TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the Internal Revenue Service Information Technology Program

September 30, 2016

Reference Number: 2016-20-094

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

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE INFORMATION TECHNOLOGY PROGRAM

Highlights

Final Report issued on September 30, 2016

Highlights of Reference Number: 2016-20-094 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

In Fiscal Year 2015, the IRS collected more than $3.3 trillion in Federal tax payments, processed hundreds of millions of tax and information returns, and paid about $403 billion in refunds to taxpayers. In addition, the IRS employs over 80,000 people in 554 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the IRS's Information Technology Program could result in computer operations that become compromised, disrupted, or outdated, which could adversely affect the IRS's ability to meet its mission of providing America's taxpayers with top-quality service by helping them understand and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 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, improving tax systems and online services, and operations for Fiscal Year 2016.

WHAT TIGTA FOUND

TIGTA has designated *Security for Taxpayer Data and IRS Employees* as the number one management and performance challenge facing the IRS for the sixth consecutive year. While the IRS continues to work toward securing tax information and maintaining taxpayer privacy, much work remains. TIGTA identified weaknesses within the IRS's cybersecurity program in which three domains need significant improvement (Information Security Continuous Monitoring, Configuration Management, and Identity and Access Management). TIGTA also identified weaknesses in the electronic authentication process controls. Additional areas that need improvement include physical security controls, backing up and restoring data, and SharePoint controls.

In addition, the IRS continues to update its systems in an effort to combat identity theft and tax refund fraud. During the 2016 Filing Season, the IRS implemented three new data elements into its Return Review Program. As of March 25, 2016, the IRS had detected $72 million in suspected tax return refund fraud that was directly attributable to the new data elements. The IRS is testing additional new data elements for future implementation.

The IRS continues to develop systems to implement the Affordable Care Act and other tax law changes. The IRS successfully tested the functionality and security of the Affordable Care Act Compliance Validation System. However, the Foreign Account Tax Compliance Act Program Withholding & Refund Release 2.0 system was built to requirements but has not provided the intended business results. Finally, TIGTA identified concerns with information technology contract administration controls and the enterprise e-mail acquisition.

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 2016, TIGTA did not make any recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 30, 2016

MEMORANDUM FOR CHIEF INFORMATION 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 # 201620002)

This report presents the results of our assessment of the Internal Revenue Service's (IRS) Information Technology Program, including security, improving tax systems and online services, and operations for Fiscal Year 2016.[1] This review is required by the IRS Restructuring and Reform Act of 1998.[2] This audit is included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenges of Security for Taxpayer Data and IRS Employees, Implementing the Affordable Care Act and Other Tax Law Changes, Fraudulent Claims and Improper Payments, Achieving Program Efficiencies and Cost Savings, and Improving Tax Systems and Online Services.

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 R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

[1] 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.
[2] 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
CIO	Chief Information Officer
DHS	Department of Homeland Security
EFDS	Electronic Fraud Detection System
FATCA	Foreign Account Tax Compliance Act
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive-12
IPM	Integrated Production Model
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
RRP	Return Review Program
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 for Fiscal Year (FY) 2016.[2] The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In FY 2015, the IRS collected approximately $3.3 trillion in Federal tax payments, processed hundreds of millions of tax and information returns, and paid approximately $403 billion in refunds to taxpayers. Further, the size and complexity of the IRS add unique operational challenges. The IRS employs almost 80,000 people in its Washington, D.C., headquarters and more than 550 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 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 Internet 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 2015, 78.2 percent of individual taxpayers chose to file electronically, a significant increase from 71.3 percent in FY 2010. Outside of filing activities, taxpayers also use the Internet to download forms, view content, and check refund status. The IRS website continued to get heavy use, with more than 493 million visits to IRS.gov during FY 2015. One of the most popular online tools (Where's My Refund?) handled a record-breaking 234 million inquiries, a 24 percent increase over the prior year.

The IRS's FY 2016 appropriations increased by $290 million to $11.2 billion over FY 2015 levels, with the increase being targeted to improve taxpayer service, combat identity theft, and improve cybersecurity. Even with the increase for FY 2016, IRS appropriations remain about 7 percent below FY 2011 levels. As the Government Accountability Office (GAO) reported in

[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.

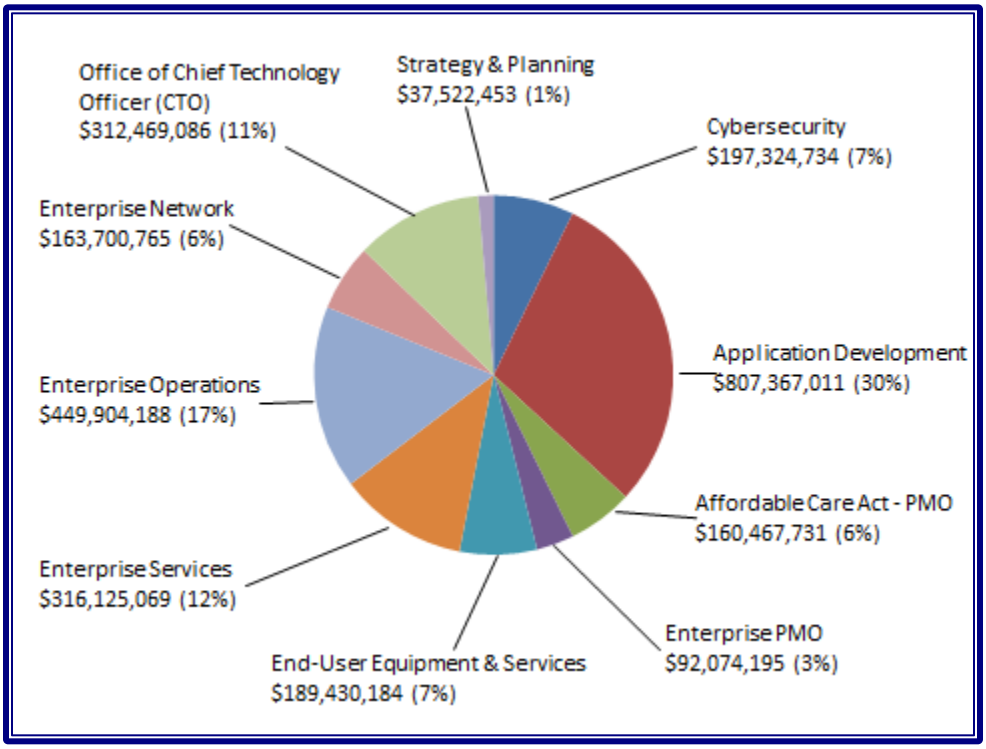
March 2016,[3] these declines have contributed to fluctuations in taxpayer service and longer wait times on the telephones than taxpayers have historically experienced.

The Information Technology (IT) organization and other information technology expenses comprise a significant portion of the IRS's budget and play a critical role in enabling the IRS to carry out its mission and responsibilities. The IRS's FY 2016 appropriations included about $2.5 billion for information technology investments; this represents 20 percent of the total IRS budget. As previously discussed, the IRS received a $290 million increase to its FY 2016 budget as compared to FY 2015 levels. Cybersecurity was allocated almost one-third of the funding, solely from the Operations Support appropriation account. This funding included $7 million to maintain the cybersecurity workforce (50 additional full-time equivalents).

Figure 1 illustrates FY 2016 information technology funding, generally aligning information technology funds by an Associate Chief Information Officer (CIO) organization. The Associate CIO User and Network Services organization is represented by two functional areas, Enterprise Networks and End-User Equipment & Services, in order to provide budget transparency.

[3] GAO, GAO-16-695, *IRS 2017 BUDGET: IRS Could Improve Presentation of Budget Data in Its Congressional Justification* (July 2016).

Figure 1: IRS IT Organization FY 2016 Total Available Funding (by Associate CIO Organization)[4]

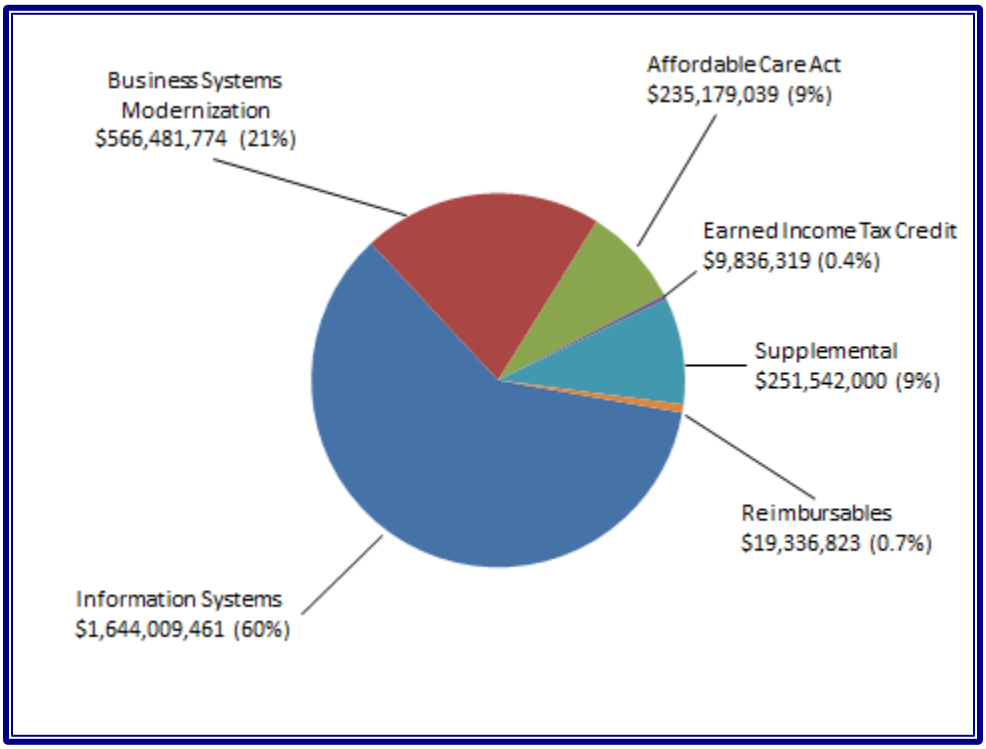


Source: TIGTA analysis of the IRS IT organization budget data as of July 2016 based on information provided by the Associate CIO, Strategy and Planning, Financial Management Services. *PMO = Program Management Office.

[4] The proportions of funding by Associate CIO areas or Associate CIOs with Business Systems Modernization funding are overstated because not all of these funds will be spent this year.

Figure 2 shows information technology funding for FY 2016 by funding source.

Figure 2: IRS IT Organization FY 2016 Total Available Funding (by Funding Source)[5]



Source: TIGTA analysis of the IRS IT organization budget data as of July 2016 based on information provided by the Associate CIO, Strategy and Planning, Financial Management Services.

[5] The proportions of funding by Associate CIO areas or Associate CIOs with Business Systems Modernization funding are overstated because not all of these funds will be spent this year.

Figure 3 illustrates that, as of July 2016, the IRS had a total of 6,703 information technology employees working across eight different business units.

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

Information Technology Business Unit	Number of Employees
Applications Development	1,936
Enterprise Operations	1,764
User and Network Services	1,463
Enterprise Services	650
Cybersecurity	338
Enterprise Program Management Office	279
Strategy & Planning	264
Office of the CIO*	9
Total	6,703

Source: Treasury Integrated Management Information System as of July 2016. *As of July 7, 2016, the IRS IT organization is now led by the CIO instead of the Chief Technology Officer. Where possible, all references to the Chief Technology Officer have been revised to the CIO.

- **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-scale 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 computing (server and mainframe) services for all IRS business entities and taxpayers.
- **Enterprise Services** is responsible for strengthening technology infrastructure across the enterprise, along with providing independent systems acceptability testing, final

integration testing, and performance and integration testing on select IRS systems and applications.

- **Strategy and Planning** collaborates with IT organization leadership to provide policy, direction, and administration of essential programs, including strategy and capital planning, performance measurement, financial management services, 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 Service Desk as the single point of contact for reporting an information technology issue, and equips the Volunteer Income Tax Assistance program.
- **The Office of the CIO** includes the CIO, two Deputy Chief Information Officers, and their staff. A Deputy Chief Information Officer serves as principal advisor to the CIO 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.

In July 2015, the IRS IT organization employed 7,042 employees, 339 more full-time personnel than in FY 2016.

The compilation of information for this report was conducted at TIGTA offices in Dallas, Texas, and New Carrollton, Maryland, during the period June through September 2016. The information presented is derived from TIGTA audit reports issued between October 1, 2015, and September 30, 2016. We also reviewed relevant GAO reports and IRS 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 the IRS's IT organization program efforts in systems security, development, 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.

For FY 2016, TIGTA designated *Security for Taxpayer Data and IRS Employees* as the number one management and performance challenge area for the sixth 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 2015 Office of Management and Budget (OMB) report to Congress,[6] malicious actors continue to gain unauthorized access to, and compromise, Federal networks, information systems, and data. During FY 2015, Federal agencies reported 77,183 cybersecurity incidents to the U.S. Computer Emergency Readiness Team, a 10 percent increase over the 69,851 incident reports in FY 2014. The U.S. Computer Emergency Readiness Team 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, 2015, to July 31, 2016, the IRS reported 376 incidents to the U.S. Computer Emergency Readiness Team. Of those 376 incidents, more than 80 percent (322) were from lost or stolen information technology equipment, and the next highest category of incidents, at 5 percent (17), involved successful malicious code attacks.

Security and Privacy of Federal Tax Information

The IRS is an attractive target to hackers because of its mission and the large amounts of tax data it processes and stores. Whether it pertains to defending its networks, detecting when incidents

[6] OMB, *Annual Report to Congress: Federal Information Security Management Act* (Mar. 2016).

occur, or remediating those incidents, the IRS takes the protection of taxpayer privacy very seriously.

We performed several audits to assess the IRS's efforts to protect its information and taxpayer data. Some of these audits focused solely on how the IRS mitigates its information security risks. We also reviewed electronic authentication process controls, data storage and backup, and several areas addressing physical security controls.

Overall assessment of the IRS Information Security Program

The Federal Information Security Modernization Act of 2014,[7] commonly referred to as the FISMA, focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. The FISMA requires Federal agencies to develop, document, and implement an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or entity. The FISMA is supported by the OMB, the Department of Homeland Security (DHS), agency security policy, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST) related to information security practices.

The FISMA directs Federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with the FISMA. The DHS is responsible for the operational aspects of Federal cybersecurity, such as establishing governmentwide incident response and operating the tool to collect FISMA metrics.

For FY 2016, the DHS issued its FISMA Inspector General Reporting Metrics[8] with three significant changes from last year.

1) The DHS organized the FY 2016 Inspector General FISMA Reporting Metrics around the five information security functions outlined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework):[9] *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. Eight security program areas evaluated in prior FISMA evaluations were aligned within the Cybersecurity Framework functions and included: Risk Management, Contractor Systems, Configuration Management, Identity and Access Management, Information Security Continuous Monitoring, Incident Response, Security and Privacy Training, and Contingency Planning.

[7] Pub. L. No. 113-283. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.
[8] DHS, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (Version 1.1.1, Aug. 2016).
[9] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, Feb. 2014).

2) The DHS implemented a new scoring methodology based on five levels of maturity: *Ad-Hoc* (level 1), *Defined* (level 2), *Consistently Implemented* (level 3), *Managed and Measureable* (level 4), and *Optimized* (level 5). Agencies with programs that score at or above the *Managed and Measureable* level for a NIST Cybersecurity Framework function are considered to have "effective" programs within that area in accordance with the definition of effectiveness in NIST Special Publication 800-53.[10] To score at or above the *Managed and Measurable* level, all metrics listed under the *Defined* and *Consistently Implemented* levels must be met, plus half or more of metrics listed under *Managed and Measureable* must be met.

3) The DHS, in coordination with other key stakeholders, continued the effort begun in FY 2015 to develop maturity models. In addition to the Information Security Continuous Monitoring maturity model, which was included in the FY 2015 Inspector General FISMA Reporting Metrics, the FY 2016 Inspector General FISMA Reporting Metrics included a maturity model for the Incident Response program area.

During our FY 2016 FISMA review,[11] we found that the IRS has established an information security program that is generally aligned with applicable FISMA requirements, OMB policy and guidance, and the NIST standards and guidelines. However, due to program attributes not yet implemented, the IRS's Information Security Program is not fully effective. Based on the DHS's scoring methodology for the FY 2016 FISMA evaluation period, three security functions rated as "not effective" and two security functions rated as "effective" as shown in Figure 4.

[10] The Inspector General FISMA Reporting Metrics leverage NIST Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013, updated Jan. 2015), which defines security control effectiveness as the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

[11] TIGTA, Ref. No. 2016-20-092, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016* (Sept. 2016).

Figure 4: Security Function Effectiveness Based on the Implementation of DHS-Specified Attributes

Cybersecurity Framework Security Functions	FY 2016 Inspector General FISMA Metric Domains	Effective Security Function
Identify	• *Risk Management* (met 13 of 16 attributes) • *Contractor Systems* (met all attributes)	No
Protect	• *Configuration Management* (did not meet a majority of attributes) • *Identity and Access Management* (did not meet a majority of attributes) • *Security and Privacy Training* (met all attributes)	No
Detect	• *Information Security Continuous Monitoring* (maturity model level of two)	No
Respond	• *Incident Response* (maturity model level of four)	Yes
Recover	• *Contingency Planning* (met all attributes)	Yes

Source: TIGTA's evaluation of security program attributes, which provided the basis for determining whether security functions were rated "effective" or "not effective."

We found that three security program areas (*Contractor Systems*, *Security and Privacy Training*, and *Contingency Planning*) met all performance attributes. The *Risk Management* program area needed improvement on three of 16 performance metrics, related to ensuring that 1) system interconnections in use had proper authorization or security agreements, 2) Plans of Action and Milestones were maintained and effective for correcting security weaknesses, and 3) an insider threat detection and prevention program is implemented.

The IRS has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with the FISMA, NIST standards, and OMB guidance. Based on the maturity model issued in the FY 2016 Inspector General FISMA Reporting Metrics for this program area, the IRS's incident response program has achieved a maturity level of four, *Managed and Measurable*, on the scale of one to five. The IRS successfully demonstrated all nine of the level-four attributes. However, TIGTA provided a comment on one metric (Metric 4.3.1.2) related to ensuring that key incident response personnel have the appropriate knowledge, skills, and abilities to successfully operate this mission-critical program.

We determined that three metric domains need significant improvement in order for the IRS to meet all performance attributes.

- ***Information Security Continuous Monitoring (ISCM)***

  The ISCM program area is at a maturity level of two (*Defined*) on the DHS's scale of one to five. The OMB requires Federal agencies to implement an ISCM program that automates asset management and maintains secure configuration of assets in real time. In July 2014, the Department of the Treasury decided to adopt a uniform approach to ISCM across the Treasury and to use the toolset selected by the DHS to meet the program requirements. The DHS is in the process of procuring a standard set of cybersecurity tools and services for use by Federal agencies. 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, ISCM 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. The IRS is working in concert with the DHS's implementation phases, and currently performs ISCM-related activities using numerous templates and tools deployed within the enterprise.

- ***Configuration Management***

  The *Configuration Management* program area did not meet the majority of the attributes specified by the DHS. The IRS has established standard baseline configurations for information systems and system components. In addition, the IRS uses automated compliance tools to scan for improper configurations, vulnerabilities, and software flaws. However, deficiencies continue to exist in ensuring baseline configurations are maintained and reported vulnerabilities are corrected timely. In addition, the IRS is still working to expand a standard automated process to deploy operating system patches Service-wide. Eventually, the IRS's *Configuration Management* program area will benefit from the implementation of ISCM, which intends to use automation to produce an accurate inventory of devices and software on the IRS network and to automate configuration management of these devices and software in near real time.

- ***Identity and Access Management***

  The Identity and Access Management program did not meet a majority of the attributes specified by the DHS. The IRS has made progress in implementing the use of personal identity verification (PIV) cards for network and remote access in compliance with

Homeland Security Presidential Directive 12 (HSPD-12),[12] but more work is needed to enforce PIV card access to systems and for physical access to IRS facilities.

Also, the IRS has not consistently implemented controls to ensure that:

- Users are not granted more access than they need.
- The use of administrative privileges is tracked and periodically reviewed.
- Accounts are terminated when no longer required.
- The use of shared accounts is controlled.

In addition to our FY 2016 FISMA work, the GAO conducted its annual IRS financial statement audit on the IRS, which includes evaluating security controls over the IRS's financial systems. During FY 2016, the GAO stated that the IRS continued to make progress in implementing an effective Information Security Program. The IRS has a well-organized framework for its program, such as assessing risk for its systems and developing security plans. However, the GAO concluded that significant weaknesses remaining in implementing the security controls limited their effectiveness in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer data.[13] Specifically, the IRS had not updated key mainframe policies and procedures to address issues such as comprehensively auditing and monitoring access. Further, the IRS had not ensured that many of its corrective actions to address previously identified deficiencies were effective.

Electronic authentication process controls

The increasing number of data breaches in the private and public sectors means more personal information than ever before is available to unscrupulous individuals. Much of these data are detailed enough to enable circumvention of most authentication processes. As such, it is critical that the methods the IRS uses to authenticate individuals' identities provide a high level of confidence that tax information and services are provided only to individuals who are entitled to receive them. The risk of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering online tools to taxpayers. The consequences of unauthorized accesses include expanding the taxpayers' preexisting identity theft issues and potential delays in tax return processing while identity theft issues are resolved.

[12] DHS, HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, was signed by President Bush on August 27, 2004. This directive established a new standard for issuing and maintaining identification badges for Federal employees and contractors entering Government facilities and accessing computer systems. The intent was to improve security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Agencies are required to use PIV badges (also referred to as SmartID cards) to access computer systems (logical access).

[13] GAO, GAO-16-398, *Information Security: IRS Needs to Further Improve Controls Over Financial and Taxpayer Data* (Mar. 2016).

The IRS deployed the Get Transcript application on its public website (www.IRS.gov) in January 2014. This application allows taxpayers to view and download their tax information, such as account transactions, line-by-line tax return information, and income reported to the IRS. From October 1, 2014, through April 15, 2015, the IRS provided 23 million transcripts to individuals using the Get Transcript application.

On May 14, 2015, the IRS Computer Security Incident Response Center identified a significant number of undeliverable e-mails sent by the online authentication system. These e-mails were the confirmation code e-mails that the system sends individuals attempting to establish an online account. The Computer Security Incident Response Center reported the backlog of undeliverable e-mails to the Information Technology organization's Cybersecurity function. Cybersecurity function officials and the Office of Compliance and Analytics analyzed the e-mails. Based on its results, the IRS removed the application from its website on May 21, 2015.

As a result of this incident, the IRS determined that of 124,870 successful accesses[14] by unauthorized individuals, the individuals successfully obtained a tax transcript in 113,383 of the access attempts (a tax transcript was not viewed in the remaining 11,487 access attempts). For the 113,383 Social Security Numbers used in these accesses, 95,181 tax returns were filed in Processing Year 2015 as of November 30, 2015. The IRS determined that 59,970 of these returns warranted review because they were filed after the account was breached through the Get Transcript application. IRS analysis of these returns identified:

- 34,201 tax returns that were detected and treated as likely identity theft. The IRS prevented a total of $119,026,062 in refunds claimed on these returns.
- 22,318 tax returns that were not treated as identity theft. The IRS paid a total of $62,196,854 in refunds claimed on these returns.
- 2,869 tax returns that were likely filed by the innocent taxpayer because the returns report either a balance due or a zero amount owed, *i.e.*, the returns do not claim a refund.

In an audit of the IRS's response to the Get Transcript incident,[15] we found that in addition to failing to identify all individuals affected by the Get Transcript application breach, the IRS did not have complete knowledge of what was being screened at the Integrated Enterprise Portal, and thus it was unaware of the weaknesses related to detecting automated attacks or which tools it might need to address them. Audit log reports were also not being adequately monitored, and the IRS did not provide responsible staff with the tools and training needed to monitor and analyze large amounts of audit log data.

[14] The attackers were able to mimic taxpayers because they had a significant amount of information on taxpayers prior to the attack, which they had obtained from non-IRS sources.
[15] TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016).

The IRS has undertaken a number of steps to improve systems and provide for more secure authentication, including strengthening application and network controls. For example, the IRS worked with the United States Digital Service[16] to identify its most pressing needs and implement an appropriate method of delivering secure account multifactor authentication. The IRS completed a number of electronic authentication improvements to implement stronger authentication, including requiring that users establish profiles, preventing one-to-many relationships for identity information (for example, an e-mail address cannot be used by more than one user), and sending a letter to taxpayers when they first create a login and password for any web application on IRS.gov. The IRS relaunched the Get Transcript application in June 2016.

Although the IRS recognizes the growing challenge it faces in establishing effective authentication processes and procedures, we identified that the IRS has not established a Service-wide approach to managing its authentication needs.[17] As a result, the level of authentication the IRS uses for its various services is not consistent. The IRS has a need to authenticate individuals' identities at two primary points of interaction—filing and processing a tax return and providing account-related services. The IRS offers a number of methods for taxpayers to interact with the IRS, *e.g.*, online, in person, and by telephone. Different access methods may require different authentication processes. The existence of differing levels of authentication assurance among the various access methods increases the risk of unscrupulous individuals accessing and obtaining personal taxpayer information or defrauding the tax system. Unscrupulous individuals can identify the weakest points of authentication and exploit them to inappropriately gain access to tax account information.

Securing data storage

In December 2010, the U.S. CIO called for a shift to a "Cloud First" policy for the Federal Government to allow agencies to optimize spending and to reinvest in their most critical mission needs.[18] In February 2011, the U.S. CIO published the *Federal Cloud Computing Strategy*, requiring Federal agencies to evaluate safe, secure cloud computing options before making any new information technology investments.[19] According to the NIST, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, *e.g.*, networks, servers, storage, applications, and services, that can be

[16] The United States Digital Service is part of the Federal Chief Information Officer Team and is tasked with working with agencies to ensure that they have the resources and talent needed to deliver great services on time, on specifications, on budget, and with optimal user functionality.
[17] TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).
[18] The White House, U.S. CIO Vivek Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 2010).
[19] The White House, U.S. CIO Vivek Kundra, *Federal Cloud Computing Strategy* (Feb. 2011).

rapidly provisioned and released with minimal management effort or service provider interaction.[20]

The Enterprise Storage Services Program provides enterprise storage for IRS data, including taxpayer and other sensitive data. The IRS reported significant cost savings with its migration of production data into the Enterprise Storage Services "Storage-As-a-Service" cloud environment since March 2013, and it estimates that this approach will save millions of dollars by providing better utilized resources. However, TIGTA found that more detailed contractual agreements are needed to support the Enterprise Storage Services Program with data security controls, including security monitoring and incident management.[21] Clear agreements between the IRS and the Enterprise Storage Services contractor would better ensure adequate preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. Also, the Service-Level Objectives established under the current contract do not clearly stipulate time frames for the contractor to mitigate losses and resecure the Enterprise Storage Services environment should a data breach occur.

Physical security controls

The FISMA provides a comprehensive framework for ensuring the effectiveness of physical and information security controls over information resources that support Federal operations and assets. Agencies are required to provide information security controls proportionate with the risk and potential harm of not having those controls in place. Agency heads are required to annually report on the effectiveness of the agencies' security programs.

The IRS's Physical Security Program, as defined in the Internal Revenue Manual, states that IRS management will provide employees with standards and processes to protect IRS lives, property, assets, and information.[22] The program states that access to facilities, sensitive information, and restricted areas where sensitive information is maintained should be granted only on a need-to-know basis as determined by business unit management officials.

- ***Access to Government Facilities and the Return of Laptop Computers When Employees Separate***

  During FY 2014, the IRS employed more than 90,000 personnel, of which more than 4,100 were full-time, permanent employees who separated for disciplinary reasons or through retirement, resignation, or death.[23] Various security-related items such as identity and building access cards must be recovered from employees prior to the effective date of separation.

[20] NIST, NIST Special Publication 800-145, *The NIST Definition of Cloud Computing* (Sept. 2011).
[21] TIGTA, Ref. No. 2016-20-002, *Measurable Agreements on Security Controls Are Needed to Support the Enterprise Storage Services Solution* (Oct. 2015).
[22] Internal Revenue Manual 10.2.1, *Physical Security*, the Physical Security Program (Sept. 2008).
[23] IRS Human Resources Reporting Center Population Report for FY 2014, including seasonal employees.

In FY 2006, the IRS began using a human resources tracking system to certify that assigned inventories of security items are recovered when employees separate from the IRS or to notate why an item is unrecoverable. Managers are responsible for entering into the system which security-related items departing employees should return and indicating when, where, and how the items will be returned.

During our review,[24] we determined that the IRS has designed controls to verify that physical access to Government facilities is secured when employees separate. The controls include a computer process to document if security items are recovered from separating employees, including a third-party verification and deactivation of the returned items. However, these controls were not effective to prevent access to Government facilities and computers after employees separated.

Based on a random sample of FY 2014 employee separations, we estimated that the IRS could not verify that all security items were recovered for over 2,700 (66 percent) of the more than 4,100 employee separations. We also reviewed a judgmental sample of 10 employees who separated during a pending disciplinary case. The IRS could not verify the recovery of the security items for six of these employees and could not provide evidence that these cases were referred to the TIGTA Office of Investigations as required. When the IRS did not collect security items, some were later used to enter IRS buildings.

In another review,[25] we determined whether IRS management implemented policies and procedures designed to provide reasonable assurance that laptop computers are returned when employees separate from the IRS. There is an additional risk when an employee separates under adverse conditions. When an employee is terminated for an adverse reason, managers are required to collect the laptop immediately to avoid loss of the computer or the potential inadvertent release of sensitive information by the separated employee. If the manager cannot recover a separating employee's laptop, a report should be submitted to the Computer Security Incident Response Center and TIGTA's Office of Investigations explaining the circumstances of the nonrecovery.

According to IRS policy, after recovery of a laptop from a separating employee, the manager should create an equipment return services ticket to arrange for return of the equipment to the IT organization. The IT organization technician reviews the laptop's barcode to assure that it is the correct computer, arranges for shipment of the equipment to one of the IRS equipment depots, and updates the IRS's asset inventory system. We found substantial recordkeeping problems, and we estimated that IRS separation records concerning the recovery of laptop computers were inaccurate for more than 850 (21 percent) of the more than 4,100 employee separations in FY 2014.

[24] TIGTA, Ref. No. 2016-10-038, *Access to Government Facilities and Computers Is Not Always Removed When Employees Separate* (June 2016).
[25] TIGTA, Ref. No. 2016-10-056, *Improvements in Controls Are Needed for Laptop Computers Recovered When Employees Separate* (Aug. 2016).

- ***Controls Over Contractor Laptop Computers***

  The IRS, like other Federal agencies, relies on contractor personnel[26] to accomplish a broad range of mission-critical functions. During FY 2014, more than 7,900 contractor employees terminated their relationship with the IRS because of the expiration of contracts or for other reasons, such as entering into other employment arrangements. Many of these contractor employees were in positions in which they were issued laptop computers, which may allow them access to IRS networks and sensitive taxpayer data. Laptop computers and other equipment must be recovered from separating contractor employees prior to the effective date of separation to prevent the loss of the equipment and sensitive data.

  Contracting officer representatives manage all technical aspects of a particular contract. These contract administration officials are responsible for assuring that all security aspects (physical, personnel, and data) of the contract are properly addressed and work with other IRS officials to identify and provide equipment and computer access needs. When a contractor employee separates from the IRS, the contract administration official is responsible for the return of any assigned laptop computers prior to separation.[27]

  During our review, contract administration documentation used to account for the issuance of laptop computers to contractor employees and the return of laptop computers from contractor employees was often incomplete, inaccurate, or not provided for review.[28] Furthermore, separately maintained computer inventory records were not always accurate or did not always match contract administration documentation. Specifically, contract administration documentation and computer inventory records only matched for 12 of 40 laptop computers associated with contractor employees we sampled. For the remaining laptop computers, contract administration documentation and computer inventory records differed. For example, IRS officials provided contract administration documentation showing that three laptop computers were issued to contractor employees in our sample, but computer inventory records did not show laptop computers were ever assigned to the contractor employees. Without better recordkeeping practices, the IRS is vulnerable to the loss of laptop computers, which may contain taxpayer information.

  These errors were caused by several factors. For example, we could not identify any guidance for the audit time period regarding how contract administration officials should document the issuance of laptop computers to contractor employees. Contract

[26] According to IRS management, the IRS employed approximately 14,800 contractor employees as of July 2015.
[27] IRS officials stated that when the contract administration official is not located in the same city as the contractor, another IRS official will arrange for the return of the laptop computer from the contractor and its pick-up by the IT organization.
[28] TIGTA, Ref. No. 2016-10-057, *Improved Controls Are Needed to Account for the Issuance and Return of Contractor Employee Laptop Computers* (Aug. 2016).

administration officials also did not always use current forms requiring barcodes to document the return of laptop computers. After the time period of our sample, the IRS developed a training package that included requirements for contract administration officials to maintain a log of IRS-issued equipment in the contract file, including a description of the equipment issued, the barcode, the serial number, the date issued, and the date returned.

- ***Physical Access to Computer Rooms and Tape Libraries***

  HSPD-12 mandated the establishment of a governmentwide standard for identity credentials to improve physical security in federally controlled facilities. HSPD-12 required all government employees and contractors be issued a new identity card based on Federal Information Processing Standard 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.[29] HSPD-12 explicitly requires the use of HSPD-12 PIV cards to gain physical access to federally controlled facilities and logical access to federally controlled information systems.

  The IRS uses two main data centers, also known as its Enterprise Computing Centers. Both Enterprise Computing Centers are Facility Security Level 5 areas as defined by the Interagency Security Committee and the DHS.[30] Facility Security Level 5 is the highest level that can be assigned to a government facility based on criticality and both its attractiveness as a target and the consequences of an event. The IRS uses the Enterprise-Wide Physical Access Control System to control access into and within the facility. Card readers are placed at doors for user's to swipe their HSPD-12 PIV cards and, for some areas, enter a personal identification number for two-factor authentication.

  During our review, we determined that computer room and tape library perimeter security needs to be updated.[31] Two-factor authentication was not being used for one of the data center locations. Access verification was not being performed after changes to or implementation of the door groups in the Enterprise-Wide Physical Access Control System that controls access to and within the IRS facilities. As a result, general access was allowed into the restricted computer rooms. Surveillance equipment was either outdated or did not exist, which limited the IRS's ability to monitor its critical infrastructure.

  We also found the continued use of temporary badges as a form of identification. This presents security concerns because these badges do not provide specific information such

[29] NIST, FIPS Pub. 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (Aug. 20134). Note: FIPS 201-2 superseded FIPS 201 (FIPS 201-1).
[30] Interagency Security Committee, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, 1st edition (Aug. 2013).
[31] TIGTA, Ref. No. 2016-20-093, *Updating Computer Room and Tape Library Physical Access Controls at the Computing Centers Will Significantly Improve Security* (Sept. 2016).

as name and employee status to authenticate the individual. Currently, the IRS uses a manual and visual process to identify visitors, increasing the risk that an unauthorized individual could gain access. Authenticating individuals by their HSPD-12 PIV card that contains the necessary data for the cardholder to be granted access to Federal facilities reduces that risk because the PIV card authenticates the individual entering the room. Lastly, we determined that automating access monitoring to the computer rooms and tape libraries will increase efficiency, oversight, and security. Currently, a manual process performed by one person is used to authorize and remove access for over 500 individuals.

Backup and restoration of data

The former IRS Chief Technology Officer requested that we review the Tier II backup environment, specifically related to an incident of lost backup data on the Work Request Management System. The Work Request Management System tracks and controls information technology work requests from submission through completion and maintains the status and assignment information. Due to lost backup data, the Work Request Management System could not be restored immediately when the database was inadvertently deleted.

The Tier II environment consists of nonmainframe servers. These servers run various operating systems and store important data including e-mail, personal and shared files, and taxpayer information. Inadequate backup and restoration of Tier II environment data could result in the loss of taxpayer or management information and unrecoverable data following a disaster. We found that the IRS is not effectively managing its Tier II environment backup and restoration process.[32] For example, 28 (35 percent) of 81 Tier II backup software applications are at their end of life, which could result in a lack of critical vendor security and maintenance support. Likewise, 104 (100 percent) of the hardware equipment used in the Tier II backup environment is beyond its useful life and has critical deficiencies that should be addressed. We also found that the dashboard created to report on the completion status of backups is not sufficient.

Furthermore, the IRS did not properly analyze, document, or take effective corrective actions in response to the database incident. As a result, management still does not have information to detect when a required backup is not created. Similarly, management does not routinely test restores of backups to ensure the integrity and reliability of the data. Effective management of the Tier II backup and restoration environment is crucial to ensure that information technology fully supports business operations by efficiently providing services to taxpayers.

SharePoint controls

SharePoint® is a Microsoft commercial off-the-shelf product that supports collaboration, information dissemination through web portals, document management, records management,

[32] TIGTA, Ref. No. 2016-20-002, *Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement* (Oct. 2015).

and application service delivery platforms. IRS business units rely on the SharePoint platform primarily for collaboration, document management, records management, and enterprise content management. The Enterprise Operations SharePoint Program Management Office provides operational oversight and governance of the SharePoint platform, including infrastructure, support, and management. In addition, the SharePoint Program Management Office establishes management, technical, and operational standards; reviews policy impact on the use of SharePoint; recommends training; and supports configuration and customization of site solutions deployed on the SharePoint platform. SharePoint site collection owners within IRS business units operate, manage, and maintain their SharePoint sites and are responsible for day-to-day site management, support, and compliance for user access, user permissions, content management, and audit trail management.

As part of our review, we reported that improved risk management across the IRS SharePoint environment is needed to ensure that adequate operational and security controls are in place and functioning as intended to protect sensitive SharePoint sites and data.[33] Operational controls are needed to ensure that SharePoint sites containing sensitive data are identified and have an approved Privacy and Civil Liberties Impact Assessment. Security controls are needed to ensure that a security assessment of the SharePoint product, sites, and data is completed; SharePoint site collection audit trails are enabled; quarterly reviews of users' accesses are performed; users' accounts and permissions are efficiently managed; security and content management policies are consistently enforced; and the Information Technology Contingency Plan and Business Impact Analysis are finalized.

Systems Development Supporting the Affordable Care Act and Other Tax Law Changes

Along with 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)) were enacted.[34] 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.

[33] TIGTA, Ref. No. 2016-20-075, *Information Technology: SharePoint Controls Need Improvement to Mitigate Risks and to Ensure That Possible Duplicate Costs Are Avoided* (Sept. 2016).
[34] 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 Internal Revenue Code and 42 U.S.C.), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.

While the U.S. Department of Health and Human Services has the lead role in all health insurance and health care policy provisions of the ACA legislation, the IRS administers the law's 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 did not exist within the tax administration system. These provisions provide incentives and tax breaks to individuals and small businesses to offset health care expenses. They also impose penalties, administered through the tax code, for individuals and businesses that do not obtain health coverage for themselves or their employees. Other provisions raise revenue to help pay for the overall cost of health insurance reform. 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.

The ACA Compliance Validation System

The ACA Program Management Office is developing numerous releases of ACA software to implement ACA provisions. The ACA systems developed through these releases provide functionality to support the Exchange's eligibility and enrollment process, processing of Premium Tax Credit claims, and storing of Exchange data. Under ACA Release 6.1, the ACA Program Management Office developed Release 1.0 of the ACA Compliance Validation System in support of post-filing compliance to perform the following:

- Identify individual returns that have failed to reconcile for receiving an advance payment of the Premium Tax Credit.
- Provide a calculation service to calculate the shared responsibility payment.

We found that the IRS successfully tested the functionality and security of the ACA Compliance Validation System prior to placing the system into production.[35] In addition, the system was placed into production on September 10, 2015, prior to the mandatory due date of September 27, 2015. By using lessons learned from previous system development projects, the project team was able to build the system and complete performance, integration, and release-level testing on schedule. Following release-level testing, the IRS properly assessed the security of the ACA Compliance Validation System.

The Cybersecurity function provided all required documents and security testing results, including the identified security risks for the authorizing official to make an informed decision authorizing the system to operate. We did find some examples of inaccurate security control descriptions in 29 (14.4 percent) of 201 controls in the ACA System Security Plan, but the errors did not cause any applicable security controls to be excluded from testing and did not affect the

[35] TIGTA, Ref. No. 2016-23-040, *Affordable Care Act Compliance Validation System: Security and Testing Risks* (May 2016).

authorization decision to place the system into operation. During the course of our fieldwork, the Cybersecurity function corrected the errors and updated the ACA System Security Plan.

The ACA Case Management System

The IRS currently maintains approximately 90 separate case management systems. Case management is the process that addresses the resolution of tax administration issues through the management of case creation, execution, maintenance, and closure. ACA Release 7.1 includes a new ACA system called the ACA Case Management-Case Management Release 1.0 (referred to as the ACA Case Management System) and focuses on the post-filing compliance activities regarding an employer's shared responsibilities for providing health care coverage.

On January 13, 2015, approximately one month after the ACA Case Management System began its project initiation phase, the IRS Commissioner approved the approach for creating an Enterprise Case Management System that can be applied throughout the IRS. The IRS also established the Enterprise Case Management Program Management Office. On June 3, 2015, IRS leadership approved the inclusion of the ACA Case Management System into the Enterprise Case Management Program.

In July 2015, a team was formed to identify overlapping requirements and capabilities between the ACA Case Management and Enterprise Case Management Systems. The team used a rapid delivery architecture approach to mitigate the concern that ACA Case Management System development would get too far ahead of the Enterprise Case Management System's development. We found only 35 (45 percent) of the 77 ACA Case Management System capabilities were mapped to Enterprise Case Management System capabilities.[36] ACA Case Management project officials explained that the remaining 42 (55 percent) capabilities are unique to the ACA Case Management System.

During the audit reporting phase of this review, the IRS decided to close the ACA Case Management project. The IRS established a Digital Subcommittee to focus on strategies for creating and prioritizing digital solutions for taxpayer services. The Digital Subcommittee conducted a risk assessment to find savings by delaying or stopping work on certain information technology projects in order to free up resources. The former Chief Technology Officer and Deputy CIO directed that, effective immediately, the IT organization was to "stop work, descope efforts, and begin an orderly and rapid shutdown" on the specified projects. As a result, on June 7, 2016, the IT ACA Governance Board approved a request to close the ACA Case Management System. The functional components and documentation will be transferred to the Enterprise Case Management Program Management Office.

[36] TIGTA, Ref. No. 2016-23-066, *The Affordable Care Act Case Management System Release 1.0* (Aug. 2016).

Foreign Account Tax Compliance Act (FATCA)[37] Program Withholding and Refund Release 2.0 Project

The FATCA Program is an important development in the IRS's efforts to improve tax compliance involving foreign financial assets and offshore accounts. The FATCA legislation was enacted in March 2010 by Congress as part of the Hiring Incentives to Restore Employment Act[38] to:

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

The primary objective of the FATCA is to improve disclosure by foreign financial institutions of U.S. account holders. FATCA withholding provisions, which took effect on July 1, 2014, impose a 30 percent withholding tax on certain types of U.S. sourced payments. To comply with the FATCA legislative requirements, foreign financial institutions are required to provide identifying information on U.S. accounts maintained by the institution. In January 2014, a foreign financial institution automated registration application system was implemented to address the FATCA regulations.

Since the implementation of the Foreign Financial Institution Registration System, the IRS has implemented the International Data Exchange Service to facilitate secure electronic submission, receipt, and exchange of FATCA data among financial institutions from many countries. In addition, the IRS has developed the International Compliance Management Model database to process FATCA data. FATCA Release 3.0 includes the work to develop and deploy Withholding & Refund Release 2.0 functionality that will use the data that were prepared in the prior FATCA Release 2.0 (via Withholding & Refund Release 1.0) to conduct automated matching and make a credit determination as to whether certain refund claims are valid. Successful implementation of FATCA Release 3.0 should significantly improve taxpayer compliance internationally and enhance IRS tax administration.

We found that the IRS made improvements, based on prior TIGTA reviews, to strengthen systems development requirements management controls for FATCA projects.[39] However, in an attempt to meet the project schedule and manage resources, Withholding & Refund Release 2.0 went forward despite critical data quality problems that resulted in unplanned work and a

[37] Pub. L. No. 111-147, Subtitle A, 124 Stat 71, *96-116 (2010) (codified in scattered sections of 26 U.S.C.).
[38] Pub. L. No. 111-147, 124 Stat. 71 (2010).
[39] TIGTA, Ref. No. 2016-20-077, *Foreign Account Tax Compliance Act Program Withholding and Refund Release 2.0 Project Development and Testing* (Aug. 2016).

four-month implementation delay. In addition, improvements are needed to ensure that high-risk issues are given priority.

While the IRS implemented Withholding & Refund Release 2.0 on the revised February 2016 deployment date and there is agreement that the system was built to requirements, the IRS spent $15 million dollars delivering functionality that has not provided the intended business results. The IRS first identified data matching issues in May 2015. Although the initial data matching issues were resolved, the IRS identified new data matching issues as recently as February 2016. The IRS does not have a time frame for when the latest data matching issues will be resolved and automated functionality will provide all of the expected business results.

Information Systems to Combat Identity Theft and Tax Refund Fraud

Identity thieves access electronic systems unlawfully and steal Personally Identifiable Information, such as names, Social Security Numbers, or other identifying information from limitless sources, to commit fraud or other crimes. One such crime, known as identity theft tax refund fraud, occurs when someone uses a legitimate taxpayer's identity to file a fraudulent tax return and claim a refund. The identity thief will use a stolen Social Security Number to file a false tax return and attempt to get a fraudulent refund early in the filing season, before the victim sends his or her tax return to the IRS to be processed. Identity theft continues to be a serious and evolving issue that has a significant impact on tax administration. During Processing Year 2015, the IRS reported that it identified 1.4 million fraudulent identity theft tax returns[40] and prevented the issuance of approximately $8.7 billion in refunds. The IRS uses the following systems during tax return processing to identify fraudulent tax returns involving identity theft:

- **Electronic Fraud Detection System (EFDS)** – During tax return processing, paper and electronically filed tax returns are analyzed through various EFDS data model formulas. The data models identify suspicious paper and electronically filed tax returns based on specific characteristics of the tax return. An associated score is then computed for each tax return. The higher the score, the greater the likelihood the tax return is fraudulent.
- **Dependent Database** – The Dependent Database is a rules-based system[41] that incorporates information from many sources that include the Department of Health and Human Services, the Social Security Administration, and the IRS. The IRS implemented identity theft rules within the Dependent Database system in Processing Year 2012.

[40] Identity theft for the purpose of tax fraud occurs when an individual uses another person's name and Taxpayer Identification Number (generally a Social Security Number) to file a fraudulent tax return to obtain a fraudulent tax refund.
[41] Tax returns are sent through the Dependent Database as they are processed for possible selection and Taxpayer Protection Program processing based on the application of a set of business rules using information from both internal and external sources.

- **Return Review Program (RRP)** – The RRP uses predictive analytics, models (*i.e.*, filters, clustering), a scoring system, business rules, and selection groups to identify suspected identity theft and fraudulent tax returns. In February 2009, the IRS began development of the RRP to replace the EFDS. The IRS determined that numerous inefficiencies and operational challenges render the EFDS too risky to maintain, upgrade, or operate long term. The IRS believes that the RRP provides new and improved capabilities that bring its fraud detection and prevention into the next generation.

The RRP is being developed in phases and, as such, the IRS will continue to use the EFDS, the Dependent Database, and the RRP simultaneously to detect fraudulent tax returns involving identity theft. The IRS does not have an estimated date for full implementation of the RRP.

RRP identity theft detection

In July 2015, we reported that, during a pilot test from April 2014 through November 2014, the RRP models identified additional tax returns as potential identity thefts that were not detected by the EFDS and the Dependent Database.[42] For example, during the pilot, the RRP identified 51,946 tax returns as potential identity theft. The IRS confirmed that 41,311[43] of those tax returns were in fact identity theft, of which 10,348 (25 percent) were not detected by either the EFDS or the Dependent Database. The refunds that were prevented for these 10,348 tax returns totaled $43 million. Based on the positive results of this pilot, the IRS expanded the use of the RRP in the detection of identity theft returns for Processing Year 2015.

During our review of the RRP in December 2015, we found that the RRP pilot successfully identified tax returns involving identity theft that were not identified by other fraud detection systems.[44] However, our analysis also showed that 54,175 confirmed identity theft tax returns with refunds totaling more than $313 million were identified by other existing fraud detection systems but were not selected by the RRP. As the IRS continues to develop the RRP, it needs to ensure that the RRP will detect identity theft cases being identified by existing systems as well as other identity theft cases.

Beginning with the 2015 Filing Season, in an effort to further combat undetected identity theft, the IRS implemented a new process to limit the number of deposits (three) to a single bank account. Our review of this process identified programming errors that resulted in 5,516 direct deposits totaling almost $13.5 million that were not properly converted to paper refund checks. The IRS addressed two of the programming errors and agreed to correct the remaining error.

[42] TIGTA, Ref. No. 2015-20-060, *The Return Review Program Enhances the Identification of Fraud; However, System Security Needs Improvement* (July 2015).
[43] The remaining 10,635 tax returns identified either were determined to not be identity theft or were still being evaluated.
[44] TIGTA, Ref. No. 2016-40-008, *Continued Refinement of the Return Review Program Identity Theft Detection Models Is Needed to Increase Detection* (Sept. 2016).

As part of our filing season readiness effort, we reviewed the 23 new data elements added to the RRP in FY 2016.[45] Only three of these elements were used systemically to filter returns and help identify potential identity theft tax refund fraud during the 2016 Filing Season. As of March 25, 2016, the IRS has identified approximately $4.1 billion in suspected identity theft tax refund fraud, of which $72 million (21,000 tax returns) was attributable to these three new data elements used systemically in the RRP. Additionally, the IRS attributed the prevention of 24,000 taxpayer returns from being incorrectly selected as potential identity theft tax refund fraud returns to one of the three data elements. For the remaining 20 new data elements, there was insufficient historical data to create business rules that would enable systemic use during the 2016 Filing Season. The Applications Development function intends to determine their potential use in future filing seasons.

The IRS told us that the data elements should remain confidential and be kept a secret from the public since making this information public would inform identity thieves of its specific plans and strategy. However, our search of the IRS's public website identified schemas that included several of the new data elements. The IRS was notified of this finding and responded by removing the schemas containing the data elements.

Ensuring that refunds claimed on potentially fraudulent tax returns are not erroneously released

The IRS's Return Integrity and Compliance Services organization is responsible for identifying, evaluating, and preventing the issuance of improper refunds. Within this organization is the Integrity and Verification Operations function, whose mission includes support of the IRS's prerefund fraud detection and prevention efforts (*i.e.*, detection during tax return processing prior to a refund being issued). The Integrity and Verification Operations function protects revenue by identifying potentially fraudulent tax returns and verifying the accuracy of reported income and withholding information. For example, once a potentially fraudulent tax return is identified, the Integrity and Verification Operations staff screens the tax return to determine whether verification of reported income and withholding is warranted. If verification is warranted, the return is sent to a tax examiner who performs this verification. The Integrity and Verification Operations function receives its inventory from the Dependent Database, the EFDS, and the External Leads Program.

We found that, due to a programming error, over $27 million of refunds were erroneously issued for 13,043 Tax Year 2013 tax returns.[46] The programming error is overriding the IRS's two-week processing delay on some refund tax returns that are identified by the IRS as potentially fraudulent. These are tax returns that the IRS Examination function also identified as claiming a questionable tax credit. The portion of the refund that is not reviewed by the

[45] TIGTA, Ref. No. 2016-20-062, *Filing Season 2016: Implementation of New Data Elements* (Sept. 2016).
[46] TIGTA, Ref. No. 2016-40-006, *Improvements Are Needed to Better Ensure That Refunds Claimed on Potentially Fraudulent Tax Returns Are Not Erroneously Released* (Nov. 2015).

Examination function is erroneously issued before the IRS can complete its verification of income and withholding.

We also found ineffective monitoring of potentially fraudulent tax returns is resulting in the erroneous release of refunds before the required verification. We identified 3,910 Tax Year 2013 tax returns selected for verification with no indication that tax examiners verified the returns. The IRS issued refunds totaling over $19 million for these tax returns. The IRS did not ensure that tax examiners timely completed their verification work. Name mismatches in IRS systems prevented refund holds from posting to tax accounts. Refund holds were either not set or not functioning as intended. Although the IRS agreed with our findings, it did state that software changes are subject to budgetary constraints, limited resources, and competing priorities.

Information Technology Contract Administration

The Federal Acquisition Regulation sets forth acquisition principles, policies, and procedures that govern acquisitions for Federal agencies. This regulation governs contracts, orders, and agreements entered into by the IRS. The IRS's Office of Procurement, within the Deputy Commissioner for Operations Support organization, is responsible for purchasing equipment, services, and supplies for the IRS. The Office of Procurement is made up of six functions, one of which is the Office of Information Technology Acquisition. This office is responsible for planning, negotiating, executing, and managing the procurement of information technology products and services. As such, this office provides technical and administrative support throughout all stages of the acquisition life cycle. We reviewed a sample of information technology contracts and also reviewed the IRS's enterprise e-mail acquisition.

Information technology contract administration controls

In our review of information technology contract administration controls,[47] we found that risks for information technology contracts awarded between October 2008 and May 2014 were not adequately mitigated to protect the IRS's systems and sensitive data and to ensure that the IRS receives services and products that meet contractual requirements. We analyzed 14 information technology contract files and supporting documentation. The estimated value of these contracts was $81.3 million.

We identified two key areas in which overall improvements are needed to address the control weaknesses identified during our review. First, clarification is needed to ensure consistent and reliable implementation of reviews required to mitigate security risks through the information technology contract administration process. Second, the overall operational controls for contract administration and fraud controls for individual information technology contracts should be carefully reexamined to ensure that post-award contract file reviews are reliable. Our review

[47] TIGTA, Ref. No. 2016-20-035, *Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks* (July 2016).

identified control weaknesses with: 1) security compliance reviews, 2) contract file documentation, 3) contractor exclusion reviews, 4) contract administration plans, and 5) contracting officer representative appointment letters.

IRS enterprise e-mail acquisition

On August 24, 2012, the OMB released a directive[48] that Federal agencies will manage both permanent and temporary e-mail records in an accessible electronic format by December 2016. The memorandum states that e-mail records must be retained in an appropriate electronic system that supports records management and litigation requirements (which may include preservation-in-place models), including the capability to identify, retrieve, and retain records for as long as they are needed.

In August 2014, the IRS prepared a draft E-Mail As a Service Request for Quote. This document stated "In compliance with the Federal Government Cloud First policy, the IRS seeks an experienced industry partner to provide a secure cloud-based E-Mail As a Service solution to replace IRS-managed e-mail servers, software, and related infrastructure components." It defined E-Mail As a Service to be a hybrid Microsoft Office 365 Online Plan 2 e-mail solution with the majority of IRS e-mail users migrating to the Microsoft Office 365 cloud and the remaining users residing in an on-premises IRS-managed Microsoft Exchange environment. It also stated that the IRS strategy is to replace the current IRS-owned and -managed enterprise e-mail system with a cloud-based service environment that is compatible with IRS and industry managed-service engineering life cycle principles. Lastly, it stated that the IRS is challenged by an e-mail infrastructure that consists of hardware assets that may be less than optimally utilized. There is currently no archive capability associated with the enterprise e-mail environment. The existing system hardware is approaching manufacturer end of support and is experiencing numerous failures resulting in a significantly increased workload on enterprise e-mail support staff.

During our review, IT organization executives told us that they made a management decision to consider the enterprise e-mail project an upgrade to existing software and not a new development project or program.[49] Therefore, the IT organization chose not to use the draft Request for Quote developed in August 2014 and not to follow the Internal Revenue Manual Enterprise Life Cycle Commercial Off-the-Shelf Path or the Managed Service Path to acquire, develop, and deploy the new enterprise e-mail system. The IRS violated the Federal Acquisition Regulation by not using full and open competition in its acquisition of Microsoft Office 365 Pro Plus and Exchange Online monthly subscriptions. Also, the software to be used via the purchased subscriptions ($12 million for subscriptions over a two-year period between June 2014 and June 2016) was never deployed. The IRS may have also violated the *bona fide* needs rule when it purchased the

[48] OMB, OMB M-12-18, *Managing Government Records Directive (*Aug. 2012).
[49] TIGTA, Ref. No. 2016-20-080, *Review of the Enterprise E-mail System Acquisition* (Sept. 2016).

subscriptions using Fiscal Years 2014 and 2015 appropriations and did not deploy the software subscriptions in those years.

Achieving Program Efficiency

As GAO reported in March 2016, the use of information technology has created many benefits for agencies such as the IRS in achieving their mission and providing information and services to the public. Agencies have become dependent on information technology, relying on systems to carry out their operations of processing, maintaining, and reporting large volumes of sensitive data, such as personal data.[50]

Integrated Production Model (IPM)

The IRS implemented the IPM in February 2007. The IPM is a centralized analytical data store that provides a single point of access to core taxpayer data (such as taxpayer accounts and tax returns) and other specific data used by a wide range of IRS business applications to support case identification, selection, prioritization, delivery, and reporting. The IPM system was designed as a replacement for two legacy systems—the Enterprise Data Warehouse Business Filers Model and the Enterprise Data Warehouse Individual Filers Model. These legacy systems previously processed data over the course of several hours per query and required users to run queries in both systems separately in order to collect the data required to meet business needs. The IPM system was designed to benefit the IRS by providing multiple IRS business organizations access to current and historical taxpayer data.

We found that the IPM system is meeting IRS business needs and has improved the efficiency of data access via a singular data repository that has taken over the processing load of two separate database systems.[51] However, key access controls were not documented, and we were unable to definitively verify that the IPM pulls data from only designated source systems. We also found that 14 (77 percent) of 18 IPM source systems reviewed perform no validation of data for accuracy, completeness, and reliability. The IPM database acts as a data repository, and there are no controls to validate received data. Without documentation and adequate management of access controls and without the ability to review system audit logs to verify unique system access, the IRS cannot be sure which systems the IPM pulls data from.

[50] GAO, GAO-16-398, *Information Security: IRS Needs to Further Improve Controls Over Financial and Taxpayer Data* (Mar. 2016).
[51] TIGTA, Ref. No. 2016-20-058, *The Integrated Production Model Increases Data Access Efficiency; However, Access Controls and Data Validation Could Be Improved* (July 2016).

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the progress of the IRS's Information Technology Program, including security, improving tax systems and online services, and operations for FY 2016.[1] This review was required by the IRS Restructuring and Reform Act of 1998.[2] 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 the 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 audit reports issued during FY 2016. During the review, we analyzed and prepared an overall assessment of the security and privacy issues.
- B. Identified and summarized relevant external oversight assessments dealing with security and privacy (*e.g.*, assessments performed by the GAO).

III. Assessed the 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 audit reports issued during FY 2016. During the review, we analyzed and prepared an overall assessment of the systems development issues.
- B. Identified and summarized relevant external oversight assessments dealing with modernization and systems development.

IV. Assessed the 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 audit reports issued during FY 2016. During the review, we analyzed and prepared an overall assessment of systems operations issues.
- B. Identified and summarized relevant external oversight assessments dealing with systems operations.

[1] See Appendix VI for a glossary of terms.
[2] 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)
Myron Gulley, Acting Director
Gwen McGowan, Director
Kent Sagara, Director
Jena Whitley, Audit Manager
Michael Curtis, Lead Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise Services
Associate Chief Information Officer, Strategy and Planning
Associate Chief Information Officer, User and Network Services
Director, Strategic Supplier Management
Director, Office of Audit Coordination

Appendix IV

List of Treasury Inspector General for Tax Administration Reports Reviewed

Number	Report Reference Number	Audit Report Title	Report Issuance Date
1	2016-20-062	*Filing Season 2016: Implementation of New Data Elements*	September 21, 2016
2	2016-20-092	*Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016*	September 28, 2016
3	2016-40-007	*Improved Tax Return Filing and Tax Account Authentication Processes and Procedures Are Needed*	November 19, 2015
4	2016-40-037	*The Internal Revenue Service Did Not Identify and Assist All Individuals Potentially Affected by the Get Transcript Application Data Breach*	May 16, 2016
5	2016-20-082	*Improvements Are Needed to Strengthen Electronic Authentication Process Controls*	September 7, 2016
6	2016-10-038	*Access to Government Facilities and Computers Is Not Always Removed When Employees Separate*	June 30, 2016
7	2016-10-056	*Improvements in Controls Are Needed for Laptop Computers Recovered When Employees Separate*	August 10, 2016
8	2016-20-093	*Updating Computer Room and Tape Library Physical Access Controls at the Computing Centers Will Significantly Improve Security*	September 29, 2016
9	2016-20-002	*Measurable Agreements on Security Controls Are Needed to Support the Enterprise Storage Services Solution*	October 30, 2015
10	2016-20-019	*Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement*	February 11, 2016

Number	Report Reference Number	Audit Report Title	Report Issuance Date
11	2016-23-040	*Affordable Care Act Compliance Validation System: Security and Testing Risks*	May 16, 2016
12	2016-23-066	*The Affordable Care Act Case Management System Release 1.0*	August 30, 2016
13	2016-20-077	*Foreign Account Tax Compliance Act Program Withholding and Refund Release 2.0 Project Development and Testing*	August 31, 2016
14	2016-40-008	*Continued Refinement of the Return Review Program Identity Theft Detection Models Is Needed to Increase Detection*	December 11, 2015
15	2016-40-006	*Improvements Are Needed to Better Ensure That Refunds Claimed on Potentially Fraudulent Tax Returns Are Not Erroneously Released*	November 12, 2015
16	2016-20-035	*Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks*	August 2, 2016
17	2016-10-057	*Improved Controls Are Needed to Account for the Issuance and Return of Contractor Employee Laptop Computers*	August 25, 2016
18	2016-20-080	*Review of the Enterprise E-Mail System Acquisition*	September 30, 2016
19	2016-20-058	*The Integrated Production Model increases Data Security; However, Access Controls and Data Validation Could Be Improved*	July 29, 2016
20	2016-20-075	*Information Technology: SharePoint Controls Need Improvement to Mitigate Risks and to Ensure That Possible Duplicate Costs Are Avoided*	September 15, 2016

Appendix V

Outcome Measures Reported in Fiscal Year 2016

Audit Report Title	Type of Measure	Amount
Review of the Enterprise E-Mail System Acquisition (Ref. No. 2016-20-080)	Inefficient Use of Resources	Potential; $12,091,320.
Continued Refinement of the Return Review Program Identity Theft Detection Models Is Needed to Increase Detection (Ref. No. 2016-40-008)	Revenue Protection	Potential; $13,473,966 from 5,616 requested direct deposits not converted to paper refund checks as required.
Improvements Are Needed to Better Ensure That Refunds Claimed on Potentially Fraudulent Tax Returns Are Not Erroneously Released (Ref. No. 2016-40-006)	Revenue Protection	Potential; $135,456,560 in erroneous refunds over five years for 65,215 tax refunds for which the IRS's two-week tax return resequencing marker is overridden by a marker that the Examination functions used to select tax returns for review of questionable refund credits.
Improved Controls Are Needed to Account for the Issuance and Return of Contractor Employee Laptop Computers (Ref. No. 2016-10-057)	Reliability of Information	Potential; 1,078 contractor employees[1] with inaccurate or unreliable clearance records.
Access to Government Facilities and Computers Is Not Always Removed When Employees Separate (Ref. No. 2016-10-038)	Reliability of Information	Potential; 2,060 employees[2] with inaccurate or unreliable clearance records.
Improvements in Controls Are Needed for Laptop Computers Recovered When Employees Separate (Ref. No. 2016-10-056)	Reliability of Information	Potential; 882 employees[3] with inaccurate clearance records or IT organization office inventory records.

[1] The point estimate projection is based on a two-sided 90 percent confidence interval. We are 90 percent confident that the point estimate is between 912 and 1,244.
[2] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 1,618 and 2,503.
[3] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 613 and 1,150.

Appendix VI

Glossary of Terms

Term	Definition
Accountability	Means 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. The ACA refers to the final amended version of the law.
Applications Development Function	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.
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
Audit Trail	A record showing who has accessed an information technology system and what operations the user has performed during a given period.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Build	A version of a software program.
Chief Technology Officer/ Chief Information 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.
Cloud Computing	A model for enabling on-demand network access to a shared pool of configurable IT capabilities and resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software As a Service, Cloud Platform As a Service, and Cloud Infrastructure As a Service); and four models for enterprise access (private cloud, community cloud, public cloud, and hybrid cloud).

Term	Definition
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Contractor	An organization external to the IRS that supplies goods and services according to a formal contract and task order. A contractor is a type of provider.
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.
Encrypted	Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.
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 transparent and competitive insurance exchange in which individuals and small businesses can buy affordable and qualified health benefit plans. They offer a choice of health plans that meet certain benefits and cost standards.
Federal Information Security Modernization Act of 2014	Amendment to The Federal Information Security Management Act of 2002 that allows for further reform to Federal information security, signed 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 OMB (Title III, P.L. 107-347).
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
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.
Hackers	Unauthorized users who attempt to or gain access to an information system.

Term	Definition
Hardware	The physical parts of a computer and related devices; it includes motherboards, hard drives, monitors, keyboards, mice, printers, and scanners.
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.
Integrated Enterprise Portal	The IRS Internet portal that allows registered individuals to access selected tax data and other sensitive applications.
Internal Revenue Manual	The IRS's primary source of instructions to its employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Mainframe	A powerful, multiuser computer capable of supporting many hundreds of thousands of users simultaneously.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Multifactor Authentication	A characteristic of an authentication system or a token that uses two or more authentication factors to achieve authentication. The three types of authentication factors are something you know, something you have, and something you are.
National Institute of Standards and Technology	The Information Technology Laboratory at the NIST 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 NIST is part of the U.S. Department of Commerce.
Operating System	The software that serves as the user interface and communicates with computer hardware to allocate memory, process tasks, and access disks and peripherals.
Patches	Updates to an operating system, application, or other software issued specifically to correct particular problems with the software.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, *etc*., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, *etc*.

Term	Definition
Personal Identity Verification Card	The process of creating and using a governmentwide secure and reliable form of identification for Federal employees and contractors in support of HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*.
Premium Tax Credit	A refundable tax credit to help taxpayers and families afford health insurance coverage purchased through an Exchange.
Privileges	Rights granted to an individual, a program, or a process.
Processing Year	The calendar year in which the tax return or document is processed by the IRS.
Release	A specific edition of software.
Remote Access	Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (*e.g.*, the Internet).
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.
Rules-Based System	In computer programming, rule-based systems are used as a way to store and manipulate knowledge to interpret information in a useful way. They are often used in artificial intelligence applications and research.
Server	A system capable of managing and running virtual machines. Also a process capable of accepting and running instructions from another process.
SharePoint	Microsoft SharePoint is a collection of products and software elements that includes web browser–based collaboration functions and a document management platform. SharePoint can be used to host websites that access shared workspaces, information stores, and documents.
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.
Taxpayer Protection Program	Responsible for handling potential identity theft cases that are scored by a set of models in the Dependent Database or selected through a query in the EFDS or selected by Integrity and Verification Operations tax examiners during the daily screening process.

Term	Definition
Tier II Environment	The IRS's Tier II environment consists of nonmainframe servers. These servers run various operating systems, including versions of Microsoft Server, Linux, and UNIX. The servers may also operate as database, web, e-mail, and file servers, and provide a host of other important functions supporting the IRS network infrastructure.
Two-Factor Authentication	A method of confirming a user's claimed identity by utilizing a combination of two different components. These components may be something that the user knows, something that the user possesses, or something that is inseparable from the user.
Web Portal	A point of entry to a network system that includes a search engine or a collection of links to other sites arranged especially by topic. It provides the infrastructure that allows users (including IRS employees and taxpayers) to have web-based access to IRS information.
Work Request Management System	Used by the IRS to track and control information technology work requests from submission through completion. It maintains the status and assignment information. Work Request Management System is the successor system for Work Request Tracking System and is implemented using HP Project and Portfolio Management Demand Management commercial off-the-shelf software.