TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the Internal Revenue Service Information Technology Program

September 30, 2014

Reference Number: 2014-20-095

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

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

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

ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE INFORMATION TECHNOLOGY PROGRAM

Highlights

Final Report issued on September 30, 2014

Highlights of Reference Number: 2014-20-095 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

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. 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

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 2014.

WHAT TIGTA FOUND

In 2014, the Government Accountability Office stated that shortcomings in the IRS's information security were the basis for its determination that the IRS had a significant deficiency in its internal control over its financial reporting systems for Fiscal Years 2012 and 2013. TIGTA's reviews in the information security area identified weaknesses in the enterprise information technology security program, the protection of Federal tax information, implementation of enterprise risk management, security issues with systems development activities, implementation of security solutions, and security of employees.

In the Modernization Program, the Customer Account Data Engine 2 database validation efforts were efficiently performed due to adequate planning and resource coordination, and a large percentage of the data fields were validated with automated data compare tools. However, TIGTA's reviews identified several issues that should be addressed to further strengthen the program including systems testing issues and requirements management process issues.

While several projects are currently on target regarding cost and schedule, other critical systems may be impacted by budget limitations. TIGTA is also concerned that the IRS's existing fraud detection system may not be capable of identifying Affordable Care Act refund fraud or schemes prior to the issuance of tax refunds. As a result, TIGTA plans to continue oversight of this area.

Efficient and cost-effective management of information technology assets is crucial to ensuring that information technology services continue to support IRS's business operations and help it to provide services to taxpayers efficiently. TIGTA's recent work involving the IRS's inventory management of mainframe and server software licenses and telecommunications equipment as well as the disposal of electronic equipment identified several opportunities for the IRS to achieve cost savings.

WHAT TIGTA RECOMMENDED

Because this was an assessment report of the IRS's Information Technology Program through Fiscal Year 2014, 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, 2014

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Annual Assessment of the Internal Revenue Service Information Technology Program (Audit # 201420009)

The overall objective of this review was to assess the progress 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 was included in our Fiscal Year 2014 Annual Audit Plan under the major management challenge of Modernization; however, it also addresses other challenge areas (*e.g.,* Security for Taxpayer Data and IRS Employees, Implementing the Affordable Care Act and Other Tax Law Changes).

Copies of this report are also being sent to the IRS managers affected by the reports contents. 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

Abbreviations

ACA	Affordable Care Act
ACIO	Associate Chief Information Officer
AIR	Affordable Care Act Information Returns
CTO	Chief Technology Officer
DLP	Data Loss Prevention
FATCA	Foreign Account Tax Compliance Act
FIT	Final Integration Test
FRS	Financial Institution Registration System
FTI	Federal Tax Information
FY	Fiscal Year
HSPD-12	Homeland Security Presidential Directive 12
IPv6	Internet Protocol version 6
IRDM	Information Reporting and Document Matching
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PMO	Program Management Office
POA&M	Plan of Action and Milestone
RQM	Rational Quality Manager
SPIIDE	Safeguarding Personally Identifiable Information Data Extracts

TASIS	Taxpayer Advocate Service Information System
TIGTA	Treasury Inspector General for Tax Administration

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 of the IRS's Information Technology Program for Fiscal Year[2] (FY) 2014.

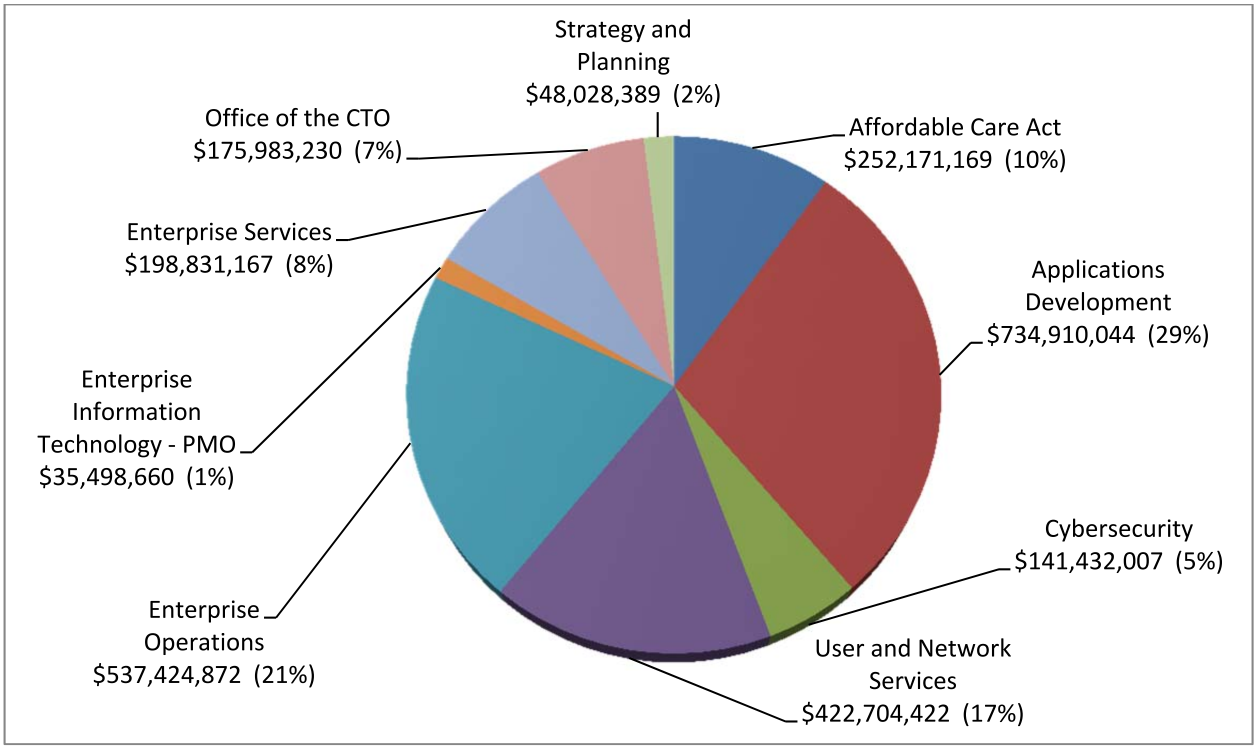
The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In FYs 2012 and 2013, the IRS collected about $2.5 trillion and $2.9 trillion, respectively, in Federal tax payments, processed hundreds of millions of tax and information returns, and paid about $373 billion and about $364 billion, respectively, in refunds to taxpayers. Further, the size and complexity of the IRS add unique operational challenges. The IRS employs more than 92,000 people in its Washington, D.C., Headquarters and more than 650 offices in all 50 States, U.S. territories, and some U.S. embassies and consulates. 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. 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.

According to March 2014 budget information provided by the Associate Chief Information Officer (ACIO), Strategy and Planning, the IRS Information Technology (IT) organization's FY 2014 budget was approximately $2.5 billion, which is up slightly from last year's budget of about $2.3 billion. Figure 1 provides a breakdown of the FY 2014 budget by ACIO organization. Figure 2 provides a breakdown of the FY 2014 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.).

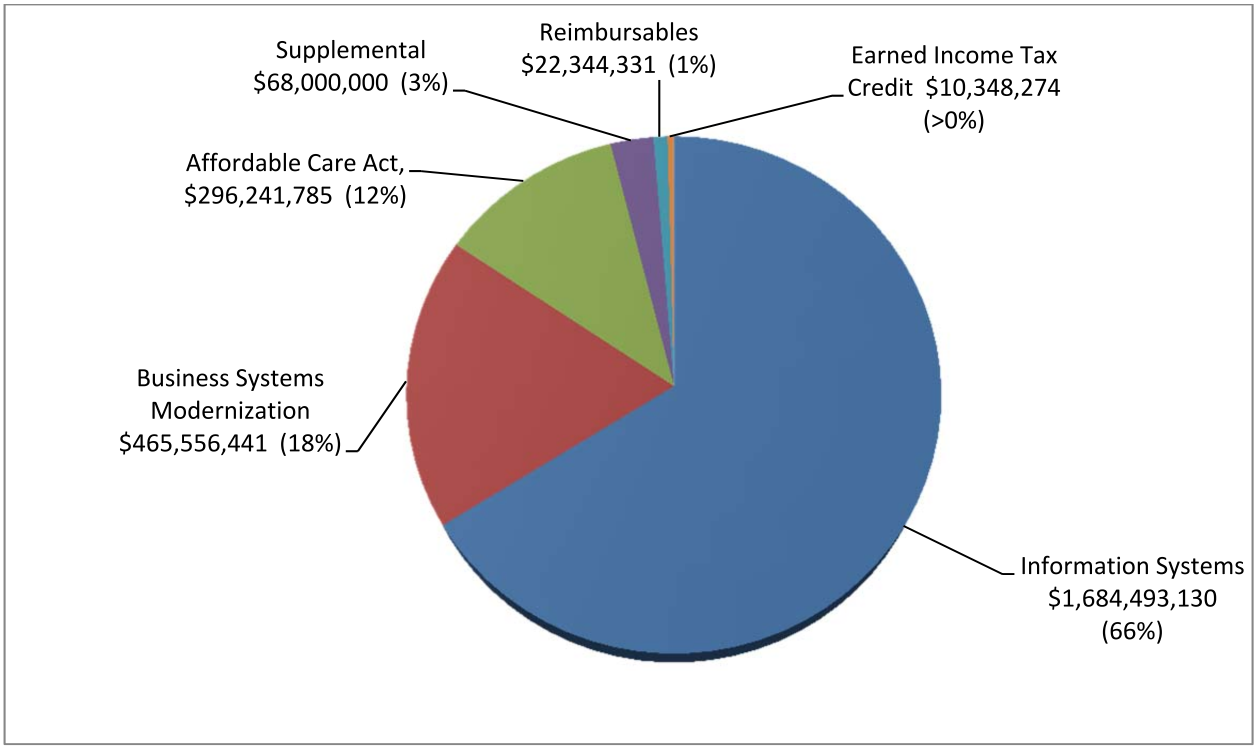
[2] See Appendix VI for a glossary of terms.

Figure 1: IRS IT Organization
FY 2014 Budget (by ACIO organization)



Source: Our analysis of the IRS IT organization budget data as of June 30, 2014, based on information provided by the ACIO, Strategy and Planning, Financial Management Services.
CTO = Chief Technology Officer. PMO = Program Management Office.

Figure 2: IRS IT Organization FY 2014 Budget (by Funding Source)



Source: Our analysis of the IRS IT organization budget data as of June 30, 2014, based on information provided by the ACIO, Strategy and Planning, Financial Management Services.

Similar to FY 2013, the IRS IT organization experienced turnover in FY 2014 in some of its executive positions. For example, the Enterprise Operations, Enterprise Information Technology – Program Management Office (PMO), and Cybersecurity organizations have new executive leadership. As of July 2014, the IRS IT organization employed 7,339 individuals, of which 7,203 work in the following eight different 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 Information Technology - PMO 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.
- Enterprise Services is responsible for strengthening technology infrastructure across the enterprise.
- Strategy and Planning collaborates with IT 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.
- Affordable Care Act (ACA)[3] - PMO 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 136 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. 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 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 IT organization employees in each business unit.

[3] 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.

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

Information Technology Business Unit	Number of Employees
Enterprise Operations	1,917
Applications Development	1,898
User and Network Services	1,572
Enterprise Services	682
Cybersecurity	363
Affordable Care Act – PMO	332
Strategy and Planning	279
Enterprise Information Technology - PMO	160
Management Services	126
Office of the CTO	10
Total	7,339

Source: Treasury Integrated Management Information System as of July 2014.

The compilation of information for this report was conducted at TIGTA offices in Atlanta, Georgia; and Memphis, Tennessee, during the period May through September 2014. The information presented is derived from TIGTA audit reports issued between October 1, 2013, and September 30, 2014. We also reviewed relevant Government Accountability Office 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 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 list of TIGTA audit reports used in this assessment is presented in Appendix IV.

Results of Review

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

For FY 2014, TIGTA designated Security for Taxpayer Data and IRS 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 cyber-attacks. 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 an 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 24.4 percent in FY 2013, when agencies reported 60,753 cyber incidents to the U.S. Computer Emergency Readiness Team as presented in Figure 4. The Department of the Treasury reported 2,962 cyber incidents to the U.S. Computer Emergency Readiness Team in FY 2013, as shown in Figure 5.

[4] OMB, *FY 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).

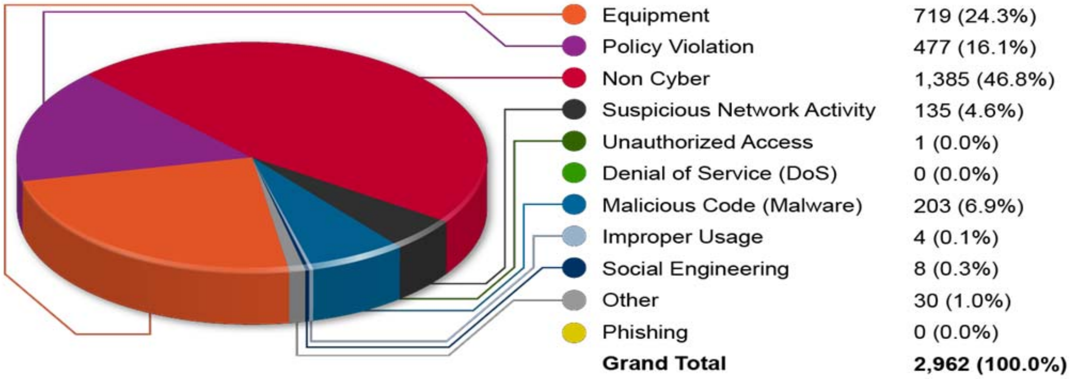
Figure 4: Cyber Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies in FY 2013

Incident Category	Number of Incidents	Percentage of Total Incidents
Non-Cyber (Personally Identifiable Information spillage or mishandling for hardcopy or printed material)	15,057	24.8%
Policy Violations (mishandling of data in storage or transit)	11,847	19.5%
Malicious Code (malware)	9,883	16.3%
Equipment (lost or stolen equipment)	9,587	15.8%
Other (low frequency incidents, such as unconfirmed third-party notifications, failed attacks, or incident with unknown causes)	5,885	9.7%
Social Engineering (fraudulent websites or attempts to entice users to provide sensitive information)	3,580	5.9%
Suspicious Network Activity	3,167	5.2%
Improper Usage (rule of behavior violations)	969	1.6%
Unauthorized Access (unprivileged users gain control of system or resource)	653	1.1%
Phishing (subset of Social Engineering, attempt to entice users to provide sensitive information)	71	0.1%
Denial of Service (successful Denial of Service attacks)	54	0.1%
Total	60,753	100.0%

Source: The OMB's FY 2013 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002[5] *dated May 2014. Percentages do not total 100 percent due to rounding.*

[5] Title III of the E-Government Act of 2002, Pub. L. No 107-374,116 Stat. 2899.

Figure 5: Cyber Incidents Reported to the U.S. Computer Emergency Readiness Team by the Department of the Treasury in FY 2013



Source: The OMB's FY 2013 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002 dated May 2014. Percentages do not total 100 percent due to rounding.

The Office of Cybersecurity provides management and oversight for the IRS IT Security Program and its mission is to ensure the security and resilience of information technology systems and data by providing solutions to the security risks encountered by IRS employees. To inform managers and employees of planned, security-related activities and how those activities inter-relate and support the overall security and business goals of the IRS, the IRS issued version 3.0 of its IT Security Program Plan in October 2013.

The plan describes the IRS's continuous efforts to mitigate security weaknesses, to improve its security posture, and to synchronize the many security activities occurring throughout the agency. This plan also continues to address current information technology security gaps and communicates to the IRS community the security initiatives that are being undertaken to resolve computer security weaknesses, comply with Federal security guidelines, and reduce security risk. Further, through continued review and collaboration with all IRS stakeholders, the plan documents efforts to ensure that the IRS is not developing duplicative processes or products.

The IRS developed its current plan under the same premise as its predecessor, using the 13 information security program elements contained in National Institute of Standards and Technology (NIST) Special Publication 800-100[6] as the framework for its Information Security Program. Under each program element, the plan presents a brief description of its scope, the current environment, and an encapsulation of near-term, mid-term, and long-term security initiatives. The plan serves as a roadmap and a basis for benchmarking security performance towards attaining security objectives, communicating initiatives either in process or planned, and

[6] NIST, Special Publication 800-100, *Information Security Handbook: A Guide for Managers* (Oct. 2006).

serving as an indicator of its commitment to meet or exceed Federal Government security requirements.

Because *Security for Taxpayer Data and IRS 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 subsequently discussed appear in multiple sections of this report.

Enterprise information technology security program

The following two audit reports provided enterprise-wide information technology security perspectives on the IRS environment.

The Government Accountability Office's 2012-2013 Financial Statement Reviews: In April 2014, the Government Accountability Office reported that the shortcomings in the IRS's information security were the basis for its determination that the IRS had a significant deficiency in its internal control over its financial reporting systems for Fiscal Years 2012 and 2013. They found that the IRS had not always (1) installed appropriate patches on all databases and servers to protect against known vulnerabilities, (2) sufficiently monitored database and mainframe controls, or (3) appropriately restricted access to its mainframe environment. In addition, the IRS allowed individuals to make changes to mainframe data processing without requiring them to follow established change control procedures to ensure that changes were authorized and did not configure all applications to use strong encryption for authentication, increasing the potential for unauthorized access.

The Federal Information Security Management Act: This Act requires Federal agencies to provide information security protections commensurate with risks and their potential harm to Federal information. Based on our FY 2014 Federal Information Security Management Act evaluation,[7] we found five of the 11 security program areas met the performance metrics specified by the Department of Homeland Security's FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics.[8]

- Risk Management.
- Plan of Action and Milestones.
- Contingency Planning.

[7] See Appendix IV, number 15.

[8] U.S. Department of Homeland Security, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics* (Dec. 2, 2013).

- Contractor Systems.
- Security Capital Planning.

Four security program areas were not fully effective due to one or more program attributes that were not met.

- Continuous Monitoring Management.
- Incident Response and Reporting.
- Security Training.
- Remote Access Management.

Two security program areas did not meet the level of performance specified by the Department of Homeland Security's FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics due to the majority of the Department of Homeland Security specified attributes not being met.

- Configuration Management.
- Identity and Access Management.

Protection of Federal tax information

Internal Revenue Code Section (§) 6103 authorizes the IRS to disclose Federal Tax Information (FTI) to other Federal, State, or local government entities for official purposes. Agencies might use FTI for various reasons such as locating delinquent taxpayers, assisting in determining a person's ability to pay on a defaulted debt, or identifying whether discrepancies exist in reporting of income. We identified weaknesses in the following audits that pertain to the protection of FTI.

Office of Safeguards Program: The IRS provides FTI to approximately 280 Federal agencies, State and local entities, and U.S. territories. Internal Revenue Code § 6103(p)(4), Internal Revenue Manual Section 11.3.36,[9] and IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies,*[10] require recipients of FTI to establish procedures to ensure the adequate protection of FTI received. The IRS Office of Safeguards is in the Governmental Liaison, Disclosure and Safeguards business unit within the Operations Support organization and has oversight responsibility of agencies that receive FTI subject to Internal Revenue Code § 6103(p)(4) to ensure that adequate safeguards are maintained.

[9] Dated August 2008.
[10] Dated August 2010.

During our review of the Office of Safeguards program,[11] we found that the Office of Safeguards did not have effective controls established to ensure that the annual report on the procedures and safeguards of agencies that receive FTI was timely submitted to the required U.S. congressional committees. As a result, the Office of Safeguards annual report to Congress for Calendar Years 2010, 2011, and 2012 was not submitted to the director of the office timely and the Calendar Years 2010 and 2011 reports were not issued to the required U.S. congressional committees timely.

Also, during our review of the Office of Safeguards program, we provided recommendations to improve internal controls over the master list of agencies receiving FTI, the review schedule of agencies receiving FTI, and the database that holds agency documents.

Further, while the Internal Revenue Manual requires the Office of Safeguards to conduct on-site agency reviews once every three years, it does not require it to perform on-site validation of an agency's ability to protect FTI prior to the release of FTI to the agency. When the primary assessment of an agency's safeguarding processes (*i.e.*, on-site reviews) is performed one to three years after receipt of FTI, there is a significant risk that the FTI provided may be subjected to unauthorized disclosure and use.

During our review of FTI provided to State agencies in support of the Affordable Care Act,[12] we found additional procedures are needed to provide greater assurance that FTI will be protected prior to approving its release. Specifically, IRS procedures did not require the Exchanges or other agencies to submit an initial independent security assessment report that could help to evaluate risk levels and the status of required security controls. The current documentation on which the Office of Safeguards bases its approval decision for release of FTI does not provide sufficient evidence that required controls have been implemented. We also found deficiencies in procedures related to obtaining signed system security authorizations and ensuring that on-site reviews of agencies that have deployed new systems occur in a timely manner.

Background Checks: Federal agencies are required to conduct a Minimal Background Investigation on all potential employees designated as moderate risk, including individuals hired to access or use FTI. The background investigation required for Federal employees with access to FTI includes 1) fingerprints, 2) a National Agency Check plus credit search; checks at local law enforcement agencies where the subject has lived, worked, and/or attended school; and, if applicable, check the appropriate agency for any identified arrests, 3) a personal subject interview, 4) written inquiries to employers, schools, and references for the past five years, and 5) a periodic reinvestigation once every 10 years. The IRS's Human Resource Division requires the Federal Minimal Background Investigation for all positions within the IRS designated as moderate risk, including positions with access to FTI. Once completed and approved, the Minimal Background Investigation would provide an IRS employee with a National Security

[11] See Appendix IV, number 9.
[12] See Appendix IV, number 10.

Non-Critical Sensitive clearance and authorization to access FTI, if access is required to perform the employee's official duties.

During our review of the Office of Safeguards program,[13] we also found that the IRS does not require and ensure that agencies conduct proper background investigations. Specifically the IRS does not set specific background investigation requirements for employees and contractors at agencies receiving FTI or are given access to FTI. The IRS allows each agency that receives FTI to set its own background investigation policies and requirements. Additionally, the IRS does not conduct on-site review tests on each agency's background investigation policies and procedures or on agency employees to determine if background investigations have been performed by the agency receiving FTI.

During our review of contractor personnel background investigations,[14] we found that taxpayer information and other Sensitive But Unclassified information may be at risk. Specifically, five contracts lacked background investigation requirements for courier, printing, document recovery, and sign language interpreter services. In 12 contracts, IRS personnel correctly determined that contractors required background investigations because they would have access to Sensitive But Unclassified information; however, some contractor personnel did not have interim access approval or final background investigations before they began working on the contracts. In 20 contracts, either some or all contractor personnel did not sign nondisclosure agreements. In June 2013, after the period covered by our audit, the IRS issued more explicit guidance requiring the execution of nondisclosure agreements.

Implementation of enterprise risk management

IRS policy defines risk management as the process of identifying, monitoring, and mitigating project and program risks. IRS policy goes on to state that organizations should thoroughly document a weakness, the risks arising from the weakness, all mitigations which were considered, the cost of mitigations, and their technical feasibility in order for management to make informed decisions. When implementing enterprise-wide risk management, a key component is oversight for risk management activities to ensure consistent and effective decisions. We identified weaknesses that pertained to risk management in the following audits.

Taxpayer Advocate Service Information System (TASIS): During our review of the TASIS project,[15] we determined that the IRS has not consistently followed the established risk management processes to identify, monitor, and mitigate significant risks during the system's development process. Specifically, risks were not consistently captured and monitored in the approved risk management system and a project-specific risk management plan was not developed.

[13] See Appendix IV, number 9.
[14] See Appendix IV, number 6.
[15] See Appendix IV, number 20.

Risk-Based Decisions: Risk-based decisions are made when the IRS wants to make an exception to its own policies and requirements based on suitable justification and a thorough assessment of evident and potential risks. For decisions related to the security of information systems, exceptions are allowed if meeting the requirement is 1) not technically or operationally possible or 2) not cost effective. IRS policy also requires Risk-Based Decisions to be tracked in a library.

During our review of the IRS risk-based decisions process on security controls,[16] we found that while the IRS tracks basic information, the information being tracked is not sufficient for risk management of information technology systems. The IRS neither supported nor adequately tracked risk-based decisions in a spreadsheet that Cybersecurity officials refer to as their library. Because these decisions are not consistently documented, reviewed, or maintained centrally, IRS management lacks the ability to adequately manage information technology risk-based decisions, which ultimately affects the IRS's ability to manage enterprise risk.

Security issues with systems development activities

The NIST Special Publication 800-37[17] stresses that security requirements are a subset of the overall functional and nonfunctional (*e.g.*, quality assurance) requirements levied on an information system and are incorporated into the system development life cycle simultaneously with the functional and nonfunctional requirements. Without the early integration of security requirements, significant expense may be incurred by the organization later in the life cycle to address security considerations that could have been included in the initial design. When security requirements are considered as an integral subset of other information system requirements, the resulting system has fewer weaknesses and deficiencies, and therefore, fewer vulnerabilities that can be exploited in the future. We found weaknesses pertaining to security issues in the following system or project development audits.

ACA Program: ACA legislation mandates that the IRS collect healthcare information reports from health insurance providers and pharmaceutical manufacturers. The ACA Information Returns (AIR) Release 1 Project will support the electronic processing of Non-Exchange ACA information returns. The AIR system's functionality includes validating, accepting/rejecting, and processing the electronic forms that will be submitted by the health insurance providers and pharmaceutical manufacturers and sending the data to the IRS systems that calculate and collect fees.

The Cybersecurity organization is responsible for conducting security testing activities designed to ensure that systems security safeguards are in place and functioning as intended. According to IRS policy, the IRS is responsible for reviewing and mitigating the vulnerability weaknesses identified in a vulnerability detection scan and creating a Plan of Action and Milestone

[16] See Appendix IV, number 13.

[17] NIST, Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Feb. 2010).

(POA&M).[18] The POA&M process provides a plan of action to correct the vulnerability and to enter the vulnerability weakness into a POA&M or to create a Risk-Based Decision. A POA&M should be initiated within 60 days for moderate systems.

IRS policy allows designated approving authorities to tailor security control baselines for their systems using a cost-effective, risk based approach. This type of risk-based decision making gives designated approving authorities a process by which they can make exceptions or deviations to IRS information technology security policies based on credible justification and a thorough assessment of the risks incurred as a result of the deviation.

As a part of testing, Cybersecurity performed one vulnerability detection scan on an ACA-related system in December 2013. This scan identified a total of 108 issues. Of these 108 issues, 25 were categorized as Critical and Major Failures and Errors. During our review to determine if the IRS is adequately mitigating system development risks under the ACA Program,[19] we informed the IRS of the following concerns:

- The POA&M was developed 56 days after the 60-day requirement for a moderate system.
- The POA&M provided details on how to address only 23 of the 25 critical and major failures and errors identified.
- Although the POA&M provided details on how to address 23 of the 25 vulnerability weaknesses, several of the mitigation target dates are nine to 12 months after the database is scheduled to start processing electronic forms on October 1, 2014.

We also reviewed the 25 critical and major failures and errors identified and concluded that the IRS had not installed two security patches on the system.

Based on the POA&M document provided to TIGTA during our review, *******2********* *********************2****************************. We are concerned that these vulnerability weaknesses may not be resolved before the database starts processing electronic forms through the AIR system, which is currently scheduled for October 1, 2014.

In addition, the Cybersecurity organization requested a source code security scan of a contractor-owned commercial off-the-shelf software application. The scan was executed in a nonproduction testing environment in August 2013. The code review identified 4,497 (87.3 percent) low code weaknesses and 655 (12.7 percent) critical, high, and medium code weaknesses, for a total of 5,152 weaknesses.

[18] Also, according to the *Federal Information System Management Act Plans of Actions and Milestones Standard Operating Procedures* dated April 4, 2014, and the NIST Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb 2004), vulnerabilities are assigned a priority level based on the severity of impact and are to be corrected within a specific time period and added to the POA&M so the vulnerabilities can be managed.

[19] See Appendix IV, number 19.

The IRS explained that the critical, high, and medium weaknesses were mitigated by hardening the AIR application server. However, the IRS could not provide documented support that would verify whether the code weaknesses were mitigated. Further, their process did not directly map the weaknesses to the mitigations that had been taken. This verification is needed to ensure that vulnerability weaknesses are adequately mitigated for the AIR system to protect sensitive ACA data. We are also concerned that these weaknesses may not have been mitigated before the AIR system was placed into production in March 2014.

Foreign Financial Institution Registration System: In 2010, Congress enacted the Foreign Account Tax Compliance Act (FATCA).[20] The FATCA Financial Institution Registration System (FRS) program is an important development in the IRS's efforts to improve U.S. tax compliance involving foreign financial assets and offshore accounts.

As a part of the security assessment and authorization process, the IRS Cybersecurity organization conducted a FATCA FRS event-driven Security Controls Assessment. The purpose of the Security Controls Assessment was to ensure that the FATCA FRS met the established security controls in accordance with NIST Special Publication 800-53, Revisions 3 and 4. During our review of the FATCA FRS,[21] we determined that while the IRS traced NIST security controls to test cases and test results, the IRS did not trace FRS system specific security requirements to test cases and test results prior to deployment.

The IRS also informed us that a risk assessment for using electronic signatures in the FRS had not been completed during the systems development. Without a risk-based approach to developing and implementing electronic signatures for the FRS, the IRS has not yet fully considered and addressed the possibility that FRS users, including Foreign Financial Institutions could:

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

Further, if the IRS cannot enforce electronic signatures implemented with the FRS, the risk of monetary loss or other adverse effects could hinder the accomplishment of international tax administration goals.

Additionally, we found that key security documents do not adequately describe how access controls were designed and implemented for the FRS. *********2***************
********************************2***. More specifically, because FRS security documentation was insufficient and the FRS design

[20] Pub. L. No. 111-147, Subtitle A, 124 Stat 71, *96-116 (2010) (codified in scattered sections of 26 U.S.C.).
[21] See Appendix IV, number 21.

relied on an open source software product with known security vulnerabilities, we could not fully evaluate the adequacy FRS access controls.

Data Loss Prevention: In response to OMB memoranda, the IRS Cybersecurity's Architecture and Implementation Branch is leading the Safeguarding Personally Identifiable Information Data Extracts (SPIIDE) Project to promote secure practices in electronic communications (e-mails and Internet access) on the IRS network to protect Sensitive But Unclassified data. Taking a phased approach, the SPIIDE Project team plans to build a system environment to implement Symantec's Data Loss Prevention (DLP) commercial off-the-shelf software solution that is capable of identifying and tracking a number of the IRS's defined Personally Identifiable Information datasets.

During our review of the SPIIDE Project,[22] we determined that the SPIIDE Project team is progressing in its development and implementation of the DLP solution. The team has completed key required enterprise life cycle deliverables and has been identifying and addressing security weaknesses as they are detected. Notwithstanding these achievements, the SPIIDE Project team continues to face challenges to timely implement the DLP solution to protect Personally Identifiable Information from disclosure and protect data that should not be exiting IRS networks.

Based on its new projected implementation date of December 31, 2014, the IRS will have taken more than four years to build and develop its DLP solution. Because of the length of time taken, we believe that stronger management oversight is needed to ensure that the DLP solution meets its new implementation date within budget. The IRS could not provide support to validate SPIIDE Project spending, which it reports to be more than $9.6 million of the $11.4 million budgeted through FY 2014.

In addition, the DLP processes and procedures can be enhanced while the DLP solution is still being developed. While we determined that the DLP Operations team correctly classified 99 (94 percent) of 105 sampled e-mail events, we also found that 17 (57 percent) of the 30 appropriately classified e-mail events were potential incidents that were not forwarded to all appropriate incident responders. These incidents should have been forwarded to and/or accepted by the Office of Privacy, Governmental Liaison and Disclosure. That office then should have advised the affected parties of the disclosure and offered credit monitoring services in 11 of the 17 potential incidents.

Implementation of security solutions

Enterprise-Wide Transition to Internet Protocol Version 6: In August 2005, the OMB mandated that Federal agencies begin planning for the transition from Internet Protocol version 4

[22] See Appendix IV, number 14.

to Internet Protocol version 6 (IPv6). In addition to extended address space, IPv6 has many new or improved features that make it significantly different from its predecessor.

During our review of the enterprise-wide transition to IPv6,[23] we found that the IRS established an IPv6 project team to manage the network conversion. The project team adequately planned for security risks during the conversion but has not completed some elements of the transition plan. For example, the IRS has not established an IPv6 Advisory Board or prepared a resource plan to ensure proper guidance and coordination of its IPv6 efforts. Lastly, we found that the project team received inadequate oversight from the Infrastructure Executive Steering Committee and did not adhere to the IRS's Enterprise Life Cycle policy.

Like any new technology standard, IPv6 introduces security risks if not implemented and managed properly. When the IRS's data and network are not secured, taxpayer information becomes vulnerable to unauthorized disclosure, which can lead to identity theft. Further, security breaches can cause network disruptions and prevent the IRS from performing vital taxpayer services, such as processing tax returns, issuing refunds, and answering taxpayer inquiries.

We also identified procurement control weaknesses in this review. We determined that if the IRS purchases equipment or software that is not IPv6 capable, the products will no longer work when the enterprise-wide IPv6 network conversion occurs at the end of FY 2014. This would not only be a waste of valuable resources, but could also potentially cause network disruption and additional resource expenditures to either replace or upgrade the equipment or software. To prevent this from happening, the IPv6 project team developed suggested changes to IRS procurement policies, but Office of Procurement officials in the Agency-Wide Shared Services organization did not agree with this request. We also found that the Office of Procurement did not establish controls to ensure that all new information technology purchases were IPv6 capable in accordance with the Federal Acquisition Regulation.

Homeland Security Presidential Directive 12: On August 27, 2004, President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, which requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal identity credentials.

During our review of the IRS's implementation of the HSPD-12 requirements,[24] we determined that as of February 27, 2014, the IRS's Personal Identity Verification (PIV) card database supported that 80,119 PIV cards had been issued to IRS network users, achieving an 85 percent issuance rate. However, the IRS has remained at the 85 percent card issuance rate since FY 2013. To resolve the issues related to data consistency and manual processes that have delayed PIV card issuance, the Department of the Treasury is implementing an enterprise solution,

[23] See Appendix IV, number 3.
[24] See Appendix IV, number 7.

known as PIV Data Synchronization, which will synchronize PIV data across the Treasury enterprise, bureaus, and external Federal systems.

We also found that while the IRS has identified 625 locations within the United States and Puerto Rico that require HSPD-12 physical access controls,[25] the IRS has implemented PIV card electronic authentication at only 130 (21 percent) of these locations. Also, the IRS determined that it will not upgrade 134 locations for HSPD-12 compliance because it believes the costs of upgrading these locations are not justified as these offices either have a lower security level, or may be consolidated or closed at some future date. Of the remaining 361 facilities, the IRS estimates that it will not complete PIV-based electronic authentication until at least FY 2018 and only if funding is available.

HSPD-12 requires agencies to use PIV cards to access Federal networks and information systems. As of May 30, 2014, only 5 percent of employees were required to use PIV cards to access the IRS network. Beginning in April 2014, the HSPD-12 project team embarked on an ambitious implementation schedule where they hope to implement mandatory use of PIV card for access to the IRS network for more than 30,000 additional IRS network users. This effort will bring the total number of network users required to log on with their PIV cards to approximately 35,700 (or 38 percent of network users) by the end of FY 2014.

The IRS also has not implemented PIV card access to most of its existing information systems and applications as required and has conducted limited work in this area. Due to limited staffing and funding, implementing mandatory logon to the IRS network using PIV cards has been a higher priority than implementing PIV card access to all IRS information systems.

Continuous Monitoring: To strengthen the Nation's cybersecurity posture, the OMB identified cybersecurity as one of 14 cross agency priority goals which included continuous monitoring of all Federal information systems. Information Security Continuous Monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. In addition to the mandatory guidelines imposed by the OMB, Department of the Treasury officials have also mandated that their bureaus use only the Treasury dashboard that will serve as the official reporting for the Information Security Continuous Monitoring program and use those security tools selected by Department of the Treasury officials for consistency.

The Department of the Treasury has issued guidance stating that there will be one dashboard to report Information Security Continuous Monitoring metrics for the Department. However, Department of the Treasury officials agreed that given the size and complexity of IRS systems, an IRS internal dashboard would give the IRS's stakeholders a comprehensive view of the status of IRS systems, allowing for a more secure environment.

[25] The IRS has employees located at more than 100 additional international offices; however, the State Department is responsible for implementing HSPD-12 physical access controls at these locations.

During our review of the Continuous Monitoring solution,[26] we raised concerns about potential drawbacks if the IRS selects the recommended Department of the Treasury tool. In the fall of 2013, the Department of the Treasury selected DbProtect as the official tool for database scanning for the bureaus.

Through discussions with IRS officials, we were informed that the IRS has moved away from DbProtect and is now using Guardium for its database scanning. Although neither product was an "out-of-the-box" solution, according to the IRS, Guardium appeared to be the more practical and cost effective choice for IRS mainframe database scanning. The IRS has invested significant resources in Guardium over the last three years to make it suitable to the IRS scanning environment.

If the IRS were to stop using Guardium and renew a contract with DbProtect, it would have wasted considerable time and resources to adapt Guardium as a database scanning tool. Further, additional time and resources would be required to make DbProtect a capable solution, with no assurance that it will be comparable to that of Guardium.

Security of employees

Mailroom Screening Procedures for Hazardous Material: In our inspection of IRS Submission Processing Centers' Mailroom Screening Procedures for Hazardous Material,[27] we determined the two IRS centers inspected had controls in place to detect and minimize the effects of explosive and hazardous material submitted via mailrooms. However, additional controls should be considered to improve procedures and ensure that effective screening measures are available throughout the year. We found that procedures were generally consistent and effective in identifying, reporting, and responding to suspicious packages and unknown substances.

***The Identification of Potentially Dangerous Taxpayer and Caution Upon Contact Designations by Frontline Employees*:** The IRS has approximately 25,000 frontline employees who have direct contact with taxpayers and their representatives. While the IRS has programs that focus on employee protection including the Potentially Dangerous Taxpayer and Caution Upon Contact programs, the IRS has not developed sufficient procedures to enable frontline employees to readily identify whether a taxpayer representative has been designated as a Potentially Dangerous Taxpayer or Caution Upon Contact. The safety of frontline employees, others working in the same facilities, and taxpayers is at risk when these employees unknowingly meet with potentially dangerous taxpayer representatives.

[26] See Appendix IV, number 11.
[27] See Appendix IV, number 1.

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

The IRS's modernization efforts include 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. While several projects are currently on target regarding cost and schedule, other critical systems may be negatively impacted by Federal budgetary limitations. For example, TASIS was put on a "strategic pause" due to a lack of funding. Also, the Information Reporting and Document Matching (IRDM) Case Management system was placed on a "strategic pause" due to budget constraints and difficulties users encountered during user acceptability testing. Finally, the Return Review Program system development was placed on "strategic pause" to allow time to evaluate the performance and design of new system functionalities.

In addition, systems development activities to implement ACA provisions will require extensive IRS resources. 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. 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.

TIGTA is also concerned that the IRS's existing fraud detection system may not be capable of identifying ACA refund fraud or schemes prior to the issuance of tax refunds. To address these concerns, TIGTA is planning to conduct reviews of the Electronic Fraud Detection System and the Return Review Program system in FY 2015.

TIGTA's audits of IRS's modernization and major projects highlighted the risks present during systems development. The risks identified in these key systems include weaknesses in systems testing and management of systems requirements.

Customer Account Data Engine 2 database validation

During our review of the Customer Account Data Engine 2 database validation,[28] we found that data validation efforts were efficiently performed due to adequate planning and resource coordination. For example, detailed data validation plans ensured that test activities were on track and a new process ensured that data defects were effectively managed.

The IRS identified the data fields to be verified and how each would be validated. While a large percentage of the data fields are validated with automated data compare tools, there is no documented plan to ensure that data fields validated using other means are validated periodically. While we determined the data sampling methodology for validating Customer Account Data

[28] See Appendix IV, number 17.

Engine 2 data is sound, key activities were not documented. After discussing the need to document the data sampling methodology, the IRS began development of the documentation.

The IRS developed a Data Quality Scorecard to track progress in meeting data quality success criteria. However, the processes needed to effectively perform these activities were not sufficiently documented. As a result, some of the metrics were initially incorrectly reported.

We also found that data discrepancy reports needed improvement. Our analysis found that 10 data field identifiers were missing from a discrepancy report. As a result, the IRS is using another automated tool to validate the 10 data field identifiers until the main tool is corrected.

AIR Release 1 Project

As mentioned in the previous section, ACA legislation mandates that the IRS collect healthcare information reports from health insurance providers and pharmaceutical manufacturers. The AIR Release 1 Project will support the processing of Non-Exchange ACA information returns electronically.

The AIR Release 1 Project personnel and the IT Implementation and Testing organization performed several types of testing to validate whether the AIR system would function as designed and meet the IRS's assigned objectives of ACA 4.1 before it was placed into production.

During our review of the AIR Release 1 Project,[29] we identified test management concerns that could affect the long-term success of the AIR system. Specifically, out of six test cases, we observed four instances where the test cases did not adequately describe the expected results. The expected results should be accurate and complete in order for the testers to fully understand what they are testing. In addition, the testers should be able to adequately compare the actual results to the expected results to ensure that the cases test the desired functionality of the system. We also observed three instances where the testers did not verify whether the actual test case results met the expected results until we questioned the testers.

IRDM Case Management system

In January 2012, the IRS issued a Tax Gap report estimating taxes owed but not paid at about $450 billion. A significant portion of this is attributed to noncompliance from businesses and corporations that underreport income. The IRS has long concluded that compliance is higher when income is subject to third-party reporting or withholding. Congress enacted IRDM legislation[30] to narrow the Tax Gap by requiring third-party payors, such as banks and brokerage firms, to submit information returns to the IRS reporting income earned by businesses on merchant payment cards and the cost basis for securities transactions. The IRS deployed four of

[29] See Appendix IV, number 19.
[30] Public Law 110-289 122 Stat. 2654, Housing and Economic Recovery Act of 2008.

five IRDM information technology projects to assimilate and correlate data submitted on filed business tax returns to information returns and select individual sole proprietor and business returns for examination. The IRDM Case Management system enables tax examiners to manage and work business cases with identified discrepancies that could potentially affect tax liabilities on business tax returns.

During our review of the IRDM Case Management system,[31] we found that the system requirements were not sufficient. User Acceptance Testing generated a high number of problem tickets, 50 percent of which were to clarify requirements and business rules. After a year of User Acceptance Testing, IRS officials acknowledged that the system could not effectively process business cases containing underreported income and could not be deployed into the production environment.

As a result, the IRS does not have an effective and efficient system to process thousands of business taxpayer cases containing underreported income. In the absence of an IRDM Case Management system, some cases were processed manually by IRS campus staff, while thousands of cases have not been processed. The IRS spent approximately $8.6 million from FYs 2009 through 2013 on developing the system. Unprocessed FY 2011 cases could have potentially resulted in assessed taxes of $54.9 million.

The TASIS

The Taxpayer Advocate Service's mission is to help taxpayers resolve problems with the IRS. The current automated tools that Taxpayer Advocate Service employees rely on are obsolete, and the multiple technology platforms in place are costly and ineffective. Successful development and implementation of the planned TASIS would enable the National Taxpayer Advocate and the estimated 1,000 case advocates to better address taxpayer's needs on a range of requests for assistance. Initial functionality for the TASIS includes managing and documenting case advocacy activities that support taxpayer requests for Taxpayer Advocate Service assistance.

During our review of the TASIS,[32] we found that, after persistent delays and concerns with the initial TASIS project, the IRS began redirecting the development effort in January 2014. Specifically, the IRS initiated a Customer Technical Review process to help validate whether the current approach for TASIS could provide the necessary functionality as designed. However, development activities for the TASIS project are currently on hold and unforeseen problems with the new system are being evaluated. We identified the following areas that needed improvement:

- Requirements management practices were not sufficient to successfully develop the TASIS. In November 2011, TASIS requirements were baselined and approved by all parties. However, as of April 2014, after 37 months and approximately $10.76 million in

[31] See Appendix IV, number 18.
[32] See Appendix IV, number 20.

expenditures, the necessary requirements still are not clarified or stabilized sufficiently to ensure that Taxpayer Advocate Service operational needs will be met under the system development path that was charted for the TASIS.

- Critical roles and responsibilities were not established or clearly communicated. Key system management documentation did not specify critical roles and responsibilities needed for TASIS development. In addition, various IRS stakeholders with key responsibilities and interests were not guided through a team approach to ensure successful systems development for the TASIS.
- System requirements have not yet been sufficiently verified. TASIS requirements were not mapped to the commercial off-the-shelf product functionality to determine whether this solution could meet 80 percent of the TASIS Project requirements as required by the Internal Revenue Manual.

We also observed that the case management functionality expected for Release 1 was one of more than 200 other case management applications across the IRS. This approach should be carefully reconsidered to address three important information technology management areas: 1) customer service, 2) system integration and efficiencies, and 3) data integrity and sharing.

FRS development

The Government Performance and Results Modernization Act of 2010[33] emphasizes the importance of: (1) establishing annual performance goals to define the level of performance; (2) expressing goals in an objective, quantifiable, and measurable form; (3) providing a description of how the performance goals are to be achieved; and (4) establishing a balanced set of performance indicators to be used in measuring or assessing progress toward each performance goal. The IRS has employed an incremental delivery approach for FATCA information technology projects and divided the FRS project into two production releases, deployed in July and December 2013. However, during our review of the FATCA FRS project,[34] we found that performance goals and measures for FRS Release 1.1 have not been implemented.

We also found that it has been almost a full year since the first delivery of FRS functionality and the IRS has not yet determined the expected benefits from this significant information technology investment. Further, we believe that future FATCA system development efforts would benefit from the earlier partnering of the Large Business and International Division with the IT organization to develop and publish performance measures. This partnering might ensure that adequate governance is in place to align information technology strategy with business

[33] Pub. L. No. 111-352, 124 Stat. 3866 (2011). This act amends the Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, 107 Stat. 285 (codified as amended in scattered sections of 5 U.S.C., 31 U.S.C., and 39 U.S.C.).

[34] See Appendix IV, number 21.

strategy and to measure the effectiveness and efficiency of FATCA information technology investments.

We also found that improved traceability of system requirements to testing can be achieved through available automated tools. The IBM Rational Quality Manager (RQM) tool is the IRS's Enterprise Architecture standard for test case management during system development. IBM Rational ReqPro was used to generate a Requirements Traceability Verification Matrix to record and track requirements from inception through system acceptability testing of the requirements. System Acceptability Testing management stated that they do not currently use full automation afforded by the Rational tool suite to integrate Rational ReqPro with the RQM for the FRS. Regarding the use of the RQM for the FATCA, System Acceptability Testing management stated that they are moving away from the use of manual spreadsheets toward implementing requirements in the RQM, which will allow better traceability in the future.

Increased Support Is Needed to Ensure the Effectiveness of the Final Integration Test

The IRS defines the Final Integration Test (FIT) program as the integrated end-to-end testing of multiple systems which support the high-level business requirements of the IRS. The FIT is the final step of the application software testing effort designed to ensure that revisions to the IRS computer applications inter-operate correctly prior to the tax return filing season.

During our review of the FIT program,[35] we identified that each year the FIT program makes a significant contribution to the success of the filing season. For Processing Year 2014, the FIT program developed a test plan including more than 2,300 test cases for 48 tax processing systems. The Processing Year 2014 FIT program identified more than 500 problems that could have resulted in the failure of individual and business tax returns to be properly processed. Although the FIT program successfully identified problems that could have resulted in the failure of tax returns to be properly processed, support for the FIT program from IRS organizations could be improved or extended.

We determined the Applications Development organization delivered programming changes in mid-December 2013, one month after the planned start of FIT execution. There were numerous programming errors identified which required FIT program resources to report and resolve. However, support from the Enterprise Operations organization and the Wage and Investment Division was withdrawn from the FIT program prior to the completion of the test execution process to support the filing season. The early loss of support resulted in unplanned deviations from the FIT plan, as not all tests could be completed as planned.

We also found that the IRS does not have a formal process to evaluate, compare, and synchronize the FIT and filing season environments, and that the Integrated Customer

[35] See Appendix IV, number 8.

Communications Environment was not available for testing. In addition, the FIT program has not established performance metrics to compare actual performance with expected performance. Finally, we found that there were problems with test analysts accessing the Employee User Portal and Integrated Enterprise Portal, which caused interruptions in the performance of the Processing Year 2014 FIT.

Information Technology Asset Management Should Be Improved to Achieve Program Efficiencies and Realize Cost Savings

Efficient and cost-effective management of information technology assets is crucial to ensuring that information technology services continue to support IRS's business operations and help it to provide services to taxpayers efficiently. We identified weaknesses in the inventory management of mainframe and server software licenses, electronic equipment being disposed of, and telecommunications equipment.

Software asset management

Software asset management is a process for tracking and reporting the use and ownership of software assets. A critical part of software asset management is mainframe and server software license management. The objective of software license management is to manage, control, and protect an organization's software assets, including management of the risks arising from the use of those software assets. Proper management of software licenses helps to minimize risks by ensuring that licenses are used in compliance with licensing agreements and cost-effectively deployed and that software purchasing and maintenance expenses are properly controlled.

During our reviews of the IRS's software license management processes for the server[36] and mainframe[37] environments, we identified that the IRS does not have an enterprise-wide software licensing program designed around industry best practices. The IRS does not have enterprise-wide or local policies, procedures, and requirements for managing server or mainframe software licenses. The IRS has defined software asset and license management roles and responsibilities only for the Chief Information Officer/CTO. IRS policy does not provide any additional roles and responsibilities for software asset and license management.

The IRS also does not have a centralized, enterprise-wide organizational structure for managing server and mainframe software licenses. Functions managing licenses are dispersed throughout the IT organization and business units depending on factors such as whether the software is platform infrastructure, a specialized application used by a specific business unit, and in general, what process the software performs.

[36] See Appendix IV, number 16.
[37] See Appendix IV, number 2.

The inadequate management of server and mainframe software licenses has resulted in a waste of funds spent on software licenses and maintenance. The IRS is in the process of developing an enterprise-wide software management program to address these weaknesses.

Physical asset management

Disposition of Assets: In October 2009, President Obama signed into law Executive Order 13514, *Federal Leadership in Environmental, Energy, and Economic Performance*,[38] with the intent to create a clean energy economy that would increase the Nation's prosperity, promote energy security, protect the interest of taxpayers, and safeguard the health of our environment. To fulfill Executive Order 13514's requirements, the General Services Administration developed guidance for Federal agencies to follow that includes establishing a comprehensive and transparent Governmentwide policy on used Federal electronics that maximizes reuse, clears data and information stored on used equipment, and ensures that all Federal electronics are processed by certified recyclers.

During our review of the IRS's disposal of information technology asset inventory,[39] we determined that while the IRS is complying with requirements to donate its previously used information technology equipment to non-Federal recipient organizations, there are several processes associated with asset disposal that need improvement. For example, improved documentation is needed to ensure compliance with media sanitization guidelines.

Controls over the processing of Federal electronic assets reported as missing, lost, or stolen can be strengthened. Information technology equipment that cannot be located are written off; however, these lost items are not reported to the Computer Security Incident Response Center as required. Further, documentation of disposal actions can be improved, and the inventory system does not archive electronic asset disposal data.

Telecommunications: In FY 2013, the IRS spent more than $13.7 million on wireless telecommunication devices and maintained an inventory of more than 49,000 devices reported as being in use. Effective controls over the assignment of and inventory accounting for these devices is important to ensure proper stewardship of Government funds.

In TIGTA's previous work,[40] we found that IRS processes for assigning and monitoring the use of devices were not adequate to ensure that employees have a business need for the devices. In addition, prior work found that the IRS paid for thousands of devices that were unused.

During our review of IRS wireless inventory controls,[41] we determined that inventory controls over wireless devices could be improved. Federal guidance requires the IRS to assess current

[38] Exec. Order No. 13514, *Federal Leadership in Environmental, Energy, and Economic Performance*, 3 C.F.R. 52117 (2009).
[39] See Appendix IV, number 5.
[40] TIGTA, Ref. No. 2013-22-094, *Increased Oversight of Information Technology Hardware Maintenance Contracts Is Necessary to Ensure Against Paying for Unnecessary Services* (Sept 2013).

device inventories and usage and establish controls to ensure that the IRS is not paying for unused or underutilized devices. We found that more than 94 percent of IRS employees were appropriately assigned a BlackBerry® smartphone, cellular phone, or wireless aircard device, while almost 6 percent were in positions that the IRS had not designated as eligible for the device. The IRS's systems of record designed to document wireless device inventory were not consistently updated as changes occurred, which resulted in almost 57 percent of inventory records being inaccurate. For example, serial numbers, barcodes, and telephone numbers were not accurately documented in inventory records.

Ineffective inventory controls resulted in unsupported and duplicate service fees. Specifically, we found the IRS paid monthly service fees for almost 6,800 wireless devices that were not captured in inventory records and for more than 700 employees who had multiple wireless devices that perform the same function according to monthly vendor billing statements.

[41] See Appendix IV, number 12.

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 2014. 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 issues 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 FY 2014. 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 Government Accountability Office).

III. Assessed systems modernization and applications development issues. We determined which issues 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 FY 2014. During the review, we analyzed and prepared an overall assessment of modernization and applications development issues.

   B. Identified and summarized relevant non-SITS and/or external oversight assessments dealing with modernizations and applications development.

IV. Assessed systems operations issues. We determined which issues 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 FY 2014. During the review, we analyzed and prepared an overall assessment of systems operations issues.

[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.).

B. Identified and summarized other relevant TIGTA assessments dealing with operations.

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
Kent Sagara, Director
Danny Verneuille, Director
Myron Gulley, Audit Manager
Ryan Perry, Lead Auditor
Andrea Barnes, Senior Auditor
Richard Borst, Senior Auditor
George Franklin, Senior Auditor
Tina Wong, 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
Deputy Chief Information Officer for Strategy and Modernization OS:CTO
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 Information Technology – Program Management Office OS:CTO:EIT
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
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	Report Reference Number	Audit Report Title	Report Issuance Date
1	2014-IE-R004	*Inspection of the Submission Processing Centers' Mailroom Screening Procedures for Hazardous Material*	December 13, 2013
2	2014-20-002	*The Internal Revenue Service Should Improve Mainframe Software Asset Management and Reduce Costs*	February 20, 2014
3	2014-20-016	*Planning Is Underway for the Enterprise-Wide Transition to Internet Protocol Version 6, but Further Actions Are Needed*	February 27, 2014
4	2014-40-020	*Improvement Is Needed to Better Enable Frontline Employee Identification of Potentially Dangerous and Caution Upon Contact Designations*	March 20, 2014
5	2014-20-021	*Used Information Technology Assets Are Being Properly Donated; However, Disposition Procedures Need to Be Improved*	April 25, 2014
6	2014-10-037	*Some Contractor Personnel Without Background Investigations Had Access to Taxpayer Data and Other Sensitive Information*	July 7, 2014
7	2014-20-069	*Progress Has Been Made; However, Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12*	September 12, 2014
8	2014-20-085	*Increased Support Is Needed to Ensure the Effectiveness of the Final Integration Test*	September 15, 2014

Number	Report Reference Number	Audit Report Title	Report Issuance Date
9	2014-20-059	*The Office of Safeguards Should Improve Management Oversight and Internal Controls to Ensure the Effective Protection of Federal Tax Information*	September 15, 2014
10	2014-23-070	*Affordable Care Act: Expanded Guidance Provided Assistance to the Exchanges, but Greater Assurance of the Protection of Federal Tax Information Is Needed*	September 16, 2014
11	2014-20-083	*The Internal Revenue Service Should Implement an Efficient, Internal Information Security Continuous Monitoring Program That Meets Its Security Needs*	September 17, 2014
12	2014-10-075	*Wireless Telecommunication Device Inventory Control Weaknesses Resulted in Inaccurate Inventory Records and Unsupported Service Fees*	September 19, 2014
13	2014-20-092	*The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decisions*	September 22, 2014
14	2014-20-087	*While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget*	September 22, 2014
15	2014-20-090	*Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2014*	September 23, 2014
16	2014-20-042	*The Internal Revenue Service Should Improve Server Software Asset Management and Reduce Costs*	September 25, 2014

Number	Report Reference Number	Audit Report Title	Report Issuance Date
17	2014-20-063	*Customer Account Data Engine 2 Database Validation Is Progressing; However, Data Coverage, Data Defect Reporting, and Documentation Need Improvement*	September 29, 2014
18	2014-20-088	*The Information Reporting and Document Matching Case Management System Could Not Be Deployed*	September 29, 2014
19	2014-23-072	*Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns Project*	September 29, 2014
20	2014-20-071	*Information Technology: Improvements Are Needed to Successfully Plan and Deliver the New Taxpayer Advocate Service Integrated System*	September 30, 2014
21	2014-20-094	*While the Foreign Financial Institution Registration System Deployed on Time, Improved Controls Are Needed*	September 30, 2014

Appendix V

Outcome Measures Reported in Fiscal Year 2014

Audit Report Title	Type of Measure	Amount
The Internal Revenue Service Should Improve Mainframe Software Asset Management and Reduce Costs	Inefficient Use of Resources – Potential	$11,649,342
	Funds Put to Better Use – Potential	$50,000
Some Contractor Personnel Without Background Investigations Had Access to Taxpayer Data and Other Sensitive Information	Taxpayer Privacy and Security – Potential	1.4 million taxpayer accounts affected
While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget	Taxpayer Privacy and Security – Potential	308 potential incidents of Personally Identifiable Information (PII) and tax account disclosures
The Information Reporting and Document Matching Case Management System Could Not Be Deployed	Inefficient Use of Resources – Potential	$8.6 million
	Increased Revenue – Potential	$54.9 million
The Internal Revenue Service Should Improve Server Software Asset Management and Reduce Costs	Inefficient Use of Resources – Potential	$97.8 million
Wireless Telecommunication Device Inventory Control Weaknesses Resulted in Inaccurate Inventory Records and Unsupported Service Fees	Cost Savings: Funds Put to Better Use – Potential	$2,183,220 for FY 2013

Appendix VI

Glossary of Terms

Term	Definition
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.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.
Critical Code Weakness	According to the IRS, critical priority weaknesses have both a high potential impact and a high likelihood of occurring. They represent the highest security risks to an application and should be remediated immediately.
Customer Account Data Engine 2	An IRS application that will replace the existing Individual Master File and Customer Account Data Engine applications. The Customer Account Data Engine 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.
Employee User Portal	The internal IRS portal that allows IRS employee users to access IRS data and systems, such as tax administration processing systems, financial information systems, and other data and applications, including mission critical applications.
Enterprise Life Cycle	A structured business systems development methodology that requires the preparation of specific work products during different phases of the development process.
Exchanges	Officially called, Health Insurance Marketplace, Exchanges are State or Federally operated programs where many people can buy health care coverage.

Term	Definition
Federal Information Security Management Act	A statute that requires agencies to assess risks to information systems and provide information security protections commensurate with the risks. The Federal Information Security Management Act 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.)
Field Identifier	An IRS file format that uses a numeric field to identify a data field.
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.
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.
High Code Weakness	According to the IRS, high priority weaknesses have the potential for high impact but a low likelihood of occurring and should be remediated in the next scheduled patch release.
Identity Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by an entity.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Integrated Customer Communications Environment	An automated self-help system that provides customer service applications through toll-free telephone service and the Internet. The toll-free telephone service provides automated self-service applications that allow taxpayers to help themselves, as well as providing avenues to route taxpayers to live customer service representatives. The Internet component of the Integrated Customer Communications Environment allows taxpayers to check their refund status.
Integrated Enterprise Portal	Allows registered individuals, third-party users, and self-authenticated individual taxpayers access to selected specific tax information and other sensitive applications and data. It supports the exchange of bulk files of information with the IRS.

Term	Definition
Internet Protocol Version 6	The next generation Internet Protocol which allows a 128-bit Internet Protocol address field in the form of eight 16-bit integers represented as four hexadecimal digits separated by colons.
Low Code Weakness	According to the IRS, low priority weaknesses have low potential impact and a low likelihood of occurring and represent a minor security risk to an application.
Medium Code Weakness	According to the IRS, medium priority weaknesses have a low potential impact but a high likelihood of occurring and represent a moderate risk to an application. They are easy to detect and exploit.
Moderate System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a Federal Information Processing Standard 199 potential impact value of moderate, and no security objective is assigned a Federal Information Processing Standard 199 potential impact value of high.
National Institute of Standards and Technology	A nonregulatory Federal agency within the Department of Commerce responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
Nation-state	A form of political organization in which a group of people who share the same history, traditions, or language live in a particular area under one government.
Out-of-the-Box Solution	A feature or functionality of a product that works immediately after installation without any configuration or modification.
Processing Year	The calendar year in which the tax return or document is processed by the IRS.
Requirement	A formalization of a need that is the statement of a capability or condition that a system, subsystem, or system component must have or meet to satisfy a contract, standard, or specification.
Requirements Traceability Verification Matrix	A tool that documents requirements and establishes the traceability relationships between the requirements to be tested and their associated test cases and test results.

Term	Definition
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.
Tax Gap	The estimated difference between the amount of tax that taxpayers should pay and the amount that is paid voluntarily and on time.
Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
Wireless Aircard	A device that provides mobile internet access from laptops when employees are working outside of an IRS office.