	This system integrates with the current processing environment to perform compliance checks and validate information on tax forms related to health insurance. The system identifies exceptions associated with the ACA when the returns are filed. Catching exceptions such as math errors and returns that do not match corresponding third-party data will reduce the number of returns that are flagged for downstream checks, routed to the Error Resolution System, or rejected altogether.
Applications Development Organization	A part of the IRS IT organization responsible for building, testing, delivering, and maintaining integrated information technology applications to support modernized systems and the filing season environment.
Build	A version of a software program.
Centers for Medicare and Medicaid Services	A division of the U.S. Department of Health and Human Services, the CMS provides health coverage for 100 million people through Medicare, Medicaid, and the Children's Health Insurance Program.
Chief Technology Officer	Leads the IRS IT organization and advises the IRS Commissioner about information technology matters, manages all IRS information system resources, and is responsible for delivering and maintaining modernized information systems throughout the IRS.

[1] The Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections 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.

Term	Definition
Contractor	An organization external to the IRS that supplies goods and services according to a formal contract or task order. A contractor is a type of provider.
Coverage Data Repository	This database will support ACA provisions by using data imported from the Integration Production Model, which contains data from the National Account Profiles, the Individual Master File, and the Individual Return Transaction File. The Coverage Data Repository contains information from the following ACA projects: Income and Family Size Verification, Premium Tax Credit, ACA Information Returns, and the Infrastructure Security Review. It also contains information received through the Health and Human Services' Data Hub that is retrievable for at-filing and post-filing usage.
Customer Account Data Engine 2	An IRS application that will replace the existing Individual Master File and CADE applications. The CADE 2 strategy, as designed, will allow the IRS to modernize the processes it uses to account for the records of individual taxpayers and create a single overall system of records. In addition, the time to process and update individual taxpayer account data would be shortened from a weekly to a daily basis, which will improve the timeliness and accuracy of this information.
Data Services Hub	A tool that allows the CMS to interface and share ACA-related information with other agencies.
Enterprise Life Cycle	A structured business systems development methodology that requires the preparation of specific work products during different phases of the development process.
Enterprise Operations	A part of the IRS IT organization that provides server and mainframe computing services for all IRS business entities and taxpayers.
Exchange	A new transparent and competitive insurance exchange in which individuals and small businesses can buy affordable and qualified health benefit plans. Exchanges offer a choice of health plans that meet certain benefits and cost standards.
Exchange Periodic Data	The data the IRS receives each month from the Exchanges. The Exchange Periodic Data flows are cumulative, meaning each submission will contain data for each month from January up to and including the current month being submitted.
Federal Exchange	An Exchange developed by the Federal Government (the CMS) to assist States that have chosen not to build their own individual State marketplace.

Term	Definition
Federal Information Security Modernization Act	Amendment to The Federal Information Security Management Act of 2002 which allows for further reform to Federal information security, signed in 2014, 12 years after the passing of the original law. This bill amends chapter 35 of title 44 of the United States Code (P.L. 113-283). The original statute requires agencies to assess risks to information systems and provide information security protections commensurate with the risks, 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 Office of Management and Budget (Title III, P.L. 107-347).
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Final Integration Test	A system test consisting of integrated end-to-end testing of mainline tax processing systems to verify that new releases of interrelated systems and hardware platforms can collectively support the IRS business functions allocated to them.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
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.
Hardware	The physical parts of a computer and related devices; it includes motherboards, hard drives, monitors, keyboards, mice, printers, and scanners.
Health and Human Services Data Services Hub	Provides a single point in which the Exchanges may access data from different sources, primarily Federal agencies. The Health and Human Services Data Services Hub does not store data; rather, it acts as a conduit for the Exchanges to access the data from where they are originally stored.
Information Sharing and Reporting	The Information Sharing and Reporting Project is responsible for facilitating the exchange of ACA data between IRS systems and the Exchanges. The Information Sharing and Reporting system performs consistency checks on the Exchange Periodic Data before transmitting it to the Coverage Data Repository.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.

Term	Definition
Managed Service	The practice of outsourcing day-to-day management responsibilities and functions as a strategic method for improving operations and cutting expenses.
Modernized e-File	The IRS's electronic filing system that enables real-time processing of tax returns while improving error detection, standardizing business rules, and expediting acknowledgements to taxpayers. The system serves to streamline filing processes and reduce the costs associated with a paper-based process.
National Institute of Standards and Technology	The Information Technology Laboratory at the National Institute of Standards and Technology develops management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of "other than national security"–related information in Federal information systems. The Institute is part of the U.S. Department of Commerce.
Operating System	The software that communicates with computer hardware to allocate memory, process tasks, access disks and peripherals, and serves as the user interface.
Oversight	IRS management of project work conducted by outside contractors to assure that IRS needs and contractual terms are met. Also, monitoring or governance of IRS projects by organizations outside the IRS.
Personally Identifiable Information	Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, and mother's maiden name.
Portal	A web-based infrastructure (hardware and software) that serves as the entry point for web access to applications and data.
Premium Tax Credit	A refundable tax credit to help taxpayers and families afford health insurance coverage purchased through an Exchange.
Processing Year	The calendar year in which the tax return or document is processed by the IRS.
Regression Test	A regression test ensures that a change did not cause system degradation or introduce new defects.
Release	A specific edition of software.
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.
Software	A general term that describes computer programs and consists of lines of code written by computer programmers that have been compiled into a computer program.

Term	Definition
Sprint	A process that develops a piece of functionality of the system with repeated cycles of requirements discovery, planning, design, development, and testing. ACA projects conduct a series of "sprints," either sequentially or even in parallel, with each release. The goal of each sprint is to get a subset of the project's functionality.
State Exchange	An Exchange fully operated by the individual State.
System Test Plan	The plan is an Enterprise Life Cycle requirement. The purpose of the plan is to provide a standard artifact to summarize the complete test effort for the release. The plan gives the project an opportunity to mitigate risks that may cause delays to project implementation.
Test Case	The foundation of a test. A test case references specific test data and the expected results associated with specific program criteria. It is used to verify a specific process in the application software and to test system requirements
Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
Windows 7	The seventh version of the Microsoft Windows Operating System, introduced in October 2009.
Windows XP	Introduced in October 2001, it was one of Microsoft's most popular operating systems, and in April 2013, Microsoft ended its extended support, which is also known as "end of life."