TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the Internal Revenue Service Information Technology Program

September 29, 2017

Reference Number: 2017-20-089

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

Redaction Legend:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

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 29, 2017

Highlights of Reference Number: 2017-20-089 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

In Fiscal Year 2016, the IRS collected approximately $3.3 trillion in Federal tax payments, processed more than 244 million tax returns and other forms, and paid approximately $426 billion in refunds to taxpayers. In addition, the IRS employs approximately 85,000 people in more than 540 offices in every State, U.S. territory, and some U.S. embassies and consulates. 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the IRS's information technology program could result in computer operations that become compromised, disrupted, or outdated, which could adversely affect the IRS's ability to meet its mission of providing America's taxpayers with top-quality service by helping them understand and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 in an evaluation of the adequacy and security of IRS information technology as required by the IRS Restructuring and Reform Act of 1998. Our overall objective was to assess the progress of the IRS's information technology program, including security, improving tax systems and online services, and operations for Fiscal Year 2017.

WHAT TIGTA FOUND

TIGTA identified a number of areas in which the IRS can more efficiently use its limited resources and make more informed business decisions. For example, identifying the availability of surplus funds and development of plans to expeditiously spend these funds on the aged hardware inventory may have resulted in a combined total of up to $67 million in additional unspent funds being available to replace aged hardware during Fiscal Years 2013 through 2016.

Our review of IRS information technology security showed that the IRS could better protect IRS systems and data by improving disaster recovery planning and testing, general support system security controls, transfers of data to external partners, e-mail records management, and external network perimeter security.

Our reviews of IRS efforts in protection of taxpayer data determined that the Return Review Program better meets the IRS business objectives of delivering greater fraud detection at a lower False Detection Rate than the Electronic Fraud Detection System. Results from recent filing seasons support the IRS decision to retire the Electronic Fraud Detection System models. In a separate audit, we determined that the IRS was not properly protecting the data transmitted to external entities by maintaining encryption controls and other security configurations.

Our reviews of IRS efforts to improve information technology systems and expand online services determined that the IRS does not have an enterprise-wide cloud strategy, the current IRS e-mail system and policies are not in compliance with Federal electronic records requirements, and the development and deployment of key online tax functionalities were significantly delayed due to a lack of funding.

WHAT TIGTA RECOMMENDED

Because this report was an assessment report of the IRS information technology program based on TIGTA reports issued during Fiscal Year 2017, TIGTA did not make any recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 29, 2017

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 # 201720003)

This report presents the results of our assessment of the Internal Revenue Service's (IRS) information technology[1] program including security, improving tax systems and online services, and operations for Fiscal Year 2017. This review is required by the IRS Restructuring and Reform Act of 1998.[2] This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenges of *Security Over Taxpayer Data and Protection of IRS Resources*, *Improving Tax Compliance*, *Improving Tax Systems and Expanding Online Services*, and *Achieving Program Efficiencies and Cost Savings*.

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

[1] See Appendix VI for a glossary of terms.
[2] Pub. L. No. 105-206, 112 Stat. 685.

Table of Contents

Abbreviations

BDA	Big Data Analytics
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Center
CY	Calendar Year
DNS	Domain Name System
EFDS	Electronic Fraud Detection System
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
IDT	Identity Theft
IPM	Integrated Production Model
IRS	Internal Revenue Service
ISAC	Identity Theft Tax Refund Fraud Information Sharing and Analysis Center
IT	Information Technology
ITIL	Information Technology Infrastructure Library®
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RRP	Return Review Program
TIGTA	Treasury Inspector General for Tax Administration
U.S.C.	United States Code

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. TIGTA's Security and Information Technology Services unit assesses the IRS's information technology programs by evaluating cybersecurity, systems development, and information technology operations. This report provides our assessment for Fiscal Year (FY) 2017.[2] The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In FY 2016, the IRS collected approximately $3.3 trillion in Federal tax payments, processed more than 244 million tax returns and other forms, and paid approximately $426 billion in refunds to taxpayers. Further, the size and complexity of the IRS add unique operational challenges. The IRS employs approximately 85,000 people in its Washington, D.C. headquarters and more than 540 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 web for anything from ordering telephone service to conducting transactions with financial institutions using traditional online and mobile devices. According to the IRS Strategic Plan (FY 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 2016, 86 percent of individual taxpayers chose to file electronically, a 21 percent increase from 71 percent in FY 2010. Outside of filing activities, taxpayers also use the Internet to download forms, view content, and check refund status. During FY 2016, the IRS website was visited more than 501 million times and taxpayers used the "Where's My Refund?" tool nearly 300 million times, a 28 percent increase over the prior year.

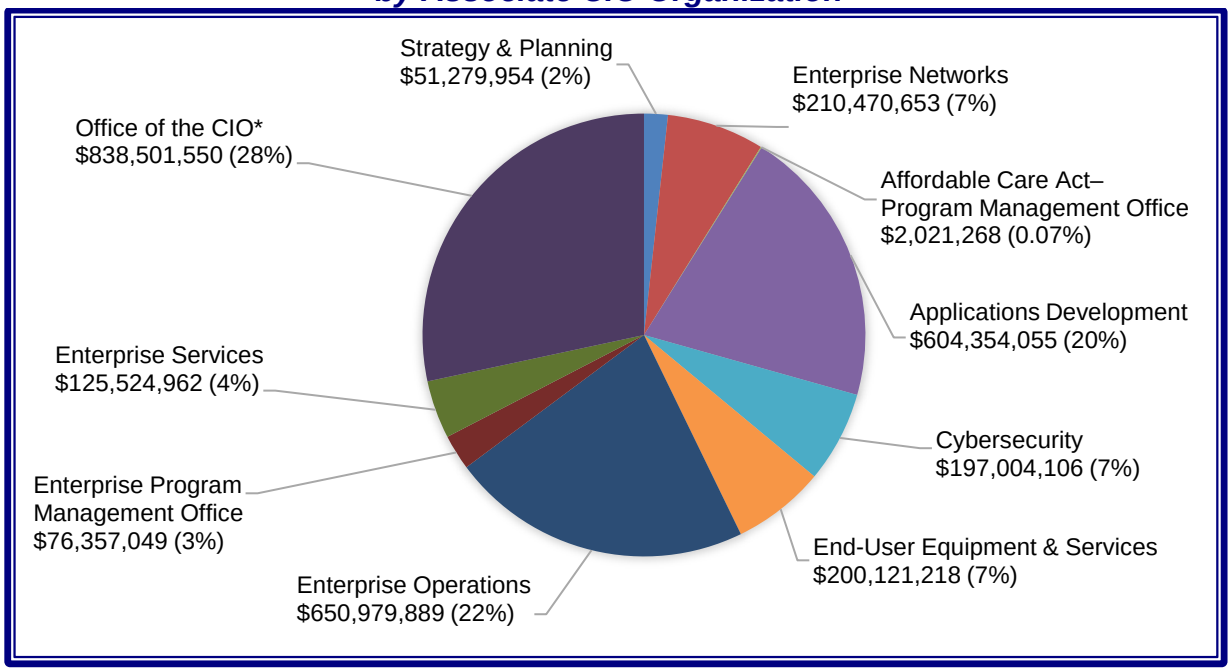
For FY 2017, the IRS was funded at $11.2 billion, thus freezing the IRS's budget at FY 2016 levels. The budget once again included $290 million for improvements in customer service, the identification and prevention of refund fraud and identity theft, and cybersecurity to safeguard taxpayer data. IRS appropriations remain about 7 percent below FY 2011 levels. As the

[1] Pub. L. No. 105-206, 112 Stat. 685.
[2] See Appendix VI for a glossary of terms.

Government Accountability Office (GAO) reported in 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 comprises a significant portion of the IRS's budget and plays a critical role in enabling the IRS to carry out its mission and responsibilities. The IRS's FY 2017 appropriations included about $2.9 billion for information technology investments; this represents 26 percent of the total IRS budget. Figure 1 illustrates FY 2017 information technology funding by the Associate Chief Information Officer (CIO) organization.

Figure 1: IRS IT Organization FY 2017 Total Available Funding by Associate CIO Organization[4]



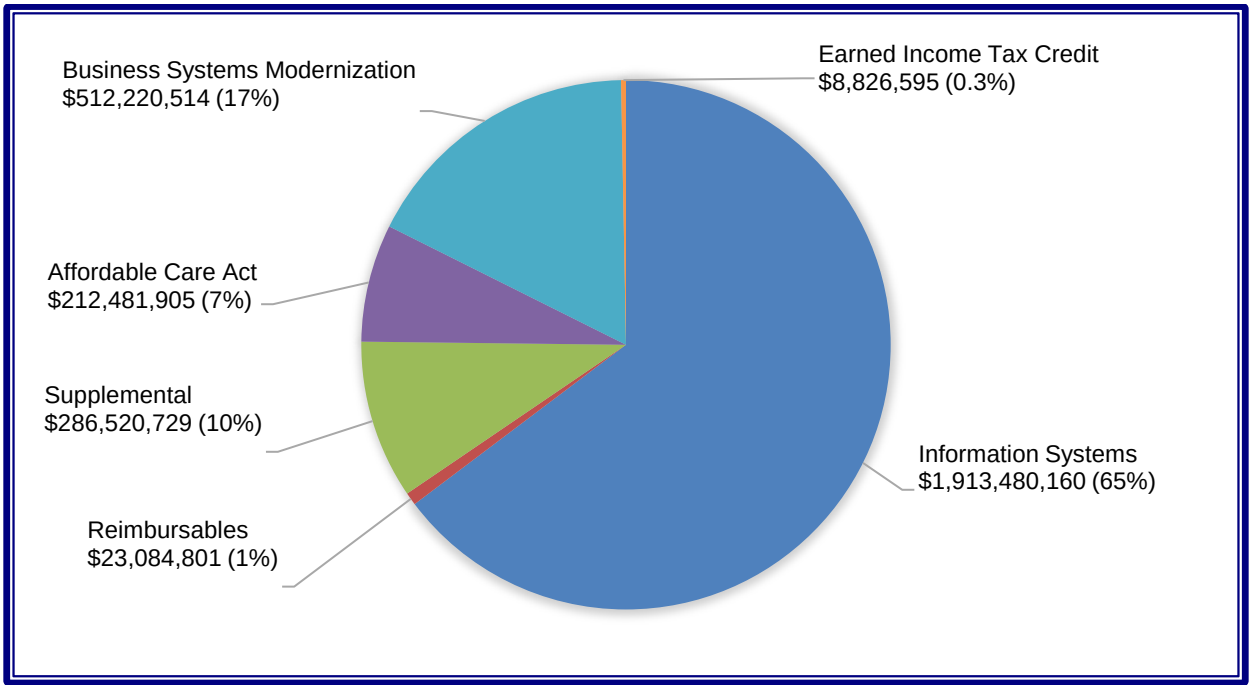
*Source: TIGTA analysis of the IRS IT organization budget data as of August 2017, based on information provided by the Associate CIO, Strategy and Planning, Financial Management Services. *Includes Business Systems Modernization funds of $512,220,514 not directly assigned to Associate CIO organizations.*

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

[4] The proportions of funding by Associate CIO organization may change because not all of these funds will be spent this year.

Figure 2 shows information technology funding for FY 2017 by funding group.

Figure 2: IRS IT Organization FY 2017 Total Available Budget by Funding Group[5]



Source: TIGTA analysis of the IRS IT organization budget data as of August 2017, based on information provided by the Associate CIO, Strategy and Planning, Financial Management Services. Note: A funding group is not the same as an appropriation source.

Figure 3 illustrates that as of June 2017, the IRS had a total of 6,749 IT organization employees, working across eight different business units.

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

Information Technology Business Unit	Number of Employees
Applications Development	1,940
Enterprise Operations	1,768
User and Network Services	1,384
Enterprise Services	642
Cybersecurity	467
Enterprise Program Management Office	268
Strategy and Planning	268
Office of the CIO	12
Total	**6,749**

Source: HRConnect human resources system, owned and operated by the U.S. Department of the Treasury as of June 2017.

- **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.
- **Strategy and Planning** collaborates with IT organization leadership to provide policy, direction, and administration of essential programs (including strategy and capital planning, and 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 CIOs, and their staffs. A Deputy CIO 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.

The compilation of information for this report was conducted at TIGTA offices during the period June through September 2017. The information presented is derived from TIGTA reports issued between October 1, 2016, and September 30, 2017. We also reviewed relevant GAO reports issued during FY 2017 and IRS documents related to IRS information technology plans and issues. The TIGTA 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 objective. 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 and a study 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. During FY 2017, TIGTA audits of the IRS information technology program addressed IRS major management and performance challenges of *Security Over Taxpayer Data and Protection of IRS Resources*; *Improving Tax Compliance*; *Improving Tax Systems and Expanding Online Services*; and *Achieving Program Efficiencies and Cost Savings*. This report presents a summary of audit results for FY 2017.

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.

Use of Information Technology Resources

Continuing to identify and achieve greater program efficiencies and cost savings is imperative for the IRS as it strives to successfully accomplish its mission in a period of shrinking budgets and declining resources. Implementing cost-saving strategies is particularly critical as the IRS is tasked with additional responsibilities, often without additional budgetary funding. In its most recent strategic plan, which guides program and budget decisions, the IRS noted that it must meet the challenge of declining resources by working to achieve the optimal scale and scope for its programs and activities.

For FY 2016, Congress appropriated $11.2 billion to the IRS, which included $290 million to address issues related to customer service, cybersecurity, and identity theft. This additional funding was the first significant increase to the IRS budget in six years. In its spend plan, the IRS informed Congress as to how the additional funds will be used to increase the telephone level of service, improve the identification and prevention of identity theft, and enhance cybersecurity to safeguard taxpayer data.

We conducted an audit of the approximate $111.6 million portion of the $290 million appropriation specifically designated for cybersecurity enhancements and identity theft

prevention.[6] We found that the IRS adequately tracked and monitored and correctly used the additional funding designated for cybersecurity enhancements and identity theft prevention.

Of the $111.6 million, $95.4 million was allocated for the Cybersecurity organization to hire additional staffing; implement a solution to further restrict IRS Local Area Network access; support a multiyear program to automate security controls and deficiency management; purchase a tool to improve both insider threat detection and application troubleshooting; implement services in response to the goals outlined in the Cybersecurity Strategy and Implementation Plan;[7] replace or retire outdated technology; enhance Cloud Computing; purchase 24/7 Subject Matter Expert support for Safeguarding Personally Identifiable Information (PII) Data Extracts; enhance vulnerability assessments; and update components to the Network Getwell Personal Identity Verification enablement solution.

The remaining $16.1 million was allocated for improvements to identity theft prevention. Funding will help protect taxpayers by combatting identity theft and refund fraud through collaborative efforts with Security Summit[8] participants; supporting a web-based authentication application allowing taxpayers to provide proof of identity; and increasing efficiency for the Taxpayer Protection Program case resolution. Funding was also allocated to enhance the IRS e-Authentication and Get Transcript applications relaunch and for IRS Cybersecurity organization work to develop advanced analytics and fraud detection capabilities. This initiative will produce significant enhancements to metrics, dashboards, and near real-time alerts to warn the IRS of potential suspicious activity.

While the IRS has taken steps to reduce costs and improve program effectiveness, TIGTA has identified a number of areas in which the IRS can more efficiently use its limited resources and make more informed business decisions. TIGTA conducted several audits that reported opportunities for the IRS to improve its use of information technology resources.

Hardware and software asset management

At the core of the IRS's tax administration is its information technology infrastructure. The IRS information technology infrastructure provides the foundation for technology services, such as server and user computing, network, storage, and communications required for day-to-day operations. Efficient and cost effective management of the IRS's hardware and software assets

[6] TIGTA, Ref. No. 2017-20-049, *Analysis of Fiscal Year 2016 Additional Appropriations for Cybersecurity and Identity Theft Prevention Improvements* (Aug. 2017).
[7] Office of Management and Budget Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (October 30, 2015), resulted from a comprehensive review in 2015 of the Federal Government's cybersecurity policies, procedures, and practices by the Cybersecurity Sprint Team.
[8] The IRS organized a Security Summit meeting on March 19, 2015, in Washington, D.C., with IRS officials, the Chief Executive Officers of the leading tax preparation firms, software developers, payroll and tax financial product processors, and State tax administrators to discuss common challenges and the ways to leverage collective resources and efforts to protect taxpayers from identity theft refund fraud.

is crucial to ensure that information technology services continue to support the IRS's business operations and to help provide services to taxpayers efficiently.

We conducted an audit to determine the efficiency and effectiveness of key ongoing or planned activities aimed at addressing the IRS operational challenge of replacing its aged hardware infrastructure.[9] We found that the IRS has not yet achieved its stated objective of reducing its aged information technology hardware to an acceptable level of 20 to 25 percent. In fact, the IRS's percentage of aged information technology hardware has steadily increased from 40 percent at the beginning of FY 2013 to 64 percent at the beginning of FY 2017.

At the beginning of FY 2016, the replacement costs for the aged hardware were estimated to be approximately $459 million, but the Sustaining Infrastructure Program's FY 2016 budget was approximately $172 million. Sustaining Infrastructure Program personnel explained that they did not receive sufficient funding each preceding fiscal year, and they would need an allocated budget of approximately two and one-half times their FY 2016 budget to replace all of the IRS's aged information technology hardware.

Each year, the IRS provides varying amounts of funds to the Sustaining Infrastructure Program from a number of different internal sources, including the IRS's base-year operations support appropriation, user fees, and carryover money from previous fiscal years not used by other IRS business units. IRS management explained that they have a process in place to monitor each financial plan and identify potential surplus funds. However, additional coordination with business units to identify the availability of surplus funds earlier in the process and development of plans to expeditiously spend these funds on the aged hardware inventory is needed. Such coordination may have resulted in a combined total of up to $67 million in additional unspent funds being available for the Sustaining Infrastructure Program during FYs 2013 through 2016.

Aged information technology hardware infrastructure still in use introduces unnecessary risk that excessive system downtime could occur due to hardware failures. When combined with the fact that components of the infrastructure and systems are interrelated and interdependent, a ripple effect may be caused making outages and failures unpredictable and introduce security risks to taxpayer data that IRS systems must protect. TIGTA analyzed 107 incident tickets most likely to involve aged hardware failures in FY 2016 and found that the aggregate length of time to resolve these issues was approximately 4,541 hours. These aged hardware failures may have also had a negative effect on IRS employee productivity, security of taxpayer information, and customer service. In addition, as the information technology hardware infrastructure ages, it becomes more difficult to obtain adequate support, and extended support from outside vendors is often very expensive.

[9] TIGTA, Ref. No. 2017-20-051, *Sixty-Four Percent of the Internal Revenue Service's Information Technology Hardware Infrastructure Is Beyond Its Useful Life* (Sept. 2017).

In addition, we initiated an audit[10] to determine the IRS's progress in addressing 14 recommendations included in three prior TIGTA audits related to software license management. In October 2016, the IRS reported that it had taken the necessary steps to address several of the previously reported recommendations and closed 11 of 14 corrective actions. However, we determined that none of the completed actions adequately addressed the recommendations and none of the corrective actions should have been closed.

Our assessment of the closed corrective actions found that the IRS did not develop an organizational structure to manage software assets and licenses; did not provide the necessary level of guidance in the documents prepared for the closure of the prior audit recommendations; did not include specific roles and responsibilities for software asset and license management in the Internal Revenue Manual; did not develop sufficient detailed Standard Operating Procedures for using software license tools for managing software licenses; and did not implement a software license tool(s) or develop and maintain an enterprise-wide inventory of software licensing data.

We also found that the IRS is not in compliance with Federal software asset management requirements set forth in Office of Management and Budget (OMB) Memorandum M-16-12, *Improving the Acquisition and Management of Common Information Technology: Software Licensing* (June 2016), or the Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016 (MEGABYTE Act of 2016).[11] For example, the IRS has not posted and maintained standard pricing and terms and conditions for acquisition agreements on the Acquisition Gateway,[12] compiled a baseline inventory of Commercial Off-The-Shelf software licenses, or reported to OMB Integrated Data Collection all cost savings and cost avoidance attributable to improved software license management.

The IRS is in the early stages of developing a program and is currently using ad hoc procedures to make progress in each of the main areas of "Govern, Manage, and Operate" towards establishing a Software Asset Management Framework. The IRS is also actively pursuing a technological solution(s) that will provide it with the ability to perform software discovery, metering, and entitlement analysis. However, at this time, the IRS is unable to establish a reliable and comprehensive software inventory and perform other aspects of software asset management such as discovery, metering, and entitlement analysis.

[10] TIGTA, Ref. No. 2017-20-062, *The Internal Revenue Service Is Not in Compliance With Federal Requirements for Software Asset Management* (Sept. 2017).
[11] Pub. L. No. 114-210, 130 Stat. 824, 40 U.S.C.
[12] The Acquisition Gateway, built by the General Services Administration, helps Federal Government buyers from all agencies act as one acquisition community.

Implementing the Information Technology Infrastructure Library® (ITIL) Framework for cost-effective computing services

We conducted this audit[13] to assess the IRS's implementation of the ITIL processes and functions in support of the Enterprise Operations organization's efforts to provide efficient, cost-effective, and highly reliable computing services. The IRS has never achieved its goal of being an organization with an overall ITIL Maturity Level 3 rating. The IRS's progress in implementing the ITIL framework has stagnated, with no significant advancements being made in FY 2017 (and this trend will most likely continue in FY 2018 and beyond). As of June 2017, 12 of the 28 adopted processes and functions related to the ITIL still have not been given an initial maturity assessment. IT organization management officials stated us that continuing budget constraints and insufficient resources are the primary causes of delaying the implementation of ITIL processes. There are currently no plans to perform additional maturity assessments or reassessments in FYs 2017 and 2018 due to the loss of key personnel (assessors) and continuing funding constraints.

As of June 2017, the IRS and its contractors have only conducted maturity assessments on 16 of the 28 adopted ITIL processes and functions and have completed reassessments on only five of the 16 previously assessed processes and functions. The FY 2016 maturity reassessments identified that the maturity level ratings for four of the five processes declined to less than a Maturity Level 3. These processes included Availability Management, Capacity Management, Change Management, and Service Asset and Configuration Management. According to IRS IT organization management officials, these declines were due in part to the identification of additional gaps, staffing changes, and changes in the overall assessment methodology using different criteria.[14] We also found that nine of the 16 existing maturity assessments have become dated, making their relevance questionable.

Finally, we found that a significant number of ITIL processes and functions do not have the directives, process descriptions, or procedures that are required for core IRS processes. Without these controls, ITIL processes and functions are likely to take longer to implement and will be less effective overall. In addition, measurement plans do not exist for many ITIL processes, and metrics are not regularly reported to management. The purpose of the measurement plan is to specify what metrics should be collected and what metrics should be computed to measure the performance and success of the process against its targeted goal and objectives.

Management officials responsible for oversight of the Information Technology Service Management program have not been regularly informed of the status of ITIL processes and functions via performance reports. If sufficient reporting is not implemented, management will

[13] TIGTA, Ref. No. 2017-20-067, *Limited Information Technology Resources Should Be Focused On Fewer Improvement Initiatives to Ensure Completion* (Sept. 2017).

[14] According to IT organization management officials, the five reassessed processes were evaluated in FY 2016 under the *International Organization for Standardization 20000-1:2011* (2nd Edition, dated April 2011) criteria and not ITIL best practices criteria used during the original maturity assessments.

be unable to gauge the performance of ITIL processes and functions or take necessary corrective actions to improve performance.

The IRS has not used Critical Position Pay Authority

In Calendar Year (CY) 1990, the Critical Position Pay Authority, codified in 5 United States Code (U.S.C.) Section (§) 5377, allows agencies to seek the approval of the Office of Personnel Management and the OMB to pay annual salaries up to the Executive Schedule Level I of $207,800 (in CY 2017) for approved staff members versus $187,000 for employees of the Senior Executive Service. Critical pay positions require an extremely high level of expertise in a scientific, technical, professional, or administrative field and must be critical to the successful accomplishment of the agency's mission.

In CY 1998, Congress provided the IRS with its own Streamlined Critical Pay authority. Similar to the Critical Position Pay Authority, the IRS would be allowed to pay salaries higher than the limit applied to employees in the Senior Executive Service and those in the Executive Schedule Level I. The Streamlined Critical Pay authority allowed the IRS to quickly hire and retain employees and compensate these employees up to the salary level of the U.S. Vice President, which in CY 2017 is $240,100. The IRS was not required to seek approval from the Office of Personnel Management and the OMB to hire and determine the salary for individuals hired into Streamlined Critical Pay positions. For this reason, the authority was considered streamlined. Congress extended the IRS's Streamlined Critical Pay authority on two occasions, and it eventually expired on September 30, 2013.

We conducted a study[15] to evaluate the IRS's efforts to use the general Federal Governmentwide Critical Position Pay Authority to fill critical technical, professional, or administrative positions. Given the sensitive information housed by the IRS, using this authority to recruit highly qualified experts to lead IRS cybersecurity and other information technology and specialized functions may better protect taxpayers from having their sensitive information misappropriated and misused.

From the inception of the Critical Position Pay Authority in CY 1990, although eligible, the IRS has not used the program. The IRS is aware of this program but has not pursued it because the IRS has used the Streamlined Critical Pay for 15 years (from CY 1998 to 2013) to fill numerous positions and believed the authority might be reinstated. The purpose of the Streamlined Critical Pay authority was to give the IRS a management tool to quickly recruit and retain employees critical to the success of the IRS's restructuring efforts. TIGTA determined that during that period, most of the Streamlined Critical Pay positions (93) were placed within the IT organization. As of March 17, 2017, the number of Streamlined Critical Pay positions still active is six. The term for all of these individuals will expire no later than September 30, 2017.

[15] TIGTA, Ref. No. 2017-IE-R007, *The Internal Revenue Service Has Not Used Critical Position Pay Authority to Hire Employees* (July 2017).

At the time of our evaluation, the IRS was preparing a request to use the Critical Position Pay Authority and had identified three Senior Executive Service positions for critical pay. These positions are the Director, Tax Processing Systems; the Director, Enterprise Architecture; and the Director, Data Management. The IRS Office of Executive Services is working with the IT organization staff to draft a justification and plans to send the request to the Secretary of the Treasury for review and approval.

Information Technology Security

For FY 2017, TIGTA designated Security Over Taxpayer Data and Protection of IRS Resources as the number one management and performance challenge area for the seventh 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 sensitive taxpayer 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 2016 OMB report to Congress,[16] malicious actors continue to gain unauthorized access to, and compromise, Federal networks, information systems, and data. During FY 2016, Federal agencies reported 30,889 impactful cybersecurity incidents to the U.S. Computer Emergency Readiness Team that led to the compromise of information or system functionality.[17] 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, 2016, to July 31, 2017, the IRS reported 304 incidents to the U.S. Computer Emergency Readiness Team. Of those 304 incidents, approximately 66 percent (201) were from lost or stolen information technology equipment. The next highest category of incidents, at 24 percent (73), involved Internal Revenue Manual noncompliance.[18]

In addition to the annual Federal Information Security Modernization Act report, we performed several audits to assess the IRS's efforts to protect its information and taxpayer data. We reviewed disaster recovery planning and testing, the computer security incident response center,

[16] OMB, *Annual Report to Congress: Federal Information Security Modernization Act* (Mar. 10, 2017).
[17] This figure cannot be compared to prior years as FY 2016 was the first year agencies were required to report impactful cyber incidents. This eliminated reporting of incidents that did not compromise information or systems.
[18] Inappropriate Usage events often originate as inside attacks conducted by legitimate users or authorized third parties on a system usually resulting in Internal Revenue Manual/Law Enforcement Manual noncompliance.

general support system security controls, e-mail records management, and external network perimeter security.

Overall assessment of the IRS Information Security Program

The Federal Information Security Modernization Act of 2014 (FISMA)[19] focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires Federal agencies to develop, document, and implement an agencywide information security program that provides security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or entity.

FISMA also 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 FISMA.

The OMB uses annual FISMA metrics to assess the implementation of agency information security capabilities and to measure overall program effectiveness in reducing risks. The FY 2017 Inspectors General FISMA Reporting Metrics were developed as a collaborative effort amongst the OMB, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency in consultation with the Federal Chief Information Officer Council. The FY 2017 metrics represent a continuation of the work that began in FY 2016 to align the Inspectors General metrics with the five cybersecurity function areas in the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[20] (Cybersecurity Framework) and transition all the function areas to maturity models. The five Cybersecurity Framework function areas are:

- IDENTIFY – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- PROTECT – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- DETECT – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- RESPOND – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

[19] Pub. L. No. 113-283. This bill amends chapter 35 of title 44 of the U.S.C. to provide for reform to Federal information security.
[20] Version 1.0, February 2014.

- RECOVER – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Figure 4 shows the alignment of the seven security program areas (or metric domains) to the five Cybersecurity Framework function areas.

Figure 4: Alignment of the NIST Cybersecurity Framework's Function Areas to the FY 2017 Inspector General FISMA Metric Domains

Cybersecurity Function Areas	FY 2017 Inspector General FISMA Metric Domains
IDENTIFY	Risk Management
PROTECT	Configuration Management Identity and Access Management Security Training
DETECT	Information Security Continuous Monitoring
RESPOND	Incident Response
RECOVER	Contingency Planning

Source: FY 2017 Inspector General FISMA Reporting Metrics.

The Inspectors General are required to assess the effectiveness of the information security programs based on a maturity model spectrum. Figure 5 details the five maturity model levels: *ad hoc*, *defined*, *consistently implemented*, *managed and measurable*, and *optimized*. The FY 2017 Inspectors General FISMA Reporting Metrics specifies that, within the context of the maturity model, Maturity Level 4 (*Managed and Measurable*) represents an effective level of security.[21]

[21] NIST Special Publication 800-53, Rev. 4, *Security and Privacy of Controls for Federal Information Systems and Organizations* (April 2013) (includes updates as of 01-22-2014), defines security control effectiveness as the extent to which the 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.

Figure 5: Inspectors General's Assessment Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measureable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2017 Inspector General FISMA Reporting Metrics.

To determine the effectiveness of the IRS's cybersecurity program, we evaluated the maturity level of the program metrics specified by the Department of Homeland Security in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0* issued on April 17, 2017. We based our FY 2017 FISMA review,[22] in part, on a representative subset of seven IRS information systems and the implementation status of key security controls. We also considered the results of TIGTA and GAO reports issued during the FY 2017 FISMA evaluation period.

We concluded 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 components not yet implemented, the IRS's information security program is not fully effective.

Based on the Department of Homeland Security's scoring methodology for the FY 2017 FISMA evaluation period, we rated two Cybersecurity Framework functions as "effective" and three as "not effective," as shown in Figure 6.

[22] TIGTA, Ref. No. 2017-20-087, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Sept. 2017).

Figure 6: Maturity Levels by Function Area

Function	Assessed Maturity Level	Effective Function
1: IDENTIFY – Risk Management	Consistently Implemented (Level 3)	No
2: PROTECT – Configuration Management Identity and Access Management Security Training	Defined (Level 2) Consistently Implemented (Level 3) Managed and Measurable (Level 4)	No
3: DETECT – Information Security Continuous Monitoring	Consistently Implemented (Level 3)	No
4: RESPOND – Incident Response	Managed and Measurable (Level 4)	Yes
5: RECOVER – Contingency Planning	Managed and Measurable (Level 4)	Yes

Source: TIGTA's evaluation of security program metrics that determined whether cybersecurity functions were rated "effective" or "not effective."

We found that two function areas (RESPOND and RECOVER, respectively) and their two security program areas (Incident Response and Contingency Planning, respectively) achieved a *Managed and Measurable* Maturity Level 4 and therefore were deemed as "effective." The remaining three Cybersecurity Framework function areas (IDENTIFY, PROTECT, and DETECT) were deemed as "not effective" for the reasons detailed below.

- **The Cybersecurity Framework function area of IDENTIFY**

  We found that the function area IDENTIFY and its security program area, Risk Management, met a *Consistently Implemented* Maturity Level 3. In order for the IRS to meet a *Managed and Measurable* Maturity Level 4 (and therefore an effective level), we believe the IRS needs to improve on the following Risk Management program performance metrics.

  - Maintain a comprehensive and accurate inventory of its information systems (including cloud systems).
  - Maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.
  - Maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting.
  - Ensure that a plan of action and milestones are used to effectively mitigate security weaknesses.

- Implement an automated solution that provides a centralized, enterprise-wide view of risks, including risk control and remediation activities, dependencies, risk scores, and management dashboards.

- **The Cybersecurity Framework function area of PROTECT**

  The function area PROTECT is made up of three security program areas: Configuration Management, Identity and Access Management, and Security Training. We found the performance metrics for Security Training achieved a *Managed and Measurable* Maturity Level 4 and was therefore considered "effective." However, the security program area of Identity and Access Management rated at a *Consistently Implemented* Maturity Level 3, and the security program area of Configuration Management rated at a *Defined* Maturity Level 2. As a result, both of these program areas were considered "not effective." Because two of the three program areas were "not effective," we rated the entire area as "not effective," and the end result of this function area was at a Maturity Level 3.

  In order for the IRS to meet an effective level for the Identity and Access Management program area, we believe the IRS needs to improve on the following performance metrics.

  - Ensure all nonprivileged and privileged users use strong authentication to access IRS facilities, network, and information systems, including remote access.
  - Employ automated mechanisms to support the management of privileged accounts.
  - Implement federally compliant encryption on all remote access connections.

  In order for the IRS to meet an effective level for the Configuration Management program area, we believe the IRS needs to improve on the following performance metrics.

  - Complete and approve configuration management plans for all IRS organizations.
  - Maintain baseline (and common secure) configurations consistently on information systems, and maintain inventories of related components at a level of granularity necessary for tracking and reporting.
  - Ensure timely remediation of information system vulnerabilities and patching.
  - Implement change control policies, procedures, and processes consistently IRS-wide.

- **The Cybersecurity Framework function area of DETECT**

  We found that the function area DETECT and its security program area, Information Security Continuous Monitoring, met a *Consistently Implemented* Maturity Level 3. In order for the IRS to meet an effective level for the Information Security Continuous

Monitoring program area, we believe the IRS needs to improve on the following performance metrics.

- Use the NIST *Special Publication 800-181, National Institute for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,*[23] to define Information Security Continuous Monitoring roles and responsibilities and map to Cybersecurity function employees, complete a skills assessment, and make targeted training recommendations in order to support a workforce capable of meeting the IRS's cybersecurity needs.
- Consistently capture qualitative and quantitative performance measures on the effectiveness of its Information Security Continuous Monitoring program.

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

In addition to our FY 2017 FISMA work, the GAO conducted an audit of IRS information security.[24] In July 2017, the GAO reported that, although the IRS has continued to make progress in addressing information security control deficiencies, the IRS has not always effectively implemented access and other controls to protect the confidentiality, integrity, and availability of its financial systems and information. Specifically, the IRS implemented controls to protect its network boundaries; however, numerous deficiencies existed in the IRS's controls related to its network devices. The IRS also took steps that improved identification and authentication controls for its computing environments; however, deficiencies in identification and authentication controls continued to exist. The GAO concluded that the collective effect of the deficiencies in information security from prior years that continued to exist in FY 2016, along with the new deficiencies it identified during the 2017 audit, represent a significant deficiency in the IRS's internal control over financial reporting systems.

Disaster recovery planning and testing

Because the IRS depends heavily on computer systems to carry out its mission, continuous operation of computing services supporting mission-essential functions is required under all circumstances. We reviewed key disaster recovery controls[25] to determine whether the IRS has a complete and adequate disaster recovery planning capability that allows it to recover major computing systems and applications from its Enterprise Computing Centers in a time frame that satisfies established business needs and priorities.

[23] August 2017.
[24] GAO, *GAO-17-395, INFORMATION SECURITY, Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2017).
[25] TIGTA, Ref. No. 2017-20-024, *Information Technology: Improvements Are Needed in Enterprise-Wide Disaster Recovery Planning and Testing* (June 2017).

Our review found an absence of a current enterprise-wide business impact analysis; a need for current and consistent mapping of mission-essential functions to supporting information technology systems and applications; and the lack of recovery priorities for recovering systems and applications supporting mission-essential functions. By not maintaining a current enterprise-wide business impact analysis, the IRS does not have reliable information to guide its disaster recovery restoration priorities. The lack of a current and consistent mapping of the IRS's critical business processes to the supporting information technology systems and applications could result in identifying incorrect and incomplete systems and applications necessary to support the IRS's critical business processes. Without recovery prioritizations of its current FISMA systems and applications for each location, operational guidance may not be sufficient to allow the IRS IT organization to efficiently recover systems and applications, especially mission-essential functions, in the event of a disruption to computing services.

According to the NIST, an agency needs to establish maximum tolerable downtimes to provide contingency planners with direction on selecting appropriate recovery strategies and methods and provide the detail needed to develop recovery procedures. Maximum tolerable downtime is the total amount of time the system owner or authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Maximum tolerable downtimes and recovery time objectives have not been identified for the IRS's mission-essential functions. Therefore, the IRS IT organization does not know how long the IRS business operating divisions are willing to be without mission-essential functions. Further, due to the IRS's practice of identifying and managing recovery time objectives for each individual system and application, sufficient information is not available to IRS IT organization management to enable them to manage an enterprise disaster recovery program effectively. The IRS also could not identify actual recovery times for all systems and applications supporting its mission-essential functions.

TIGTA observed July 2015 disaster recovery testing to determine whether the IRS is able to recover major computing systems and applications within its Enterprise Computing Centers in a time frame that satisfies established business needs and priorities. The IRS successfully recovered two of its four high-availability general support systems and satisfied the general support systems' stated recovery time objectives.

Computer Security Incident Response Center (CSIRC)

The IRS CSIRC serves as a mechanism for receiving and disseminating computer security incident information and provides a consistent capability to respond to and report cyber incidents. The CSIRC possesses capabilities that monitor, detect, and mitigate cyber threats from various sources and includes a technical team that provides deployment, maintenance, and administration of CSIRC security detection, prevention, monitoring, analysis, and reporting devices.

We conducted an audit[26] to evaluate the CSIRC's effectiveness at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. In addition, TIGTA followed up on the corrective actions for findings and recommendations from two prior audit reports that involved CSIRC operations.

Planned corrective actions from the prior TIGTA reports for computer security incident handling weaknesses were generally implemented. Five of the seven recommendations from the two TIGTA audit reports were fully implemented, one was no longer applicable, and one was partially implemented. The partially implemented recommendation was for the CSIRC to develop a standalone Incident Response Plan that includes the elements recommended by the NIST. The corrective action for the recommendation was closed December 2012, indicating that the corrective action was completed. Generally, CSIRC Incident Response Plan guidelines and procedures addressed most key elements required by Federal regulations and NIST recommendations that were included in the Internal Revenue Manual; however, the plan either did not include or only partially addressed nine (28 percent) of 32 NIST recommended elements applicable to the Incident Response Plan in the areas of policy, plan, procedure, and sharing (interactions) with outside parties.

In general, the CSIRC prevented, detected, reported, and responded to cybersecurity incidents. For example, TIGTA sampled 100 incidents from a total population of 368 incidents for FYs 2015 and 2016 (through April 30, 2016). The CSIRC properly identified and documented the type, nature, and scope of all 100 incidents with information such as the systems and applications affected, the source of the incident, and the specific kind of lost equipment. However, TIGTA identified areas in which the CSIRC could improve its operations. Specifically, we identified that improvements are needed in reporting incidents for a single threat vector to the Department of the Treasury CSIRC; consistently applying reporting procedures for like incidents by threat vectors; updating the CSIRC Incident Response Plan; and meeting FISMA training requirements for employees and contractors as well as specialized security training for employees.

TIGTA also found that not all incidents were properly reported, some supporting incident documentation was insufficient, incident costs were not captured, and reporting procedures were inconsistently applied. For example, 64 of 100 incidents were required to be reported to the Department of the Treasury CSIRC because the incidents were confirmed to have compromised the confidentiality, integrity, or availability of a Federal Government information system. Of the 64 incidents, 22 were not reported as required. On February 15, 2017, after bringing the noncompliance to the IRS's attention, the 22 incidents were reported to the Department of the Treasury CSIRC.

[26] TIGTA, Ref. No. 2017-20-050, *The Computer Security Incident Response Center Is Preventing, Detecting, Reporting, and Responding to Incidents, but Improvements Are Needed* (Aug. 2017).

CSIRC employees and contractors did not always meet training guidelines, and skill assessments demonstrate a need for more training. Not all CSIRC employees complied with FISMA and other required internal specialized security training for FYs 2015 and 2016. The employees took courses the IRS deemed as specialized; however, TIGTA disagreed with the designation after a closer review of the courses' objectives. In addition, there was no documentation that contractors met the same requirements for the same periods. A key finding of a study conducted by McAfee, the self-proclaimed world's largest dedicated security company, is that a shortage of cybersecurity skills makes organizations more desirable hacking targets.

Big Data Analytics (BDA) General Support System (GSS) security controls

The Integrated Production Model (IPM) system is a centralized analytical data store that provides a single point of access to core taxpayer data (such as taxpayer accounts and tax returns). It also provides other specific data used by a wide range of IRS business applications to support case identification, selection, prioritization, delivery, and reporting. We conducted a review[27] to determine whether IPM system security has been effectively incorporated into the BDA GSS. Security weaknesses could adversely affect tax administration and the protection of taxpayer data.

The IRS made a variety of significant changes to the IPM system, including moving its data to different software and hardware platforms. When these changes were made, business ownership and security responsibilities of the IPM system also changed and, as a result, the IPM is no longer classified as a major application. The IPM system is now part of the BDA GSS.

The IRS did not follow established procedures requiring the submission of a security change request for new information systems being introduced to the IRS infrastructure and for changes to existing information systems. The change request to move the IPM system to the BDA GSS security boundary was submitted on July 9, 2015; however, the IRS approved the move April 2015. As a result of not following the established security change management process, approximately 10 percent of security controls that previously protected IPM system data were not captured by the BDA GSS.

The IRS did not update its Memorandum of Understanding between the BDA office and the Applications Development function that included the Applications Development function's responsibilities when the IPM system moved under the BDA's GSS security boundary. As a result, the Applications Development function was unclear of its responsibilities with regard to the controls and assumed the BDA GSS was responsible for implementing the IPM system's noninherited controls. Without following the security change management process, there is an increased risk that changes could expose the BDA GSS and its taxpayer data to additional security vulnerabilities.

[27] TIGTA, Ref. No. 2017-20-029, *The Big Data Analytics General Support System Security Controls Need Improvement* (June 2017).

The IRS did not follow existing policy regarding system access and approval. For the BDA GSS, we found that 21 (40 percent) of 52 accounts were not authorized through the Online 5081 application. We divided these accounts into the two categories required to follow the Online 5081 process and determined that three (23 percent) of 13 database administrator accounts and 18 (46 percent) of 39 service accounts were not approved. Improper account management increases the risk of an unauthorized user gaining access to sensitive and privileged data such as a taxpayer's PII (including date of birth and Social Security Number).

External network perimeter security

The IRS uses numerous public-facing information systems on its IRS.gov website to engage taxpayers for tax administration purposes. These systems may process and store PII and tax return data for millions of taxpayers. Because this information is considered extremely valuable, the IRS has become a target of cyber criminals and identity thieves. As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information continues to be a top concern for the IRS. The mission of the IRS may be seriously undermined if the systems and data used to meet tax administration responsibilities are not secure from unauthorized access and misuse.

We completed an audit[28] to evaluate the effectiveness of the network perimeter security controls to protect the IRS against external threats and cyberattacks. To assist with this review, TIGTA hired a contractor to perform penetration testing that simulated an advanced, highly-funded attacker attempting to gain access to IRS sensitive systems and information through the Internet. TIGTA also completed audit steps to determine whether the IRS had implemented adequate policies and procedures for maintaining a secure perimeter and correcting reported vulnerabilities in a timely manner.

The penetration tests conducted by the contractor showed that the IRS's perimeter network was generally secure and has appropriate security measures against attacks. Also, other recently completed IRS penetration testing on its perimeter and web applications generally found it was secure as well. Further, in October 2016, the Department of Homeland Security National Cybersecurity Assessment and Technical Services team conducted a Risk and Vulnerability Assessment (as mandated by the OMB) on Internet Protocol addresses associated with two IRS high-value assets and selected internal Internet Protocol address ranges provided by the IRS. The National Cybersecurity Assessment and Technical Services team also conducts a weekly external vulnerability scan to search for issues on the IRS's external network. The weekly scan revealed an administrative interface that could permit an attack to gain control of the network router, which was deemed a medium-level vulnerability. The IRS indicated that it has corrected the vulnerability.

[28] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017).

However, we found improvements were needed to ensure that the IRS perimeter inventory is accurate and complete and that the vulnerabilities identified by scans are timely addressed. Inventory records for the IRS's perimeter security system were inaccurate and incomplete, and scans performed on the perimeter security system components for the months of August, September, and October 2016 did not align with the components in the inventory lists.

- The IRS provided policy checker reports for only 39 of the 282 servers listed in the September 2016 inventory and provided reports for 49 servers that were not listed.
- The IRS provided Tripwire scanning reports for only 19 of the 263 servers listed in the January 2017 inventory[29] and provided reports for 144 servers that were not listed.
- The IRS provided Guidelines, Standards, and Procedures scan reports for only 112 of the total 190 firewalls, routers, and switches listed in the September 2016 inventory and provided reports for 41 devices that were not listed.

Without an accurate GSS-1 inventory, the IRS cannot ensure that it is properly monitoring and maintaining all its perimeter supporting components in a secure manner.

Vulnerabilities identified by scans we reviewed were not timely corrected. We identified instances in which high-level vulnerabilities were not corrected within the 30-day required time frame and medium-level vulnerabilities were not corrected within the 90-day required period. The IRS indicated that, due to resource constraints, it is not addressing repeated medium- or low-level vulnerabilities until it completes its work to address its high-level vulnerabilities. However, the scan reports we reviewed revealed that not all high-level vulnerabilities were being corrected timely, in addition to the medium- and low-level vulnerabilities that also persisted.

Protection of Taxpayer Data

The trillions of dollars that flow through the IRS each year make it an attractive target for criminals who exploit the tax administration system in various ways for personal gain. Tax-related scams, and the methods used to perpetrate them, are continually changing and require constant monitoring by the IRS. As a result, TIGTA has added Identity Theft and Impersonation Fraud as the number two management and performance challenge facing the IRS.

The IRS has made progress in protecting individuals against identity theft. So far for CY 2017, individuals reporting identity theft have declined sharply compared to the same time in CYs 2016 and 2015. In the first five months of CY 2017, about 107,000 taxpayers reported being victims of identity theft, compared to the same period in CY 2016, when 204,000 filed

[29] We compared the Tripwire reports against the January 2017 GSS-1 inventory because the IRS initially only provided Tripwire reports for servers that had high-level vulnerabilities during the months of August through October 2016. At our second request for the Tripwire reports for all GSS-1 servers, the IRS provided reports for the months of December 2016 through February 2017. Therefore, we compared the Tripwire reports against the January 2017 GSS-1 inventory.

victim reports. That is about 97,000 fewer victims, representing a drop of 47 percent. For comparison, there were nearly 297,000 identity theft victims during the first five months of CY 2015.

Despite this progress, identity theft continues to have a significant impact on both the IRS and on victims of this crime. The threat is constantly evolving as fraudsters and criminal enterprises use complex and highly sophisticated tactics and look for new ways to reach their target. The IRS has seen an increase in identity theft involving business-related tax returns. The IRS has identified approximately 10,000 business returns as potential identity theft through June 1, 2017, compared to about 4,000 for CY 2016 and 350 for CY 2015. The potential dollar amounts were significant: $137 million for CY 2017, $268 million for CY 2016, and $122 million for CY 2015.

In March 2017, the IRS shut down the online Data Retrieval Tool because identity thieves that had obtained personal information outside of the IRS used the tool to steal additional data. The Data Retrieval Tool is accessible from the fafsa.gov and StudentLoans.gov websites and allows applicants to automatically populate their tax return information to the Free Application for Federal Student Aid or to apply for an income-driven repayment plan for their student loans. The data obtained through the unauthorized use of the tool were later used to file fraudulent returns. The IRS found that approximately 100,000 individuals may have had their taxpayer information compromised. About 8,000 fraudulent refunds were issued, costing $30 million. The IRS fraud detection systems stopped 52,000 returns and prevented 14,000 illegal refund claims from being sent.

In a report of the IRS 2017 Filing Season,[30] the GAO reported on an IRS effort to help combat identity theft refund fraud and improper payments. For the 2017 Filing Season, the IRS implemented W-2 systemic verification, which compares Form W-2, *Wage and Tax Statement*, data to taxpayers returns before paying refunds. Wage information that employers report on Forms W-2 had not been available to the IRS until after it issued most refunds. In its testimony to the Subcommittee on Oversight, Committee on Ways and Means, House of Representatives, the GAO reported that the Form W-2 data helped identify $863 million in refunds as potentially fraudulent. However, wage data were not available in time for all tax returns due to older computer systems and paper Forms W-2 (which had to be manually processed).

TIGTA conducted the following audits during FY 2017 to address IRS efforts to detect fraud and prevent identity theft.

The Return Review Program (RRP) and retirement of the Electronic Fraud Detection System (EFDS)

The goal of implementing the RRP is to replace the older EFDS with an automated system that would better enhance the IRS's capabilities to prevent, detect, and resolve criminal and civil

[30] The period from January through mid-April when most individual income tax returns are filed.

noncompliance. The RRP is an important development to the IRS's efforts to keep pace with increasing levels of fraud and to serve the organization's evolving compliance needs. The IRS has implemented progressive RRP functionality since launching its first pilot of RRP Identity Theft (IDT) models in April 2014. We conducted a review[31] to determine if the RRP system can identify all fraud currently identified by other existing fraud detection systems and to assess EFDS retirement plans. We concluded that the RRP better meets the IRS business objectives of delivering greater fraud detection at a lower False Detection Rate.

Results from recent filing seasons support the IRS decision to retire the EFDS models. We believe the RRP is better positioned than the EFDS to address the changing nature of IDT because: 1) The EFDS uses models to generate one fraud score for each return. In contrast, RRP models generate a set of predictive scores for every return. This enables the RRP to individually assess tax returns across all IDT and Non-IDT fraudulent categories. 2) The RRP has a more robust business rules engine compared to the EFDS, giving it greater flexibility to adjust to emerging fraud trends.

The IRS retired the EFDS IDT models for the 2016 Filing Season. The EFDS IDT model selections that were not selected by any other fraud detection system accounted for $60 million, which is 1.5 percent of the total $3.92 billion IRS IDT revenue protection. In comparison, the RRP IDT model selections that were not selected by any other fraud detection system totaled $1.88 billion, accounting for 47.8 percent of the total $3.93 billion IRS IDT revenue protection.

In addition, when the IRS ran the EFDS and the RRP Non-IDT models in parallel for one full filing season, the RRP Non-IDT models selected 41,710 fraudulent tax returns not selected by the EFDS, representing $328 million in revenue protection. In comparison, the EFDS Non-IDT models selected 6,824 fraudulent tax returns not selected by the RRP, representing $17 million in revenue protected. Just as with the IDT models, we do not believe that the relatively small number of tax returns selected by the EFDS Non-IDT models warranted delaying the retirement of those models after the 2016 Filing Season.

In a prior audit report, TIGTA recommended the IRS develop a system retirement plan for the EFDS and retire the system after validating that the RRP effectively identifies, at a minimum, all issues currently identified by the EFDS. The IRS agreed with the recommendation, and in December 2015, the IRS Executive Steering Committee unanimously approved the EFDS Retirement Strategy. Our review of the EFDS Retirement Strategy showed that the IRS cannot shut down the EFDS until all 19 system components have been decommissioned. Eleven of the 19 components are related to the Enterprise Case Management project and have retirement dates as late as December 2018. Because the Enterprise Case Management project is starting over with a software selection, the IRS will likely miss the December 2018 target date to retire the remaining 11 EFDS components. As a result, the IRS will continue to incur annual costs to

[31] TIGTA, Ref. No. 2017-20-080, *The Return Review Program Increases Fraud Detection; However, Full Retirement of the Electronic Fraud Detection System Will Be Delayed* (Sept. 2017).

operate and maintain the EFDS system each filing season beyond the 2018 Filing Season. The IRS stated that the annual operating and maintenance cost for the EFDS for the 2018 Filing Season is an estimated $13.9 million.

Security of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center

In January 2017, the IRS established the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (hereafter referred to as the ISAC) to provide a secure platform for sharing identity theft tax refund fraud information among the IRS, State tax agencies, and the private industry tax sector. TIGTA conducted an audit[32] to determine whether the IRS developed the ISAC in accordance with Federal security standards to ensure that sensitive fraud data are protected against unauthorized access. The IRS contracted with a company to create and maintain the ISAC and ensure the site's reliability and security. We found that the ISAC generally adhered to data protection standards; however, some security controls were still planned or needed improvement.

- **********2**********
  **********2**********
  **********2**********
  **********[33]*******2**********.
- **********2**********
  **********2**********
  **********2**********
  **********2**********
  *********2**********.
- ***The Privacy Incident Response Plan was still under development –*** The contractor did not have a Privacy Incident Response Plan in place specifically for the ISAC. Without a Privacy Incident Response Plan, privacy-related incidents may not be reported in a timely manner to appropriate IRS officials to allow for a quick response to any potential security incident or unauthorized disclosure.
- ***A risk assessment of the harm that could result from unauthorized access was not conducted –*** The contractor did not conduct a risk assessment specifically of the ISAC. The contractor indicated that it was in the process of developing a separate risk assessment for the ISAC, expecting to complete it by July 2017. The lack of a risk

[32] TIGTA, Ref. No. 2017-20-064, *The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Generally Adhered to Data Protection Standards, but Additional Actions Are Needed* (Sept. 2017).
[33] Cache poisoning, also called DNS poisoning or DNS cache poisoning, is the corruption of an Internet server's DNS table by replacing an Internet address with that of another rogue address.

assessment of the ISAC environment may result in risks not being properly assessed and raises the risk that vulnerabilities would persist and not be timely corrected or mitigated.

- ***The Flaw Remediation Policy was incomplete and not fully implemented –*** The contractor's policy did not specify a time frame to address vulnerabilities identified as high impact. In addition, our review of vulnerability scanning reports showed that one ISAC server, in operation in January 2017, was not updated until March 2017 with a security patch that was released by the vendor in November 2016. This left the server exposed to high-level vulnerabilities, **********2********** **********2**********. The contractor did not always correct medium vulnerabilities within its established time frame of 10 business days. Examples of medium vulnerabilities that persisted for 69 business days or longer included **********2********** **********2**********. When information system flaws are not timely corrected, vulnerabilities may be exploited.
- ***Plan of Action and Milestones processes needed improvement to ensure effective monitoring of weaknesses –*** Processes could be improved to ensure that Plan of Action and Milestones weaknesses are adequately tracked and timely corrected. For example, we noted instances in which Plan of Action and Milestones tracking reports were inconsistent in regards to tracking remediation to completion and containing the data elements required by the IRS and the OMB. Tracking remediation of identified weaknesses is less effective when Plans of Action and Milestones are inaccurate or incomplete and do not include necessary details to determine the proper status of corrective actions.
- ***The physical security portion of the Computer Security Assessment has not been performed –*** The IRS has not yet performed the physical security portion of the Computer Security Assessment. Without an assessment of the physical security controls at the contractor site, the IRS has no information on the status of these controls.

Protection of data transfers to external partners

The IRS shares data with various outside entities including Federal, State, and local agencies; financial institutions; and contractors for tax administration purposes. The data may include sensitive information, such as PII and taxpayer information. IRS and Federal guidelines require that sensitive data be protected during transmission to prevent unauthorized access or disclosure. TIGTA completed an audit[34] to determine whether the IRS was properly protecting the data it transmits to external entities through secure file transfer technology and whether the IRS was maintaining encryption controls and other security configurations in accordance with the NIST.

[34] TIGTA Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).

We reported that the IRS did not ensure that encryption requirements are being enforced and that nonsecure protocols, including File Transfer Protocol and Telnet, are not being used in order to fully protect information during transmission. The IRS stated that it cannot fully enforce encryption requirements or disallow use of the nonsecure protocols because not all of its external partners that trade data with the IRS can comply with encryption requirements. The IRS was unable to determine during our audit how many external partners do not comply with Federal standard encryption and therefore need to be accommodated. The IRS indicated a change request was prepared in July 2016 to modify ciphers within the managed file transfer solution to ensure compliance with Federal encryption standards.

Until the IRS has better information on its data transfer environment and its partners that require data transfers without encryption, it cannot make a proper determination on whether to accept the risk of continuing to allow the nonsecure protocols or to enforce its policy to encrypt data transmissions and insist its partners do so as well. Transmitting unencrypted information puts information at risk of unauthorized disclosure.

Risk of improper disclosure of taxpayer information increases by not adhering to electronic mail (e-mail) policies

E-mail is a prevalent form of communication in the IRS. Employees who have frequent contact with taxpayers, *i.e.*, revenue officers and revenue agents, need to ensure that appropriate steps to safeguard e-mails are being taken. We initiated an audit[35] to determine whether Small Business/Self-Employed Division employees followed e-mail policies and properly safeguarded taxpayer PII and tax return information contained in e-mail correspondence. The proper protection of taxpayer PII and tax return information helps maintain taxpayer confidence and the IRS's reputation for privacy protection, which are critical for the IRS to perform its mission.

The IRS uses the Secure Enterprise Messaging System (Secure Messaging) to send encrypted Microsoft Outlook[36] messages between IRS employees when those messages contain taxpayer PII or tax return information. IRS employees may not send taxpayer PII or tax return information by e-mail outside the IRS unless the IT organization approves an exception. We reviewed a random sample of 80 Small Business/Self-Employed Division employees' e-mails sent during May and June 2015. Based on our sample results, we estimate that 11,416 Small Business/Self-Employed Division employees sent 95,396 unencrypted e-mails with taxpayer PII or tax return information for 2.4 million taxpayers during the four-week period of our sample. If this four-week period is typical, we estimate that more than 1.1 million unencrypted e-mails with taxpayer PII or tax return information of 28.2 million taxpayers could be sent annually.

TIGTA identified 275 unencrypted e-mails that contained taxpayer PII or tax return information that were sent internally to other IRS employees. These e-mails were sent inside the IRS internal

[35] TIGTA, Ref. No. 2017-30-010, *Employees Sometimes Did Not Adhere to E-mail Policies Which Increased the Risk of Improper Disclosure of Taxpayer Information* (Oct. 2016).
[36] E-mail software commonly used by the IRS.

information system firewall and therefore pose less risk of improper disclosure or improper access. TIGTA also identified 51 unencrypted e-mails that contained taxpayer PII or tax return information that were sent externally to non-IRS e-mail accounts. Additionally, 20 e-mails sent by six employees to personal e-mail accounts involved official IRS business.

Improving Information Technology Systems and Expanding Online Services

Successful modernization of IRS systems and the development and implementation of new information technology applications are critical to meet the IRS's evolving business needs and to enhance services provided to taxpayers. A primary focus for the IRS over the past two decades has been to migrate taxpayers to electronic filing. Outside of filing activities, taxpayers also use the Internet to download forms, view content, and check the status of their refund. These types of online activities will increase as the IRS implements its Future State Initiative.

The IRS's modernization effort continues to focus on core tax administration systems designed to provide more sophisticated tools to taxpayers and IRS employees. It will provide the foundation for implementing a real-time tax system, reducing improper payments and fraudulent refunds, and providing the technology infrastructure and architecture that will enable taxpayers and other stakeholders the capability to securely access tax account information. TIGTA identified several areas in which the IRS can improve its information technology systems.

IRS cloud strategy

In an audit[37] to review the IRS's progress in establishing an enterprise-wide cloud strategy and its compliance with Federal and agency guidelines and best practices, we found that the IRS does not have an enterprise-wide cloud strategy and did not follow Federal and agency cloud service guidelines for the Form 990 Cloud Project.[38] Not having a documented enterprise-wide cloud strategy creates a significant risk that organizations outside of the IRS Chief Information Officer and IT organization may deploy systems and potentially expose Federal tax information with no reasonable assurance that the systems meet applicable Federal security guidelines. The IRS may also miss the opportunity to deliver public value by increasing operational efficiency and responding faster to constituent needs.

In July 2016, the IRS created an Integrated Planning Team with an overall goal of developing an enterprise-wide cloud strategy for implementation within the IRS. The Integrated Planning Team's mission is to help the IRS define a "cloud" and some specific guidance to assist in the selection and deployment of cloud services within the IRS. At the end of our fieldwork, the

[37] TIGTA, Ref. No. 2017-20-032, *The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service* (Aug. 2017).
[38] A cloud service project initiated by the IRS Tax Exempt and Government Entities Division to allow public access to certain Form 990, *Return of Organization Exempt From Income Tax*, information.

Integrated Planning Team had not yet formulated an IRS definition for cloud or maintained an adequate inventory of cloud systems. Although the IRS has taken steps to develop an enterprise-wide cloud strategy, it remains in the early stages of defining an official enterprise-wide policy. The IRS stated that there is no current timetable for adoption and implementation of the enterprise-wide cloud strategy.

In part, as a result of the IRS's lack of an enterprise-wide cloud strategy, the Tax Exempt and Government Entities Division entered into an agreement to use a public cloud service with limited involvement from the IRS IT organization. In October 2015, the Tax Exempt and Government Entities Division had discussions with the Associate Chief Information Officer for Enterprise Services regarding the Form 990 Cloud Project. However, the Tax Exempt and Government Entities Division was not instructed to appoint an authorizing official, generate an agency Authority to Operate letter, or ensure that the cloud service complied with Federal Risk and Authorization Management Program requirements. By not adhering to Federal guidelines regarding cloud implementation, the IRS risks Form 990 data accuracy and availability issues due to the lack of clearly defined roles and responsibilities for the cloud service provider in measurable terms. Additionally, the IRS did not incorporate any service-level agreements into the current user agreement with Amazon Web Services.

Web Applications Systems Release 1.0

In November 2013, a task force of IRS executives convened to develop a Future State Vision designed to transform IRS operations in order to modernize the taxpayer experience, make filing simpler for taxpayers, and increase voluntary compliance. The Web Applications (Web Apps) Program Management Office was initiated to drive innovation and create digital services to meet taxpayer needs. Its primary purpose was to establish an online account for individual taxpayers that links the taxpayer to various IRS services. TIGTA initiated an audit[39] to determine whether the IRS adequately developed and tested the functionality of the taxpayer's online account provided by Release 1.0 of the Web Apps system. This release was designed to deliver an online account for individual taxpayers along with the ability to see a balance due, see the payment status/history, make a payment, and view/download tax transcripts.

We found that the development and deployment of Release 1.0 of the Web Apps system was significantly delayed. The Web Apps Program Management Office was initially tasked with delivering its four original functionalities for Release 1.0 of the Web Apps system by September 30, 2015. A lack of funding caused a delay in the Web Apps Program Management Office obtaining the necessary staffing resources. Similarly, inconsistent governance contributed to project delays. The Web Apps Program Management Office was transferred to various executive steering committees and governance boards that were responsible for approving the funding for the system's staffing resources. These delays prevented taxpayers from being able to use any of

[39] TIGTA, Ref. No. 2017-20-057, *While Release 1.0 of the Web Applications System Was Successfully Deployed, Several Factors Contributed to Implementation Delays* (Sept. 2017).

Release 1.0 of the Web Apps system's planned functionalities for the 2016 Filing Season. The Program Management Office deployed the Minimum Viable Product, *i.e.*, *See a Balance Due* and *Make a Payment*, externally for taxpayers to use in November 2016. Following the initial deployment, the Web Apps Program Management Office continued to work on delivering the remaining two planned functionalities for Release 1.0 of the Web Apps system. As of June 2017, these two functionalities, *See the Payment Status/History* and *View/Download Tax Transcripts*, were added to the Web Apps system and made available for taxpayers to use.

Additionally, an incompatible work request process caused delays in receiving products and services for the development of Release 1.0 of the Web Apps system. These deficiencies in resources caused the program to refocus its priorities to first develop the *See a Balance Due* and *Make a Payment* functionality. Due to the delayed deployment of the two Web Apps system functionalities, the IRS missed an opportunity for greater success in its efforts to improve taxpayer access to information and reduce taxpayer burden. As a result, at the start of the 2017 Filing Season, taxpayers were unable to use the Web Apps system to see payment status and history or view and download transcripts. To acquire this information, taxpayers had to use the separate Get Transcript Online Service, use the IRS2GO mobile phone app, call, mail, fax, or visit an IRS taxpayer assistance center, which does not achieve its goals to "modernize the taxpayer experience" and increase its efficiency. These requests could have been provided in a more timely and direct manner by Release 1.0 of the Web Apps system if it had been deployed on schedule.

IRS enterprise e-mail system

We conducted two audits that evaluated the IRS enterprise e-mail system. The objective of the first audit was to 1) determine what the IRS's policies are for record retention and whether they comply with Federal requirements and 2) determine whether the IRS's practices for responding to Freedom of Information Act[40] requests, litigation holds,[41] and congressional requests ensure that responsive records are retained and provided according to Federal requirements. This audit[42] was requested by the Chairman of the House Committee on Ways and Means and Chairman of the Senate Committee on Finance to determine the IRS's policies for record retention, whether the policies comply with Federal requirements, and whether the IRS's practices for responding to requests for records ensure that responsive records are retained and provided according to Federal requirements.

We determined that IRS policies are not in compliance with Federal electronic records requirements and regulations. The IRS's current e-mail system, Exchange Server 2010, and

[40] 5 U.S.C. § 552.
[41] A litigation hold is a mechanism used to preserve relevant and responsive records related to any known or anticipated court proceedings.
[42] TIGTA, Ref. No. 2017-10-034, *Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested* (July 2017).

record retention policies do not ensure that e-mail records are automatically archived for all employees and can be searched and retrieved for as long as needed. The current e-mail system requires users to take manual actions to archive e-mail and results in e-mail records that could be stored in multiple locations such as mailbox folders, the exchange server, network shared drives, hard drives, removable media, and backup tape.

IRS standard policies for disposal of computer devices, including desktops, laptops, computer hard drives, and backup tapes, have been revised and reversed several times between May 2013 and January 2016. These repeated changes affected the effectiveness of the IRS's record retention. Specifically, although policy updates were put in place, the hard drives from laptop and desktop computers stored by the IT organization Enterprise Operations function were not always associated with the name of the employee or the laptop from which the hard drive was taken. Without this correlation, successfully completing a search for specific e-mail or other electronic information residing on a disposed hard drive would be highly unlikely and could result in destroyed records. In addition, there was no policy in place to ensure that laptops of separating employees under litigation holds were maintained. We found that when an employee under a litigation hold separated from the IRS in August 2014, the employee's laptop was sent to the IT organization for standard sanitization and disposal.

The IRS's current Exchange Server 2010 e-mail system, which lacks sufficient storage and automatic archiving of e-mail, requires users to take manual actions to archive, to their computer hard drives, all e-mail and instant messages that are Federal records. According to the IRS, its Future State e-mail system being developed will potentially allow records to be available and searchable while automatically applying a retention policy. However, until a solution is effectively implemented, these e-mails remain difficult, if not impossible, to retain and search.

In December 2014, the IRS issued an interim policy that requires e-mail to be archived for all executives whose positions and responsibilities make them most likely to produce e-mail messages that meet the definition of a Federal record. TIGTA found that this policy was not implemented effectively. We found four of a sample of 20 executives did not properly configure their e-mail accounts to archive e-mail as required. Also, there were no controls in place to ensure that newly on-boarded executives were also identified and their e-mail accounts were configured to archive their e-mail to a shared network drive. Consequently, the IRS took corrective action and, in September 2016, finalized Standard Operating Procedures designed to ensure that e-mail is archived for all newly on-boarded executives.

Lastly, the IRS does not maintain one authoritative list of executive e-mail accounts. The Standard Operating Procedure does not provide for a reconciliation of the separate lists of executives compiled by the IT organization and the Privacy, Governmental Liaison, and Disclosure organization. Without one authoritative list, the IRS cannot ensure that all executives are included in this effort and cannot verify that e-mails are archived for all required accounts.

We conducted the second audit[43] to evaluate the readiness of the IRS to establish the information technology capabilities to manage temporary and permanent e-mail records in compliance with the OMB Memorandum M-12-18, *Managing Government Records Directive*, by the December 21, 2016, deadline. The Directive, issued in August 2012, requires that agencies eliminate paper and use electronic recordkeeping to the fullest extent possible. The Exchange 2016 upgrade is planned to enhance mailbox sizes and provide an archiving solution that will enable the IRS to implement standardized record retention policies.

To help implement the electronic recordkeeping functionalities in the Code of Federal Regulations, in April 2016, the National Archives and Records Administration issued the *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18)* to provide clarification of the existing requirements that directly relate to the e-mail management success criteria.[44] Successful e-mail management was defined as having policies and systems in place to ensure that e-mail records can be used, accessed, and the appropriate disposition applied.

We found that more effort is needed to meet the e-mail management success criteria prior to the deployment of the enterprise e-mail solution. To evaluate the IRS's progress in meeting the Directive's goals, the audit team developed a data collection instrument that incorporated the requirements of the 32 questions from Appendix A of the *Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18).* We determined that 13 requirements related to the 32 (41 percent) individual questions associated with the four e-mail management success criteria remained under development as of January 31, 2017. The requirements need to be fully developed and implemented before the IRS can successfully deploy its enterprise e-mail solution. Due to delays in developing and deploying the enterprise e-mail solution, the IRS will most likely not begin receiving any of the expected benefits of Federal records reform until the end of CY 2017, nearly a year after the mandated deployment date.

We found that project risk mitigation was not sufficient for the Enterprise Exchange Upgrade Project. A July 2016 *IT Executive Oversight Team Weekly Discussion Notes and Actions* included only two high-level risks. However, risk mitigation actions were not well defined and did not include detailed mitigation plans. In addition, accountable owners were not identified, due dates were not specified, and the cost of mitigation actions was not estimated.

Risk management controls concerning risk roles and responsibilities, risk identification, and risk mitigation were not sufficiently designed and implemented, which would have significantly affected the IRS's readiness to deploy any enterprise e-mail solution. Further, a Risk Management Plan had not been initially developed and approved by IT organization

[43] TIGTA, Ref. No. 2017-20-039, *Additional Efforts Are Needed to Ensure the Enterprise E-Mail Records Management Solution Meets All Requirements Before Deployment* (Aug. 2017).
[44] 36 C.F.R. § 1236.20(b) (2011).

management for the Enterprise Exchange Upgrade Project. During the audit, the IRS implemented controls to define risk roles and responsibilities; identify risks and risk owners; and manage risk impact, probability of occurrence, criticality, and mitigation strategies for the Enterprise Exchange Upgrade Project.

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 2017.[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 2017. 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 2017. 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 and a study issued during FY 2017. 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.

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. This report presents an overall assessment of the IRS information technology program based on a compilation of the audit results reported during FY 2017. Therefore, we did not evaluate internal controls as part of this review.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
John Ledford, Director
Myron Gulley, Audit Manager
Joan Bonomi, Lead Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
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/Study Report Title	Report Issuance Date
1	2017-30-010	*Employees Sometimes Did Not Adhere to E-mail Policies Which Increased the Risk of Improper Disclosure of Taxpayer Information*	October 14, 2016
2	2017-20-004	*Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners*	October 24, 2016
3	2017-20-024	*Information Technology: Improvements Are Needed in Enterprise-Wide Disaster Recovery Planning and Testing*	June 1, 2017
4	2017-20-029	*The Big Data Analytics General Support System Security Controls Need Improvement*	June 9, 2017
5	2017-10-034	*Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested*	July 13, 2017
6	2017-IE-R007	*The Internal Revenue Service Has Not Used Critical Position Pay Authority to Hire Employees*	July 24, 2017
7	2017-20-039	*Additional Efforts Are Needed to Ensure the Enterprise E-Mail Records Management Solution Meets All Requirements Before Deployment*	August 7, 2017
8	2017-20-032	*The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service*	August 7, 2017
9	2017-20-049	*Analysis of Fiscal Year 2016 Additional Appropriations for Cybersecurity and Identity Theft Prevention Improvements*	August 14, 2017

Number	Report Reference Number	Audit/Study Report Title	Report Issuance Date
10	2017-20-050	*The Computer Security Incident Response Center Is Preventing, Detecting, Reporting, and Responding to Incidents, but Improvements Are Needed*	August 28, 2017
11	2017-20-057	*While Release 1.0 of the Web Applications System Was Successfully Deployed, Several Factors Contributed to Implementation Delays*	September 7, 2017
12	2017-20-051	*Sixty-Four Percent of the Internal Revenue Service's Information Technology Hardware Infrastructure Is Beyond Its Useful Life*	September 11, 2017
13	2017-20-062	*The Internal Revenue Service Is Not in Compliance With Federal Requirements for Software Asset Management*	September 18, 2017
14	2017-20-067	*Limited Information Technology Resources Should Be Focused on Fewer Improvement Initiatives to Ensure Completion*	September 18, 2017
15	2017-20-061	*The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved*	September 20, 2017
16	2017-20-080	*The Return Review Program Increases Fraud Detection; However, Full Retirement of the Electronic Fraud Detection System Will Be Delayed*	September 25, 2017
17	2017-20-064	*The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Generally Adhered to Data Protection Standards, but Additional Actions Are Needed*	September 28, 2017
18	2017-20-087	*Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017*	September 29, 2017

Appendix V

Outcome Measure Reported in Fiscal Year 2017

Audit Report Title	Type of Measure	Amount
Sixty-Four Percent of the Internal Revenue Service's Information Technology Hardware Infrastructure Is Beyond Its Useful Life (Ref. No. 2017-20-051)	Inefficient Use of Resources	Potential; $67,000,000

Appendix VI

Glossary of Terms

Term	Definition
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 information technology 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.
Contractor	An organization external to the IRS that supplies goods and services according to a formal contract or task order.
Domain Name System	A device to access Internet resources by user-friendly domain names rather than Internet Protocol addresses; users need a system that translates these domain names to Internet Protocol addresses and back.
e-Authentication	The process of establishing confidence in user identities electronically presented to an information system.

Term	Definition
Federal Information Security Modernization Act	Amendment to The Federal Information Security Management Act of 2002 that allows for further reform to Federal information security; signed in 2014, 12 years after the passing of the original law. This bill amends chapter 35 of title 44 of the U.S.C. (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).
File Transfer Protocol	A service that supports file transfer between local and remote computers.
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.
Hardware	The physical parts of a computer and related devices; it includes motherboards, hard drives, monitors, keyboards, mice, printers, and scanners.
Incident Response Plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against an organization's information systems.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.

Term	Definition
Information Technology Infrastructure Library®	Provides guidelines for the use and management of software and licenses. It is a widely accepted set of concepts and practices for the Information Technology Service Management program derived from user and vendor experts in both the private and public sectors. It focuses on the key service management principles pertaining to service strategy, service design, service transition, service operation, and continual service improvement, with each principle being covered in a separate core publication.
Information Technology Infrastructure Library Maturity Levels	Maturity levels refer to an information technology organization's ability to perform. An organization passes through the following five evolutionary maturity levels as it becomes more competent: - Level 1: Initial – Focuses on technology and technology excellence/experts. - Level 2: Repeatable – Focuses on products/services and operational processes, *e.g.*, Service Support. - Level 3: Defined – Focuses on the customer and proper service-level management. - Level 4: Managed – Focuses on business/information technology alignment. - Level 5: Optimized – Focuses on value and the seamless integration of information technology into the business and strategy-making.
Information Technology Organization	Works closely with each IRS operating division and functional area to deliver quality, world-class information technology support, services, and solutions.
Internet Protocol Address	A 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a Transmission Control Protocol/Internet Protocol network.
Local Area Network	A group of computers and associated devices that share a common communications line or wireless link to a server. Typically encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment. Computers and other mobile devices use the connection to share resources such as a printer or network storage.

Term	Definition
National Institute of Standards and Technology	Part of the U.S. Department of Commerce. It 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.
Penetration Testing	A test methodology in which assessors, using all available documentation, *e.g.*, system design, source code, manuals, and working under specific constraints, attempt to circumvent the security features of an information system.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Release	A specific edition of software.
Risk	A potential event that could have an unwanted impact on the cost, schedule, business, or technical performance of an information technology program, project, or organization.
Taxpayer Protection Program	Responsible for identifying potential identity theft cases that are scored by a set of identity theft models in the Dependent Database (an application that is designed to identify potentially ineligible tax returns claiming certain refundable credits); selected through filters in the RRP system; or manually selected by Integrity and Verification Operation, an IRS organization whose mission is to support IRS civil fraud detection and prevention efforts in a prerefund environment.
Telnet	A telecommunications protocol providing specifications for emulating a remote computer terminal so that one can access a distant computer and function online using an interface that appears to be part of the user's local system.