TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the Internal Revenue Service's Information Technology Program for Fiscal Year 2018

September 26, 2018

Reference Number: 2018-20-083

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.

HIGHLIGHTS

ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE'S INFORMATION TECHNOLOGY PROGRAM FOR FISCAL YEAR 2018

Highlights

Final Report issued on September 26, 2018

Highlights of Reference Number: 2018-20-083 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

In Fiscal Year 2017, the IRS collected approximately $3.4 trillion in Federal tax payments, processed more than 245 million tax returns and other forms, and paid approximately $437 billion in refunds to taxpayers. In addition, the IRS employs approximately 81,000 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the IRS's information technology program could result in computer operations that become compromised, disrupted, or outdated, which could adversely affect the IRS's ability to meet its mission of providing America's taxpayers with top-quality service by helping them understand and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

The IRS Restructuring and Reform Act of 1998 requires TIGTA to annually assess and report on an evaluation of the adequacy and security of IRS information technology. Our overall objective was to assess the adequacy and security of the IRS's information technology program.

WHAT TIGTA FOUND

The IRS has made progress in many areas, but additional improvements are needed. TIGTA and the Government Accountability Office identified a number of areas in which the IRS can more efficiently use its limited resources and make more informed business decisions. For example, in the area of system security and privacy of taxpayer data, TIGTA found that the IRS is taking steps to improve its security program deficiencies and fully implement all security program areas in compliance with the Federal Information Security Modernization Act of 2014 requirements. However, taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure until all areas of the IRS security program are fully implemented. Problems were also reported in the IRS's handling of the privacy of taxpayer data; physical security and systems access controls; authentication controls; identification and protection of system boundary components; system configuration and change management; system scanning, vulnerability remediation, and patching; network monitoring and audit logs; and system security documentation.

In our reviews of systems development and information technology operations, TIGTA found that the IRS's initial efforts to develop an Enterprise Case Management solution were unsuccessful, costing $85.4 million and approximately two and a half years of work. Problems were also reported with the IRS's information technology acquisitions, project management, hardware and software asset management, human capital, and implementation of corrective actions.

In our reviews of filing season readiness, TIGTA found that, while the IRS effectively responded to the April 17, 2018, Tax Day outage and resumed tax processing operations, the major outage process needs improvement to reduce risk and response times in the future. TIGTA found that the IRS successfully implemented Section 201 of the Protecting Americans from Tax Hikes Act of 2015, but noted specific risks related to the implementation of the Tax Cuts and Jobs Act of 2017.

WHAT TIGTA RECOMMENDED

Because this report was an assessment report of the IRS's information technology program based on TIGTA and Government Accountability Office reports issued during Fiscal Year 2018, TIGTA did not make any further recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 26, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Annual Assessment of the Internal Revenue Service’s Information Technology Program for Fiscal Year 2018 (Audit # 201820002)

This report presents the results of our assessment of the adequacy and security of the Internal Revenue Service’s (IRS) information technology program for Fiscal Year 2018. This review is required by the IRS Restructuring and Reform Act of 1998.[1] This audit is included in our Fiscal Year 2018 Annual Audit Plan and addresses the major management challenges of *Security Over Taxpayer Data and Protection of IRS Resources*; *Providing Quality Taxpayer Service and Expanding Online Services*; *Implementing Tax Law Changes*; *Improving Tax Compliance*; *Reducing Fraudulent Claims and Improper Payments*; and *Achieving Program Efficiencies and Cost Savings*.

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

[1] Pub. L. No. 105-206, 112 Stat. 685.

Table of Contents

Background....Page 1

Results of Review....Page 6

System Security and Privacy of Taxpayer Data....Page 6

Systems Development and Information Technology Operations....Page 44

Filing Season Readiness....Page 57

Appendices

Appendix I – Detailed Objective, Scope, and Methodology....Page 61

Appendix II – Major Contributors to This Report....Page 63

Appendix III – Report Distribution List....Page 64

Appendix IV – List of Treasury Inspector General for Tax Administration and Government Accountability Office Reports Reviewed....Page 65

Appendix V – Glossary of Terms....Page 67

Abbreviations

CIO	Chief Information Officer
CSDW	Cybersecurity Data Warehouse
ECM	Enterprise Case Management
EFTPS	Electronic Federal Tax Payment System
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act of 2014
GAO	Government Accountability Office
IMF	Individual Master File
IRS	Internal Revenue Service
IT	Information Technology
JAMES	Joint Audit Management Enterprise System
KISAM-AM	Knowledge Incident/Problem Service Asset Management-Asset Manager
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PATH Act	Protecting Americans from Tax Hikes Act of 2015
PCA	Planned Corrective Action
POA&M	Plan of Action and Milestones
Smart ID	Smart Identification
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number

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's 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 2018.[2]

The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In Fiscal Year 2017, the IRS collected approximately $3.4 trillion in Federal tax payments, processed more than 245 million tax returns and other forms, and paid approximately $437 billion in refunds to taxpayers. Further, the size and complexity of the IRS add unique operational challenges. The IRS employs approximately 81,000 people in its Washington, D.C., headquarters and its 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 continued growth of the Internet 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 (Fiscal Years 2018 – 2022), customers continue to 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 Fiscal Year 2017, 87 percent of individual taxpayers chose to file electronically, a 52.6 percent increase from 57 percent in Fiscal Year 2007. During Fiscal Year 2017, the IRS website was visited more than 495 million times, and taxpayers used the "Where's My Refund?" tool nearly 328 million times, a 9 percent increase over the prior year.

The IRS's Fiscal Year 2018 appropriations increased by $195.6 million over Fiscal Year 2017 levels to $11.4 billion, of which $320 million designated for taxpayer services, enforcement, and operations support was to be used for implementing the Tax Cuts and Jobs Act of 2017.[3] The

[1] Pub. L. No. 105-206, 112 Stat. 685.

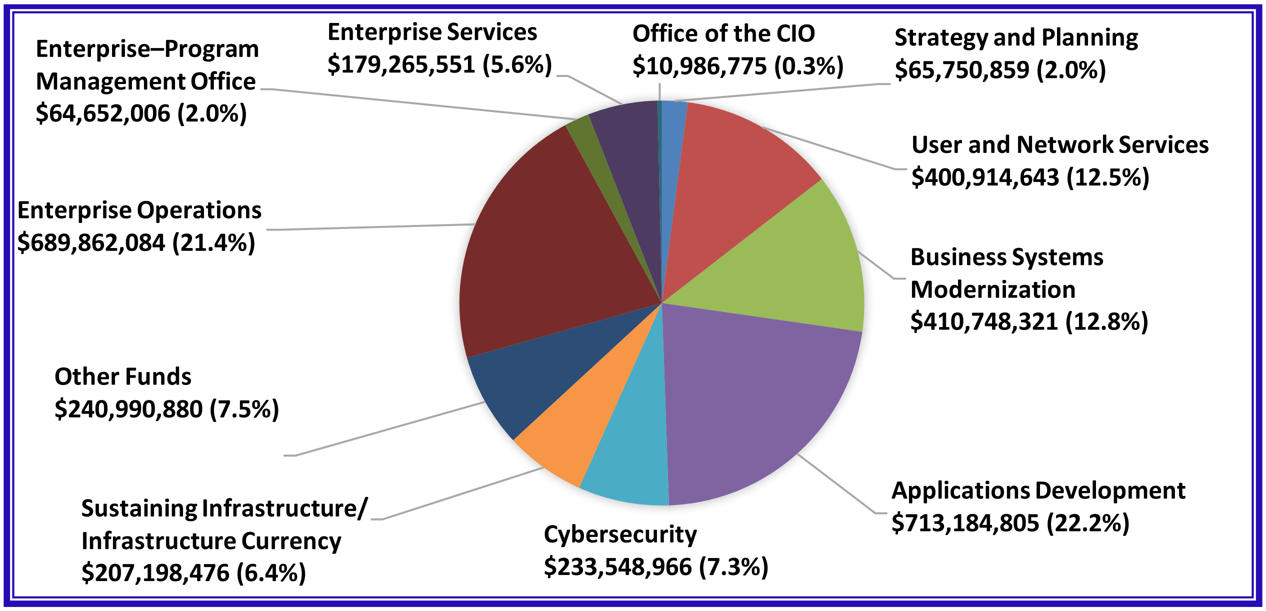
[2] See Appendix V for a glossary of terms.

[3] Pub. L. No. 115-97.

Information Technology (IT) organization's portion of this designated funding amount was $275 million, or 86 percent.

The 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 Fiscal Year 2018 projected available funds included about $3.2 billion for information technology investments, representing 28 percent of the total IRS budget, up from approximately $2.9 billion in Fiscal Year 2017. Figure 1 illustrates the IRS's Fiscal Year 2018 information technology funding by the Associate Chief Information Officer (CIO) organization and major program.

Figure 1: Fiscal Year 2018 Total Available Funding by Associate CIO Organization and Major Program[4]

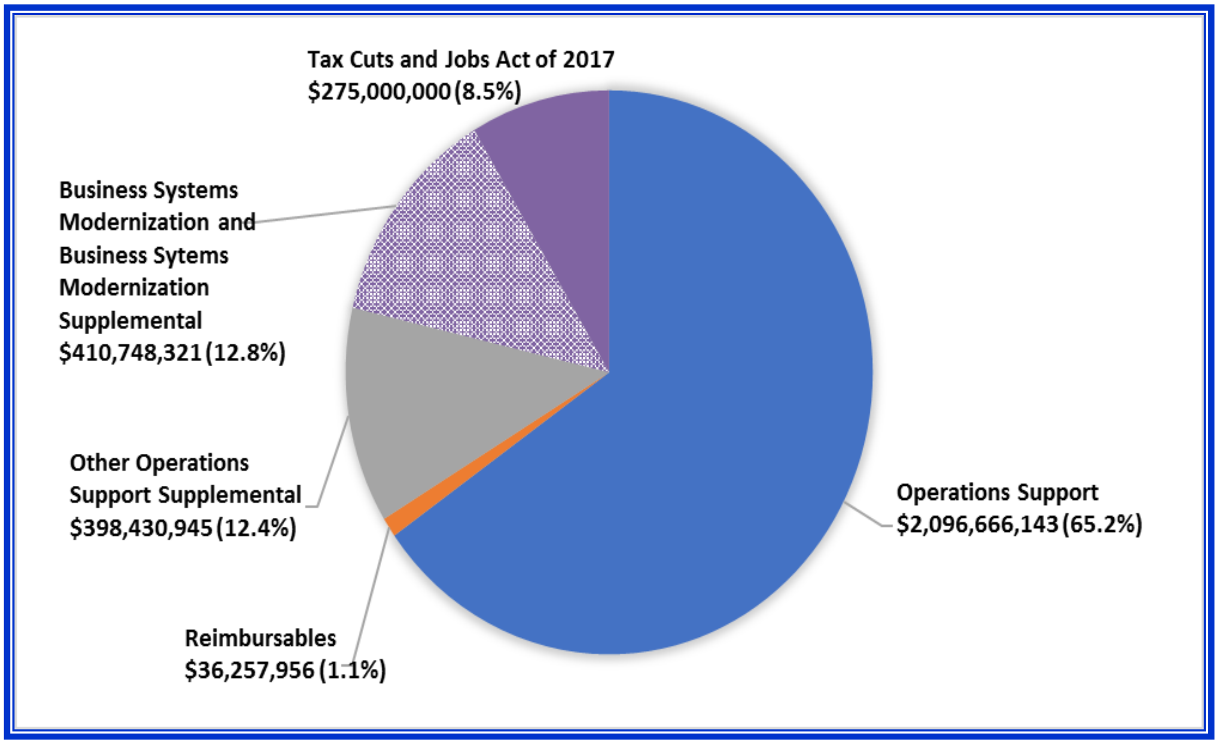


Source: *The IT organization budget data as of May 2018, based on information provided by the Strategy and Planning function's Office of Financial Management Services. The Other Funds category includes the Treasury Franchise Fund, Shared Support, and Funds Awaiting Distribution.*

Figure 2 shows the IT organization funding for Fiscal Year 2018 by funding source.

[4] The difference of $1 between the total available funding amounts in Figures 1 and 2 is due to rounding.

Figure 2: Fiscal Year 2018 Total Available Funding by Funding Source



Source: The IT organization budget data as of May 2018, based on information provided by the Strategy and Planning function's Office of Financial Management Services.

Figure 3 illustrates that, as of July 2018, the IRS had a total of 6,511 information technology employees working across eight different business units, 238 fewer employees than in Fiscal Year 2017.

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

Information Technology Business Unit	Number of Employees
Applications Development	1,840
Enterprise Operations	1,724
User and Network Services	1,298
Enterprise Services	651
Cybersecurity	458
Strategy and Planning	267
Enterprise-Program Management Office	262
Office of the CIO	11
Total	6,511

Source: IRS Human Resources Reporting Center as of July 2018.

- **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 Operations** provides computing (server and mainframe) services for all IRS business entities and taxpayers.

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

- **Enterprise Services** is responsible for strengthening technology infrastructure across the enterprise.

- **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.

- **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.

- **Enterprise-Program Management Office** is responsible for the delivery of integrated solutions for several of the IRS's large-scaled programs. It plays a key role in establishing configuration management and release plans and implementing new information system functional capabilities.
- **The Office of the CIO** includes the CIO, two Deputy CIOs, and their staff. 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 various TIGTA offices during the period of May through September 2018. The information presented is derived from TIGTA and Government Accountability Office (GAO) reports issued during Fiscal Year 2018 as well as IRS documents related to its 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 and GAO audit reports used in this assessment is presented in Appendix IV.

Results of Review

During this annual review, we summarize information from the information technology program efforts in systems security, development, and operations as required by the IRS Restructuring and Reform Act of 1998. During Fiscal Year 2018, TIGTA audits of the information technology program addressed the IRS major management and performance challenges of *Security Over Taxpayer Data and Protection of IRS Resources*; *Providing Quality Taxpayer Service and Expanding Online Services*; *Implementing Tax Law Changes*; *Improving Tax Compliance*; *Reducing Fraudulent Claims and Improper Payments*; and *Achieving Program Efficiencies and Cost Savings*. This report presents a summary of TIGTA and GAO audit results for Fiscal Year 2018.

The IRS has made progress in many areas, but additional improvements are needed. Overall, the IRS needs to ensure that it continues to leverage 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.

System Security and Privacy of Taxpayer Data

Protecting the confidentiality of sensitive taxpayer information is paramount. Otherwise, taxpayers could be exposed to financial and privacy loss as well as damages resulting from identity theft or other financial crimes. The U.S. Computer Emergency Readiness Team receives computer security incident reports from the Federal, State, and local governments, commercial enterprises, U.S. citizens, and international Computer Security Incident Response Teams.

According to the Office of Management and Budget's (OMB) annual report to Congress for Fiscal Year 2017,[5] Federal agencies reported 35,277 cybersecurity incidents, across nine vector categories,[6] to the U.S. Computer Emergency Readiness Team.[7] This represents a 14 percent increase from Fiscal Year 2016, when agencies reported 30,899 incidents. E-mail/Phishing

[5] OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress – Fiscal Year 2017*.

[6] The vector categories include: Attrition; E-mail/Phishing; External/Removable Media; Improper Usage; Loss or Theft of Equipment; Web; Physical Cause; Other; and Multiple Attack Vectors.

[7] As of April 1, 2017, Federal agencies are required to report to the U.S. Computer Emergency Readiness Team only information security incidents in which the confidentiality, integrity, or availability of a Federal information system of a civilian Executive Branch agency is potentially compromised. Incidents that have been found not to impact confidentiality, integrity, or availability may be reported voluntarily; however, they may not be included in the OMB's report to Congress.

continues to be a highly targeted attack vector, with 7,328 incidents occurring in the prior year. Moreover, nearly 31 percent of all incidents did not have an identified attack vector, which continues to suggest that the Government must take additional steps to help agencies identify the sources and vectors of these incidents. Of the 35,277 incidents, Federal agencies reported five incidents that met the threshold for major incidents, one of which involved the IRS. On March 3, 2017, the IRS identified a breach in which 100,210 taxpayers had their adjusted gross income information exposed to unauthorized parties via impersonation through its Data Retrieval Tool.[8]

Without effective security controls, computer systems are vulnerable to human actions committed in error or with malicious intent. People acting with malicious intent can use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks. These threats to computer systems and related critical infrastructure can come from sources that are internal and external to an organization. Internal threats include equipment failure, human errors, and fraudulent or malicious acts by employees or contractors. External threats include the ever-growing number of cyber-based attacks that can come from a variety of sources such as individuals, groups, and countries who wish to do harm to an organization's systems or steal an organization's data.

For Fiscal Year 2018, TIGTA designated *Security Over Taxpayer Data and Protection of IRS Resources* as the number one major management and performance challenge area for the eighth 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 and improper disclosure or destruction and that computer operations supporting tax administration are secured against disruption or compromise.

In addition to TIGTA's annual Federal Information Security Modernization Act of 2014[9] (FISMA) report, we performed several audits to assess the IRS's efforts to protect its information and taxpayer data. Our audits covered privacy of taxpayer data; physical security and systems access controls; authentication controls; identification and protection of system boundary components; system configuration and change management; system scanning, vulnerability remediation, and patching; network monitoring and audit logs; and system security documentation.

[8] The Data Retrieval Tool allows students and parents to access their adjusted gross income information through an interface with the IRS to complete the Free Application for Federal Student Aid [a Department of Education application]. Identity thieves used personal information of individuals that they obtained outside the tax system to start the application process in order to secure the adjusted gross income tax information from the IRS through the Data Retrieval Tool.

[9] 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.

Overall assessment of the Information Security Program

The FISMA focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. The FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and the systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or entity. It also requires each agency Inspector General, or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency.

The 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 the 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 Fiscal Year 2018 Inspector 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 CIO Council. The Fiscal Year 2018 Inspector General metrics align with the five cybersecurity function areas in the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[10] (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.
- 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.

[10] Version 1.0, February 2014.

Figure 4 shows the alignment of the eight metric domains, *i.e.*, security program areas, to the five Cybersecurity Framework function areas.

Figure 4: Alignment of the NIST Cybersecurity Framework's Function Areas to the Fiscal Year 2018 Inspector General FISMA Metric Domains

Cybersecurity Function Areas	Fiscal Year 2018 Inspector General FISMA Metric Domains
IDENTIFY	Risk Management
PROTECT	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
DETECT	Information Security Continuous Monitoring
RESPOND	Incident Response
RECOVER	Contingency Planning

Source: Fiscal Year 2018 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 Fiscal Year 2018 Inspector General FISMA Reporting Metrics specify that, within the context of the maturity model, *Managed and Measurable* (Maturity Level 4) represents an "effective" level of security.[11]

[11] NIST, Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) (includes updates as of January 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: Inspector General's Assessment Maturity Model Spectrum

Maturity Model Level	Maturity Model 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: *Fiscal Year 2018 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 *Fiscal Year 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 1.0*, issued on April 11, 2018. We based our Fiscal Year 2018 FISMA review,[12] 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 Fiscal Year 2018 FISMA evaluation period.

We concluded that the IRS has established a Cybersecurity Program that was generally aligned with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. However, due to two of the five program components being partially implemented, the Cybersecurity Program was not fully effective.

Based on the Department of Homeland Security's scoring methodology for the Fiscal Year 2018 FISMA evaluation period, we rated three Cybersecurity Framework functions as "effective" and two as "not effective," as shown in Figure 6.

[12] TIGTA, Ref. No. 2018-20-082, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Sept. 2018).

Figure 6: Maturity Levels by Function Area

Framework Foundation Function	Assessed Maturity Level	Effective?
IDENTIFY – Risk Management	***Managed and Measurable* (Level 4)**	**Yes**
PROTECT –		**No**
Configuration Management	***Defined* (Level 2)**	
Identity and Access Management	***Consistently Implemented* (Level 3)**	
Data Protection and Privacy	***Defined* (Level 2)**	
Security Training	***Managed and Measurable* (Level 4)**	
DETECT – Information Security Continuous Monitoring	***Consistently Implemented* (Level 3)**	**No**
RESPOND – Incident Response	***Managed and Measurable* (Level 4)**	**Yes**
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 three Cybersecurity Framework function areas, *i.e.*, IDENTIFY, RESPOND, and RECOVER, and their three security program components, *i.e.*, Risk Management, Incident Response, and Contingency Planning, respectively, achieved a *Managed and Measurable* (Maturity Level 4) and therefore were deemed as "effective." For the remaining two function areas, *i.e.*, PROTECT and DETECT, we found that four of their five security program components were deemed as "not effective" for the reasons subsequently discussed.

<u>The Cybersecurity Framework function area of PROTECT</u>

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

In order for the IRS to meet an effective level for the Configuration Management, Identity and Access Management, and Data Protection and Privacy program components, we believe that it needs to improve on the following performance metrics.

- Ensure that policy and procedures for maintaining baseline configurations or component inventories, secure configurations settings in compliance with IRS policy, flaw remediation and patching, and configuration change control are consistently implemented.

- Use automated processes for discovering and disabling accounts.
- Ensure that all nonprivileged and privileged users use strong authentication to access IRS information systems.
- Ensure that privileged accounts are provisioned, managed, and reviewed.
- Review and remove unnecessary Personally Identifiable Information collections on a regular basis.
- Fully implement all elements of the Data Loss Prevention solution, specifically those related to data at rest.
- Implement security controls to prevent data exfiltration, including checking outbound communications to detect encrypted exfiltration of information.
- Ensure that updates are made to its privacy program as a result of training exercises.

The Cybersecurity Framework function area of DETECT

We found that the function area DETECT and its security program component, 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 component, we believe that it needs to improve on the following performance metrics.

- Continue to automate and develop additional performance measures for the processes and procedures that support Information Security Continuous Monitoring.
- Address the challenge of a shortage of human resources with critical skills in order to address the gaps in knowledge and skills that are essential to the success of key information technology investments.
- Continue to implement a data analysis tool and reporting system to achieve requirements for data collection, storage, analysis, retrieval, and reporting.

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

Privacy of taxpayer data

The risk of fraud has increased as more Personally Identifiable Information has become readily available as a result of large-scale cyberattacks on entities including the IRS, the Office of Personnel Management, and more recently, Equifax.® For example, in May 2015, the IRS temporarily suspended its Get Transcript service after fraudsters used Personally Identifiable

Information obtained from sources outside the IRS to pose as legitimate taxpayers and access tax return information for up to 724,000 accounts. In June and July 2015, the Office of Personnel Management announced two data breaches affecting approximately 22.1 million current or former Federal employees and contractors and their family members. Among the data stolen were Social Security Numbers as well as financial and personal health information. In September 2017, Equifax announced that criminals had exploited a vulnerability in its systems and obtained Personally Identifiable Information, including names, Social Security Numbers, birth dates, addresses, and in some cases, driver's license information, on 145.5 million individuals. The proliferation of stolen Personally Identifiable Information poses a significant threat to tax administration by making it difficult for the IRS to distinguish legitimate taxpayers from fraudsters.

The trillions of dollars that flow through the IRS each year make it an attractive target for criminals who want to exploit the tax 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 major management and performance challenge facing the IRS. The IRS estimates that at least $12.2 billion in identity theft tax refund fraud was attempted in Calendar Year 2016 and that it prevented the theft of at least $10.5 billion of that amount. However, the IRS reports that at least $1.6 billion was paid out to fraudsters. The IRS's ability to continuously monitor and improve its approach to taxpayer authentication is a critical step in defending the agency against evolving cyber threats and fraud schemes and in protecting billions of taxpayer dollars.

During Fiscal Year 2018, TIGTA conducted two audits to evaluate data protection measures–one of private collection agencies participating in the Private Debt Collection Program[13] and the other of the IRS's eServices Transcript Delivery System.[14] In the private collection agency audit, we identified that end-to-end encryption is not enforced for the transferring of taxpayer data to the private collection agencies. The process for transferring cases to private collection agencies requires a secure tunnel for transmission of the data. The data at rest prior to transmission are located in a folder that is specific to each private collection agency. The private collection agency retrieves the data from its own specific folder. We determined that the data at rest in the specific folders were not encrypted before or after transit once they reached the private collection agencies. The data should be encrypted before reaching this secure file transfers function and should remain encrypted until reaching the employees at the private collection agencies who are authorized to access the data. When the data at rest are not encrypted, unauthorized disclosure of taxpayer information can occur because the files containing the data are unencrypted and anyone

[13] TIGTA, Ref. No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).

[14] TIGTA, Ref. No. 2018-40-014, *Transcript Delivery System Authentication and Authorization Processes Do Not Adequately Protect Against Unauthorized Release of Tax Information* (Mar. 2018).

with access to the files can read the information. Therefore, taxpayer data are at risk of unauthorized browsing.

Our review of the processes that eServices Transcript Delivery System users or taxpayers can use to request and obtain tax transcripts identified that the IRS cannot confirm with certainty that a taxpayer actually authorized the release of his or her tax information. The IRS is responsible for protecting taxpayers' data from unauthorized disclosure and, as such, needs to ensure that taxpayers have authorized the release of their tax information. The IRS has the authority to disclose taxpayer return information to a third party designated by the taxpayer; however, the taxpayer's or an authorized person's signature must be on the request document in order to provide authorization for the IRS to disclose taxpayer information. In addition, the taxpayer's information may be provided only to a third party whose name and address is listed on the properly signed authorization.

Tax transcripts, if obtained by unscrupulous individuals, provide valuable tax information that can be used to prepare and file fraudulent tax returns. Although we are unable to conclusively determine that a tax transcript was not requested by the legitimate taxpayer or their representative, our comparison of tax transcript requests to tax returns identified by the IRS as fraudulent raises concern of the potential improper use of the Transcript Delivery System. Our comparison of Tax Years 2013 through 2016 tax transcript requests to taxpayer accounts that had confirmed identity theft found that 430,000 taxpayer accounts had a total of 1,472,369 tax transcripts requested for the tax year prior to the tax year identity theft was confirmed. In addition, we found that 222,534 taxpayer accounts had a total of 647,208 tax transcripts requested for the same tax year as the tax year with confirmed identity theft.

During Fiscal Year 2018, the GAO conducted a review of protecting sensitive financial and taxpayer data[15] and found that the IRS corrected 13 of the 34 encryption control deficiencies that the GAO previously identified. For example, the IRS encrypted the authentication from its workstations to one of its systems. The IRS also configured various platforms and client software to encrypt connections between systems as well as used encryption on servers supporting several systems. However, the IRS had not yet addressed 21 of the 34 recommendations. For example, the IRS had not enforced the use of encryption algorithms compliant with NIST Federal Information Processing Standard 140-2, *Security Requirements for Cryptographic Modules*,[16] on some systems and applications. In addition, the IRS had not yet encrypted sensitive data on its Oracle® databases supporting 11 systems and applications the GAO previously reviewed. As a result, the IRS has an increased risk that an unauthorized individual could exploit encryption weaknesses to view and then use data, such as user account and passwords, to gain access to systems that contain financial and sensitive data.

[15] GAO, GAO-18-391, *INFORMATION SECURITY: IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

[16] Initially released March 28, 2003, and last updated May 25, 2018.

Access controls

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. This is accomplished by designing and implementing controls to prevent and limit unauthorized access to programs, data, facilities, and other computing resources. Access controls include both physical and system security controls.

Physical security access controls

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. They include, among other things, policies and practices for background investigations of an individual's qualifications, suitability, and fitness for employment in the Civil Service; use of access cards and locks authorizing individuals' physical access to facilities and resources designed to protect IRS personnel, assets, computer systems, and information; and periodically reviewing access authorizations in order to ensure that continued access is necessary.

For Fiscal Year 2018, TIGTA and the GAO conducted audit coverage of physical security controls at the IRS in five audits. We performed an audit of Smart Identification (Smart ID) cards[17] and found that controls did not provide assurance that Smart ID cards were returned when contractor employees separated. Our review of a statistical random sample of contractor employee separations found substantial recordkeeping issues[18] and could not determine whether 96 (85 percent) of the 113 Smart ID cards were recovered from the sampled contractor employees who separated from the IRS between April 1, 2015, and March 31, 2016. Based on the results, we estimated that the IRS cannot verify the return of Smart ID cards for 523 (85 percent)[19] of the more than 600 contractor employee separations during the same period.

We performed additional analyses of the destruction logs, the deactivation and destruction dates in USAccess, and the last IRS computer facilities or system access date by the contractor employee in our sample and identified the following:

- Seventy-nine Smart ID cards were marked as deactivated and destroyed in USAccess. We also found that eight of the 79 former contractor employees accessed systems,

[17] TIGTA, Ref. No. 2018-10-004, *Improved Controls Are Needed to Account for the Return of Contractor Employee Identification Cards* (Nov. 2017).
[18] We reviewed Forms 13716-A, *Request for ID Media/Access Card for Contract Employee*, and destruction logs to determine if Smart ID cards were returned. We did not accept USAccess information as proof that Smart ID cards were returned because the cards can be deactivated and marked as destroyed in the system without the IRS having recovered them.
[19] The point estimate projection is based on a two-sided 95 percent confidence interval. We are 95 percent confident that the point estimate is between 479 and 557.

according to access logs, after IRS records show the contractor employee separated. In these instances, IRS management provided reasonable explanations for the accesses.[20]

- Seventeen Smart ID cards were either not marked as destroyed in USAccess[21] or had conflicting information regarding the cards' use and destruction. In addition, logs show that several of the contractor employees accessed IRS facilities and systems after their separation date; however, IRS officials could not provide explanations or determine whether Smart ID cards were used for these accesses.

In our audit of active directory and Criminal Investigation computer rooms,[22] we identified that its computer rooms housing domain controllers lack physical security controls. We conducted site visits at 11 IRS locations: two enterprise computing centers; one campus; and eight field offices located throughout the United States. We found a total of 88 policy exceptions relating to physical security controls, with 87 (99 percent) of the exceptions observed at the eight field offices. Some of the physical security control policy exceptions included the following:

- Limited Areas – We found that only two of the eight field offices had properly designated their Criminal Investigation computer rooms as limited areas. Further, all eight field offices and one enterprise computing center did not issue Smart ID cards to all employees with the required "R" indicator, which signifies an individual assigned to the limited area. We also found that seven of the eight field offices did not always completely implement, use, and properly retain Form 5421, *Limited Area Register*.

  In addition, six of eight field offices did not use approved access lists for the Criminal Investigation computer rooms. Of those two field offices that used the access list, one of the lists was extremely outdated and included unlimited access to the computer room by separated employees. We did not find records at any of the eight field offices that documented the required monthly reviews of the authorized access list and the limited area register; therefore, this information was not forwarded on to the local security office for review and retention.

- Two-Factor Authentication – We found that two-factor authentication has not been implemented for any of the Criminal Investigation computer rooms located in the eight field offices. The Criminal Investigation field offices are instead using badge only, key, or cipher lock to access the computer room. We found two-factor authentication in place at each of the two enterprise computing centers and the campus, with

[20] For example, several of the system accesses were made by former contractor employees who later became IRS employees. We verified that the system accesses were made after the former contractor employees became IRS employees.

[21] The Smart ID card for one separated contractor employee was still active in USAccess.

[22] TIGTA, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018).

one exception. The visitor badges issued for entry into the campus computer rooms were not functioning properly.

- Control and Safeguarding Lock Combinations – We found combination locks to gain access to the Criminal Investigation computer rooms in five of the eight field office locations. However, none of the five offices had a process in place to ensure that the locks were being changed in accordance with the Internal Revenue Manual.[23] Specifically, exceptions included that personnel were unaware of the requirements relating to combination locks, one location was still using the manufacturer default as the combination, and other offices only changed the combination when employees departed the IRS. The Internal Revenue Manual requires the combination to each lock be changed when the safe or lock is originally received, at least every three years, when a person knowing the combination no longer requires access to it and other controls do not exist to prevent his or her access, and when the combination is compromised.

Our review of the private collection agencies at four locations determined that the physical access controls were working as intended and the restricted areas, such as the collection, data, and mail processing areas, had limited access. Three of the four private collection agencies had a separate secure space for extracting mail. Security cameras recorded video footage for various doors and restricted areas in all the private collection agencies' facilities. However, we determined that the IRS Facilities Management and Security Services office did not perform a physical security assessment of the private collection agencies' mailrooms or mail processing areas for three of the four private collection agencies.

Because the mailroom and processing areas are high-risk and the private collection agencies are receiving payments similar to those received by IRS lockbox sites, we determined that lockbox site guidelines should be added to the Facilities Management and Security Services office assessments. Lockbox site guidelines are very specific on security controls, such as separating mailroom processing from other business processes as well as security camera coverage and recording. Without assessing the security of the mailrooms and mail processing areas, the IRS may not realize the risk that taxpayer payments are vulnerable to theft. Ensuring that higher security standards are implemented in high-risk areas at the private collection agencies mitigates the risk of theft and ensures continued trust in the Private Debt Collection Program.

In addition, we determined that security over taxpayer misdirected payments needs improvement. During our site visit to a private collection agency, we observed a courier envelope containing taxpayer checks was left in an open wire tray on a file cabinet next to an exit door. We did not identify any security camera that monitored or captured video of the area, and the tray was not secure. The envelope remained in the tray unsecured until the courier came to pick it up. This same private collection agency had more than 63 employees with physical access to the mailroom where all incoming mail is processed. However, only 12 of the

[23] Internal Revenue Manual 10.2.14, *Methods of Providing Protection* (Aug. 17, 2016).

63 employees are authorized IRS contractor employees, and only three of the 12 contractor employees are approved to open IRS and taxpayer correspondence. Areas that receive taxpayer payments, even when unexpected, should enforce high security standards that are equivalent to other IRS sites that receive taxpayer payments. Payments that are left in an unsecured area create an opportunity for theft. During our review, we found that, from June through November 2017, all four private collection agencies received more than 200 "misdirected" payments totaling more than $150,000.

Additionally, we determined that private collection agencies should implement higher standards for security camera coverage of IRS contract areas, such as mailrooms, opening and printing of taxpayer correspondence, taxpayer payments received and sent to the IRS, and other areas with sensitive taxpayer data. Specifically, we found that one private collection agency did not provide security cameras in areas where taxpayer correspondence was received and letters were printed; sensitive shred documents were stored; and mail was transported, sorted, and delivered. We also identified that three of the four private collection agencies did not create and/or store backup video footage of IRS contract areas at alternate off-site locations. Without appropriate visual coverage for high-risk areas, the private collection agencies increase the risk that taxpayer data are exposed to potential loss, damage, theft, or destruction. Backup video recordings stored at off-site locations may help determine the cause or source of an incident that may happen at a facility. Without live backup data, it is difficult to determine if suspicious activities can be investigated immediately and action taken as necessary if taxpayer information is comprised.

The GAO found similar physical security control issues in two reviews. In its review of protecting sensitive financial and taxpayer data, the GAO found that the IRS had implemented multiple physical security controls at its enterprise computing centers to safeguard assets against possible theft and malicious actions. For example, the IRS implemented security measures to control physical access to restricted areas at its computing center with the use of badge sensors and keypads for card/Personal Identification Number credentialing. It also corrected a previously identified deficiency by ensuring that network equipment in restricted areas was housed in locked cabinets. However, the IRS had not corrected previously identified deficiencies regarding effectively reviewing access lists of individuals with an ongoing need to access restricted areas at two computing centers. The access lists continued to include individuals who no longer required access and who should have been removed from the lists. Because individuals may be allowed inappropriate access to restricted areas, the IRS has reduced assurance that its computing resources and sensitive information are protected from unauthorized access. In its review of the IRS's financial statements for Fiscal Years 2017 and 2016,[24] the GAO found control deficiencies relating to the ineffective implementation and monitoring of certain controls designed to safeguard and prevent unauthorized access to IRS facilities.

[24] GAO, GAO-18-165, *FINANCIAL AUDIT: IRS's Fiscal Years 2017 and 2016 Financial Statements* (Nov. 2017).

Systems access controls

System access controls is a policy that is uniformly enforced across all subjects and objects within the boundary of an information system. The access management process is responsible for allowing users to make use of information technology services, data, or other assets. Access management helps to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify them. Access management implements the policies of information security management.

In Fiscal Year 2018, TIGTA and the GAO conducted four audits covering system access controls. We conducted an audit of High Value Assets.[25] The Department of the Treasury notified the IRS that two of its systems were identified for inclusion in a Top 10 list of Department of the Treasury High Value Assets. We determined that the IRS cannot readily identify all individuals who have privileged access to its High Value Asset components because it did not maintain a complete inventory list of privileged users and accounts for the systems as of March 1, 2017. The two High Value Asset system security plans identified 13 hardware components comprising of 37 servers (including virtual, partitioned, systems development, testing, and disaster recovery servers). It took the IRS more than three months to provide a partial list of privileged users and accounts for only 10 (30 percent) of 33 servers.[26] Given that the IRS has been unable to provide this basic but critical information, we question whether the IRS has sufficiently inventoried, validated, and minimized the number of privileged users and accounts as required by the OMB Cybersecurity Strategy and Implementation Plan or complied with its own requirements to review privileged accounts semiannually.

To gauge the population scope and the time required to determine whether the privileged users are authorized, we conducted an initial assessment on September 14, 2017, of the partial list provided to us by the IRS. In our analysis of nine of the 10 servers, for the two High Value Asset systems for which data were provided, we identified 1,053 users approved for privileged access. Due to the volume and manual process necessary to verify whether a user is authorized and approved to have privileged access to a specific server, we conducted limited testing in this area by selecting a judgmental sample[27] of 10 privileged users for review. We found that the user role for all 10 privileged users were authorized and approved on a privileged role request form and on the Online 5081 system.

In addition, the Enterprise Operations organization stated that it does not maintain historical information on nonproduction servers, only the current state of users having privileged access. This is concerning because live taxpayer data can be maintained on these servers. While historical information of privileged users and accounts on production servers is maintained, the IRS was unable to provide us privileged users and accounts information for two production

[25] TIGTA, Ref. No. 2018-20-029, *Security Over High Value Assets Should Be Strengthened* (May 2018).

[26] Four servers were retired: two virtual servers on December 13, 2011; one virtual server on May 16, 2012; and one production server on August 13, 2013.

[27] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

servers. Further, we gave the IRS another opportunity to provide current privileged users and accounts information. The IRS still took approximately one month to provide this information. A different methodology was used to generate the data, and complete source data were not provided to us. Because we were not provided complete source data, we could not determine their validity. As a result, we were unable to verify that the IRS has successfully taken steps to minimize the number of privileged users for its High Value Assets.

Privileged accounts are a known target for malicious actors. In the vast majority of security breaches, stolen credentials and privileged accounts continue to be the prime target for hackers because they unlock the access required to virtually exploit any part of an organization's network, including critical and sensitive data. Despite this, identifying and managing privileged users and accounts at the IRS still relies on manual, time-consuming tasks.

In our audit of active directory and Criminal Investigation computer rooms, we determined that Criminal Investigation does not have an automated process for discovering and disabling accounts. According to a Criminal Investigation system administrator, the manual process to review account inactivity is time-consuming, and Criminal Investigation is therefore not complying with policy to determine the period of account inactivity. As a result, Criminal Investigation cannot ensure that inactive accounts are disabled, quarantined, and removed within the appropriate time frames.

Additionally, we reviewed Criminal Investigation system settings governing account password and lockout policies and found that they are in compliance with current Internal Revenue Manual[28] requirements. However, when we evaluated accounts individually, we found 295 service account and 1,751 user account exceptions due to improper configurations. The service and user account policy exceptions we found in the Criminal Investigation active directory forest include: enabled service accounts are located outside the service accounts organizational unit (seven exceptions); enabled service accounts do not follow the proper naming standard (41 exceptions); enabled service account passwords set to not expire (247 exceptions); enabled user account passwords set to never expire (25 exceptions); and enabled user accounts are not required to use Smart ID card (1,726 exceptions).

Based on these results, we determined that Criminal Investigation is not effectively enforcing policy governing service and user accounts. Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network monitoring tools. Terminated contractor and employee accounts have often been misused in this way. This places Criminal Investigation's sensitive data at risk for loss, manipulation, and other unauthorized access.

Further, in its review of the IRS's financial statements for Fiscal Years 2017 and 2016, the GAO found control deficiencies in limiting or preventing unnecessary access to systems. Specifically, the GAO identified that IRS user account control settings were not in compliance with its policy,

[28] Internal Revenue Manual 10.8.1, *Information Technology Security – Policy and Guidance* (July 8, 2015).

authorizing officials did not review and appropriately restrict access to several user and service accounts, the IRS did not consistently implement its policies for controlling access on the servers supporting several key financial systems, and the IRS did not correct a previously identified control deficiency concerning segregation of duties in which certain IRS employees continued to have both security and nonsecurity access roles to a key financial system.

In the GAO review of protecting sensitive financial and taxpayer data, the GAO found that the IRS had improved enforcing password complexity for several user and system-level accounts on various servers and by setting password expiration parameters for user and service accounts on several servers and databases. The IRS also corrected four of 22 control deficiencies, *e.g.*, restricted unnecessary user access on Oracle databases and restricted excessive user privileges by limiting users' ability to enter certain database commands.

Nevertheless, deficiencies persisted. For example, the IRS did not: enforce password expiration limits for several applications reviewed; enforce minimum password lengths for service accounts supporting several applications reviewed; enable certificate revocation lists to check Smart ID certificates for user authentication to a financial system; enter correct expiration dates for contractor employee passwords for 10 contractor profiles in production and 197 contractor profiles in the test environment of the mainframe, *e.g.*, expiration dates that extended beyond the end of the contract period of performance; and maintain and approve authorizations for 20 nonunique accounts that were used for its training environment. Until the IRS fully remediates these control deficiencies, it is at increased risk that controls could be compromised, permitting unauthorized access to its systems and data.

Authentication controls

Identification is the process of distinguishing one user from others as a prerequisite for granting access to resources in an information system. User identification is important because it is the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of a user identification is typically not protected. For this reason, other means of authenticating users, *i.e.*, determining whether individuals are who they claim to be, are typically implemented.

TIGTA and the GAO conducted four audits covering user and taxpayer authentication during our review period. We conducted an audit of electronic authentication[29] (hereafter referred to as eAuthentication) and found that the IRS has taken a number of steps to provide for more secure authentication. Following the discovery of unauthorized access to the Get Transcript application in May 2015, the IRS redesigned its eAuthentication process to provide multifactor remote authentication techniques for its online applications that contain sensitive information. In particular, the IRS improved its authentication processes to achieve compliance with the NIST

[29] TIGTA, Ref. No. 2018-20-007, *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented* (Feb. 2018).

Special Publication 800-63-2, *Electronic Authentication Guideline*, Level 3 standards[30] that require multifactor (at least two-factor) authentication to create a user profile. Two-factor authentication requires additional credentials beyond username and password for gaining access to the application. The IRS's new Level 3 authentication involves verification using financial information and having a text-enabled mobile phone associated with the profile. Users must receive a security code text to complete the identity validation process and when returning to access their profiles. The security code is sent to the mobile phone of record (something the user possesses) to verify account access authorization. Users without a text-enabled phone are issued a mailed activation code to the address of record. Upon receipt, the users can complete the identity validation process.

The IRS calls its new means to authenticate and authorize online users "Secure Access eAuthentication," which it describes as a rigorous identity verification process that helps protect taxpayer data and IRS systems from automated cyberattacks. Before accessing certain IRS online self-help tools, users must first register through Secure Access eAuthentication and authenticate their identities. Thereafter, each time registered users return to the tool, they must enter both their credentials (username and password) and a security code sent via mobile phone text. This enhanced eAuthentication solution is currently used for five online applications.[31]

However, eAuthentication control enhancements to improve the prevention of improper profile creation and unauthorized access to tax data were not fully effective. Specifically, controls did not always prevent improper creation of profiles. The IRS stated that it implemented a control enhancement in July 2015 to enforce a relationship of one Taxpayer Identification Number (TIN) to *************************************2*************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
****2****.

We reported this information to the IRS on March 28, 2017. The IRS officials responded that they were aware of the deficiency, and subsequently indicated that they had corrected it on May 14, 2017. However, we are concerned about the IRS's ability to test and monitor enhanced

[30] While this report was being drafted, the NIST released the final version of NIST Special Publication 800-63-3, *Digital Identity Guidelines*, in June 2017. The new guidance replaced NIST Special Publication 800-63-2. During the course of our review, the IRS indicated it would work to ensure that it is compliant with the new guidance once issued. We plan to review the IRS's implementation of the new guidance in a subsequent audit.

[31] The five online applications that use eAuthentication are Get Transcript, Identity Protection Personal Identification Number, Online Payment Agreement Individual Master File, Online Account – View Payment Status and History, and Taxpayer Digital Communications.

application controls based on the amount of time it took to discover and correct this deficiency. *************************************2************************************ *************************************2************************************ ****2****. However, it took almost two years for the IRS to discover and address the deficiency in the control's effectiveness.

In our Transcript Delivery System audit, we found that the processes and procedures to authenticate eServices users, including those users accessing the application, do not comply with Federal Government information security standards. For example, the IRS continues to use single-factor authentication to authenticate users despite the IRS performing a risk assessment, in both Calendar Years 2011 and 2015, rating the level of assurance at a NIST Level 3, multifactor (at least two-factor) authentication.

When we discussed this noncompliance, IRS management indicated that they originally intended to have eServices, including the Transcript Delivery System application, use the same two-factor authentication processes that were implemented in May 2016 in response to the Get Transcript breach. However, IRS management indicated that during the testing of implementing two-factor authentication for eServices, the IRS identified unexpected barriers. These barriers included that other IRS applications would be impacted by the two-factor authentication requirements, and the IRS needed additional time to identify a solution. In addition, external stakeholders raised concerns that users would be unable to receive the confirmation codes via text message because some businesses do not allow employees to have their personal cellphones at work. Therefore, IRS management indicated that they proceeded with implementing an interim solution. IRS management stated that they were not foregoing the implementation of two-factor authentication but rather were ensuring a successful implementation for both the IRS and its external stakeholders.

We also found that management did not ensure successful implementation of interim authentication requirements. In an effort to improve authentication, the IRS implemented an interim process that required existing eServices Transcript Delivery System users to reauthenticate their identity. These interim requirements subjected existing users to more rigorous identity proofing. It should be noted that, although these interim requirements strengthened identity proofing, they still did not meet the standard for multifactor authentication as required by the NIST. On November 29, 2016, the IRS published an important update about eServices on its public website.[32] The update notified Transcript Delivery System users that they would receive letters by mail with instructions on how to reauthenticate their identity. During the first two weeks of December 2016, the IRS sent letters to users that requested tax transcripts or updated their eServices account between October 2015 and November 2016. The IRS considers these users to be active users. These letters instructed the users that reauthentication was required to be completed within 30 days or access to eServices would be revoked. Users were provided with three options to reauthenticate: visit www.IRS.gov/transcript and complete

[32] www.IRS.gov.

the "Get Transcript Online" registration; call the eServices Help Desk with the notification letter in hand; or visit an IRS Taxpayer Assistance Center and verify their identity in person.

Our analysis of tax transcript request logs from October 1, 2015, to March 31, 2017, identified 4,022 eServices Transcript Delivery System users that requested tax transcripts were not sent a letter to notify them of the new interim authentication requirements. This occurred because management did not ensure that all users were identified and sent notification letters. As a result, 1,507 of the 4,022 users continued to request a total of 96,639 tax transcripts without being required to reauthenticate in compliance with the interim requirements; consequently, tax account information for 17,792 taxpayers was disclosed without proper authorization.

In addition, management did not ensure that eServices Transcript Delivery System users that did not complete the required interim authentication had their privileges revoked. Our review identified that 138 users (134 Income and Verification Express Services participants and four Electronic Return Originators) failed to reauthenticate, but their accesses to eServices were not revoked as required. Subsequent to February 5, 2017, the date when these users' privileges should have been revoked, the 134 Income and Verification Express Services participants and four Electronic Return Originators requested 29,163 and 16 tax transcripts, respectively.

We also conducted an audit of the Electronic Federal Payment Posting System.[33] The IRS uses the Electronic Federal Payment Posting System to process and record Electronic Federal Tax Payment System (EFTPS) payments. The EFTPS processes payments initiated via other payment methods that do not require a taxpayer to be enrolled in the EFTPS to submit their payment. These additional payment methods include the Direct Pay System, accessed through IRS.gov, with which individual taxpayers[34] can make payments to the IRS from their bank account, and the Credit and Debit Card Payment application with which taxpayers can pay when filing a return or in response to a bill or notice using a credit and debit card payment processor. The payment processor validates the taxpayer's TIN with the IRS through the Department of the Treasury's Financial Agent. Once a TIN is validated, the payment processors prepare a payment file for processing through the EFTPS.

We identified that strengthened authentication is needed to mitigate potential misuse of the ****************2****************. Specifically, ************2************** are required to provide ************************2***************************** to the IRS for use in validating payments. In response, *****************2***************** *****************2**************** it verifies as valid. The authentication criteria used for credit and debit card processors is significantly inconsistent when compared with the extensiveness of the authentication processes used to validate taxpayer payments submitted through the EFTPS or the Direct Pay System. For example, payments initiated in the EFTPS

[33] TIGTA, Ref. No. 2018-40-031, *Proactive Processes to Identify and Mitigate Potential Misuse of Electronic Payment Systems Are Needed* (Apr. 2018).

[34] Business taxpayers are not eligible to make payments through the Direct Pay System.

require enrollment, and the taxpayer must provide entity information including their TIN, name, telephone number, and contact information. After the IRS validates enrollment entity information, the IRS mails a Personal Identification Number to the taxpayer's address of record. To submit payments, the taxpayer is required to provide his or her TIN, EFTPS Personal Identification Number, and a password he or she established as part of the enrollment process. The IRS uses this information to authenticate the taxpayer. However, the Direct Pay System does not require enrollment and only requires taxpayers to verify their identity by providing their name, TIN, filing status, date of birth, and address, when making a payment.

Of additional concern is the fact that unscrupulous individuals can use *********2*********** *****************2*********************. For example, an unscrupulous individual can **************************************2************************************ **************************************2************************************ **************************************2************************************ *****************2****************************** transactions made between September 29, 2016, and December 14, 2016, identified potential misuse of this payment process. We identified 1,236 small-dollar payments with amounts ranging from ******2****** *****************2*****************. Although the TINs associated with these 1,236 payments were confirmed by the IRS's systems as valid, a total of 1,084 (88 percent) of the payments could not post to an associated tax account on the IRS's Master File because there was no active tax account for the taxpayer. For the remaining 152 payments, the payments posted to the taxpayer's account, but there was no amount owed by the taxpayer. Both scenarios raise a concern as to the potential misuse of the payment process as it brings into question why a taxpayer would submit a payment on a tax account for which they had no recent tax return filings or when no amount was owed.

When we discussed our analysis with IRS management, they acknowledged that the payments we identified were questionable. Management stated that they began updating *****2***** ****2**** validation requirements in Calendar Year 2016 to include requiring taxpayers to provide their ********2******** for authentication. On March 30, 2017, the IRS advised us that the new credit and debit card validation requirements were scheduled for implementation in January 2018. However, on October 5, 2017, IRS management stated that they ******2******* **************************************2************************************ **************************************2************************************ **************************************2************************************ . The delay will allow the ***********2************ time to update their processes to comply with these new validation requirements.

IRS management explained that the *********2**************plays a major role in the card processors' ability to accept tax payments from taxpayers who have chosen this as the payment option. However, the volume of payments received using the *********2********** ******2******* is minimal when compared to those ***************2***************** *********************2**********************. The IRS received more than 6 million

***********2*********** totaling more than $5.9 billion in Calendar Year 2016. Of these, the IRS reported that 888,703 (14 percent) payments totaling more than $422 million (7 percent) were received through the *************2**************.

Although the IRS initially identified concerns regarding the potential misuse of this payment process in Calendar Year 2015, some three years later, the IRS still has not taken the necessary actions to reduce the ability of unscrupulous individuals to use this system to potentially commit fraud. With the risks associated with tax fraud involving identity theft and how it is evolving and becoming more complex, delaying the implementation of authentication-strengthening processes continues to be a concern. IRS management noted that for the 2018 Filing Season, they will monitor credit and debit card payments to identify any suspicious payments.

The GAO conducted a review of taxpayer authentication[35] and found that, while the IRS has made progress on monitoring and improving authentication, including developing an authentication strategy with high-level strategic efforts, it has not prioritized the initiatives supporting its strategy nor identified the resources required to complete them. Doing so would help the IRS clarify relationships between its authentication efforts and articulate resource needs relative to expected benefits.

The GAO also found that the IRS can further strengthen authentication to stay ahead of fraudsters. While the IRS has taken preliminary steps to implement the NIST's new guidance for secure digital authentication, it does not have clear plans and timelines to fully implement it by June 2018, as required by the OMB. As a result, the IRS may not be positioned to address its most vulnerable authentication areas in a timely manner. Further, the IRS lacks a comprehensive process to evaluate potential new authentication technologies. The best authentication approach relies on multiple strategies and sources of information, while giving taxpayers options for actively protecting their identity. Evaluating alternatives for taxpayer authentication will help the IRS avoid missing opportunities for improving authentication.

Identification and protection of system boundary components

NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires that agencies must establish, maintain, and update an inventory that contains a list of all programs and information systems identified as collecting, using, maintaining, or sharing Personally Identifiable Information. Agencies cannot begin efforts to fully protect its information technology systems if system boundary components are not accurately identified and inventoried. Failure to maintain a correct inventory of all components within the authorization boundary increases the risk of having insecure components that can introduce vulnerabilities into the system. Boundary protection controls the logical connectivity into and out of networks and to and from devices attached to the network. Unnecessary connectivity to an organization's network increases not only the number of access

[35] GAO, GAO-18-418, *IDENTITY THEFT: IRS Needs to Strengthen Taxpayer Authentication Efforts* (June 2018).

paths that must be managed and the complexity of the task but also the risk of unauthorized access in a shared environment.

During Fiscal Year 2018, TIGTA and the GAO conducted five audits covering the identification and protection of IRS system boundary components. In our audit of High Value Assets, we reviewed the system security plans for two High Value Assets dated November 9, 2016, and October 17, 2016, respectively, and found that not all system boundary components were accurately identified. In addition, one system security plan was not updated when a significant change was made to the inventory of components within the system environment. Specifically, a primary mainframe was replaced in December 2016, and the system security plan was not updated as required. Similarly, four servers were retired (two in December 2011, one in May 2012, and one in August 2013) but remain listed in the most current system security plan.

Additionally, the Customer Account Data Engine 2 database is not identified either as within or as an interconnecting system outside the system environment in both system security plans. However, it should have been identified as an interconnecting system in both system security plans. In November 2017, the IRS updated both system security plans to reflect the changes in the inventory of components we identified.

In an audit of the Cybersecurity Data Warehouse (CSDW),[36] we requested a comprehensive list of all system names that send taxpayer data to the CSDW, but the IRS did not maintain an inventory of those systems. To address our request, system administrators were able to provide a comprehensive list of Internet Protocol addresses that are transferring data to the CSDW. The system is divided into two data repositories. The first is the legacy CSDW system that receives system log data from 9,540 unique addresses. These addresses belong to network devices, such as firewalls, routers, or switches. The second repository receives transfers from an additional 181 addresses that are associated with IRS systems that contain taxpayer data used by the Cybersecurity Fraud Analytics and Management team for fraud analysis. We found host names for 179 of the 181 addresses of systems containing Personally Identifiable Information but not the specific systems. The system administrators could not identify the IRS systems comprising the 181 addresses associated with the fraud analysis repository. According to IRS personnel, they did not have the resources to maintain an ongoing list of systems transferring data to the CSDW. It was not until after the closing conference and the completion of our fieldwork that the IRS provided a comprehensive list and additional evidence for the identified systems that transfer data to the CSDW.

In addition, we initiated an audit of the IRS's contracted Integrated Enterprise Portal-Registered User Portal, which offers external web services to the public.[37] We found that improvement is needed to ensure that the information system component inventory is accurate and complete for

[36] TIGTA, Ref. No. 2018-20-030, *The Cybersecurity Data Warehouse Needs Improved Security Controls* (June 2018).
[37] TIGTA, Ref. No. 2018-20-036, *The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved* (July 2018).

the Integrated Enterprise Portal. We identified missing*****2****** for all **2** physical servers and **2** network devices that included hardware and ************2************* *****2*****. Additionally, ***************2************************************* ***************2************* were missing for some of the physical servers and network devices. During the audit, the contractor worked to locate all missing information on its inventory and admitted that correcting the inventory in the Configuration Management Database is largely a manual process. The contractor stated that this was the first time it had performed this type of inventory reconciliation.

We also identified that the Cybersecurity organization reported a similar issue in March 2015. The Integrated Enterprise Portal inventory did not include the level of detail necessary for tracking and reporting as well as did not include the necessary information to support component accountability. The report recommended that the authorizing official ensure that the inventory was accurate and appropriately updated when components were installed, removed, and updated. In April 2015, a Plan of Action and Milestones (POA&M) was created for this issue. In November 2015, after conducting a follow-up review, the Cybersecurity organization validated that the issue was closed. We reviewed the artifacts the Cybersecurity organization used to close the POA&M and found similar types of missing information that we found during our review more than a year later.

In its reviews of the IRS's financial statements for Fiscal Years 2017 and 2016 and protecting sensitive financial and taxpayer data, the GAO found similar deficiencies with the IRS's security management of its information systems and system boundary control. Specifically, system security plans for key IRS systems had not been updated to reflect the current system environment, and a contingency plan had not been fully updated to document the existence of a server that was added to the operating environment for one of its tax processing systems. In addition, the IRS did not correct previously reported boundary control deficiencies, such as not implementing access control lists on certain network devices to prevent unauthorized users from logging into the network devices and not ensuring that authenticated network protocols were being used on its network devices. Until the IRS corrects these deficiencies to its network boundaries, increased risk exists that its network devices and systems could be compromised, which could affect system availability.

System configuration and change management

Configuration management administers security features for all hardware, software, and firmware components of an information system throughout its life cycle. Effective configuration management provides reasonable assurance that systems are operating securely and as intended. It encompasses policies, plans, and procedures that call for proper authorization, testing, approval, and tracking of all configuration changes and for timely software updates to protect against known vulnerabilities. Ineffective configuration management controls increase the risk that unauthorized changes could occur and that systems are not protected against known vulnerabilities. The lack of effective change management increases the agency's risk that unauthorized changes can be made to applications that result in the loss of data or program integrity.

TIGTA and the GAO conducted coverage of system configuration and change management controls in four audits. In our review of the IRS's contracted Integrated Enterprise Portal-Registered User Portal, we found that high-risk configuration weaknesses were not always remediated and were not always timely corrected. We reviewed the contractor's ****2***** configuration compliance reports from February 2016 through May 2017 and identified a total of **2** high-risk configuration weaknesses. *******************2*********************** **2*************************************** ******************2**********************. We found that **2** (*2* percent) of **2** high-risk configuration weaknesses were not corrected as of May 24, 2017. Further analysis showed that these **2** configuration weaknesses **************2************** **2*************************************** ************************2**********************. The unique types of vulnerabilities include: 1) ******************************2*************************************** ****2***; 2) ************2**; 3) ****2***** **2*************************************** ************************2********************************; 4) **********2******** ************************2***************; 5) ***************2********************* **********; 6) **************************2************************************* *******************2****************************; and 7) *********2************ Protocol service was not disabled.

We also identified that the Cybersecurity organization reported some of the same unique types of vulnerabilities. The Cybersecurity organization identified **************2***************** **2*************************************** **2*************************************** **2***************** not found due to it being outside the review period, and we believe *****2**** due to the sampling methodology. The Cybersecurity organization recommended that the IRS's authorizing official ensure that configuration settings are configured to the most restrictive mode, enforced, and documented for all system components. The Cybersecurity organization also recommended ensuring that all vulnerabilities identified are reviewed, analyzed, and appropriately addressed.

The NIST requires an organization to review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses. In addition, the NIST requires that configuration change decisions associated with the information system be documented and retained.[38] Internal Revenue Manual 10.8.1 also requires the IRS to ensure that all business and functional unit owners use the

[38] NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (updated Jan. 2015); *Configuration Management, CM-3 (Configuration Change Control).*

FISMA guidance and standard operating procedures[39] for security configuration management. These procedures require that a security change request must be submitted for changes to existing information systems.

However, in our audit of the CSDW, we identified that the IRS did not follow its security change management process. Specifically, the IRS transferred transactional audit logs containing taxpayer data from the Get Transcript application into the CSDW without completing the change request process as required by Federal and organizational policies and procedures. The IRS submitted a security change request for review to the Security Change Advisory Board; however, the IRS did not complete the required tasks before it made a significant system change to the CSDW. IRS executives stated that transferring taxpayer data to the CSDW was essential to perform the fraud analysis that could prevent further security incidents involving the Get Transcript application, and therefore it did not prioritize the system documentation. As a result, the IRS did not follow established security control processes. Two years after the IRS decision to transfer taxpayer data to the CSDW, some controls remain weak and documentation is not complete.

Because the IRS did not follow established change management processes, the General Support System-1 authorizing official was unaware that the CSDW now stores taxpayer data for use in fraud analysis. During our fieldwork, we notified this official that Personally Identifiable Information is now housed within the CSDW. The IRS introduced new security weaknesses and risk to the CSDW when it began transferring taxpayer data from the Get Transcript application to the CSDW without following the established change management process. For example, if appropriate officials are unaware that Personally Identifiable Information has been transferred into a system that was not originally designed to protect it, they cannot adequately protect those data or take steps to prioritize necessary resources to appropriately manage the system from a security and risk perspective.

The GAO found similar issues. In its review of the IRS's financial statements for Fiscal Years 2017 and 2016, the GAO found that change control procedures were not properly enforced on mainframe systems that process tax and financial management data. In its review of protecting sensitive financial and taxpayer data, the GAO found that the IRS was unable to provide supporting documentation for 13 changes made to critical mainframe datasets. In addition, as in previous years, the agency continued to alter production data processing on the mainframe outside established change control procedures. The lack of effective change management increases the agency's risk that unauthorized changes can be made to applications that result in the loss of data or program integrity.

[39] *IRS Security Change Management Standard Operating Procedures*, Version 6.7 (August 20, 2012).

System scanning, vulnerability remediation, and patching

One of the basic tenets of network security is the periodic monitoring and scanning for network vulnerabilities and timely remediation of identified vulnerabilities in order to reduce the exposure of exploitation. The information technology landscape is dynamic and always evolving in order to become more efficient and secure. Hardware and software vendors are constantly identifying bugs and glitches within their components and issuing fixes to patch these weaknesses. Users must be diligent to identify weaknesses and take appropriate actions to minimize the chance of these weaknesses being exploited.

During Fiscal Year 2018, TIGTA and the GAO conducted six audits involving system scanning and vulnerability patching of IRS systems. In our audit of High Value Assets, we found that the IRS was updating and applying changes, *e.g.*, maintenance, fixes, modifications, and enhancements, to its mainframes in the Tier I environment that support the High Value Assets.[40] According to the IRS, the process to update and apply system changes to its mainframes is more structured than its Tier II environment servers. Updates with the changes to the IBM and Unisys mainframes are typically scheduled every two years by the vendors. For the IBM mainframes, the updates are tested by the vendor and released in a bundled package that is automatically applied to the mainframe in coordination with the IRS. For the Unisys mainframes, the updates are also tested by the vendor prior to release. From September 2015 to June 2017, there were four bundled updates consisting of 890 changes applied to the IBM mainframes and one operating system update and two bundled updates consisting of 60 changes applied to the Unisys mainframes.

However, the IRS did not effectively manage its patch management program in the Tier II environment. Specifically, the IRS was not capturing complete historical patch implementation data to help identify trends in managing its patch management program related to one of its High Value Asset's hardware components operating in the Tier II environment.[41] For example, while the IRS stated that it had metrics tracking the implementation of patches since December 2016, the IRS does not capture, verify, or maintain historical data on patch implementation dates of any active or retired servers or identify trends in the patch management program. As a result, the IRS was unable to provide us with complete patch information for each of the hardware components identified in the High Value Asset's system security plan. As of August 2, 2017, the IRS took more than three months to provide patch information for 14 (78 percent) of the 18 identified hardware components related to this High Value Asset.

The Enterprise Operations organization's Infrastructure Risk Analysis Section is responsible for program oversight of all nonexecution functions of patch management, which includes

[40] The IRS does not use the term "patching" to describe its Tier I mainframes but rather uses the terms "updates" and "changes." In addition, the IRS does not associate these updates and changes to a specific system but to the mainframe that supports these individual systems and applications.

[41] The High Value Asset's system security plan provides that its infrastructure does not operate in the Tier II environment, only in the Tier I mainframe environment.

generating patch schedules, notifications, coordination, and reporting. At the request of the TIGTA audit team, the Infrastructure Risk Analysis Section provided a newly created and still-under-development *Patch Implementation Report* for April 2017. No other metrics report regarding whether the IRS was complying with its 30-calendar-day requirement of patching critical and high-risk security patches existed prior to this *Patch Implementation Report*.

According to the IRS, to be compliant with the Internal Revenue Manual,[42] the report identified all patches released by vendors during the month of April 2017 as well as the number and percentage of outstanding and applied patches to the IRS's Tier II environment. The intended purpose of this report is to provide IRS management with a monthly status of the IRS's overall compliance with patch management. However, this report was not complete because it did not provide trends in patch compliance for patches released prior to June 2017 and it did not capture any patch implementation dates until July 2017. Based on the IRS not having an established process that measures patch management compliance and the fact that the report was newly created and still under development, our scope was limited to recent reports that contained the IRS patch implementation dates.

Based on our review of these reports, we found that the IRS was not always timely applying critical and high-risk security patches for one of its High Value Asset servers. In a *Patch Implementation Report* dated June 5, 2017, that included all outstanding patches,[43] the IRS reported that one of its High Value Assets had 77 outstanding security patches rated as critical and high-risk. Based upon our calculation between the patch release date and the date the report was created, our analysis determined that 37 (48 percent) of the patches were over-aged by an additional 25 calendar days.[44] These unpatched vulnerabilities related to servers running the Microsoft® Windows 2003 operating system. Without effective patch management program metrics, an organization cannot determine whether vulnerabilities are timely mitigated. Failure to timely remediate security vulnerabilities may allow known weaknesses to be exploited and could result in the loss or disruption of the High Value Asset or other systems that are critical to an organization's operations.

In our audit of active directory and Criminal Investigation computer rooms, we found that Criminal Investigation has successfully deployed the necessary tools and implemented procedures to detect software vulnerabilities and protect the domain controllers against malicious code. Criminal Investigation uses *******2******* as its primary enterprise vulnerability scanning tool. *****2********* uses the Common Vulnerability Scoring System, and its quantitative model ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.

[42] Internal Revenue Manual 10.8.50, *Information Technology Security, Servicewide Security Patch Management* (April 29, 2016).

[43] The *Patch Implementation Report* for April 2017 provided information on patches released by vendors only for the month of April 2017.

[44] The IRS considers any critical and high-risk security patches not applied within 30 calendar days over-aged.

We reviewed two ***2*** vulnerability reports, both dated December 5, 2017, for all Criminal Investigation domain controllers to evaluate the effectiveness of its vulnerability scanning program. The first report provided vulnerability rankings based on high, medium, or low vulnerability scores for each domain controller. We found that 74 (8 percent) of 981 entries were identified as medium-level vulnerabilities, with no high-, critical-, or low-level vulnerabilities identified. The second report showed limited historical information, such as first seen, last seen, last scan date, and remediation status. The first and last seen dates allowed us to determine previous scan dates. We found that scanning intervals between dates did not exceed two weeks, except in one instance. We also found 74 entries with medium-risk vulnerabilities that were not remediated; however, 70 of those entries were discovered only in the most recent scan.

Along with vulnerability scanning and remediation, the IRS is required to protect information systems from malicious code. Working with Criminal Investigation system administrators, we observed on-site that all domain controllers were up to date with antivirus malicious code protection and virus definitions that did not exceed 24 hours. All scans were dated within a week of the date we ran the report on-site.

However, we found that the Windows Policy Checker scans and reports of all Criminal Investigation domain controllers failed, with an average score of 63.76 percent as of August 3, 2017. The Windows Policy Checker is an application that validates applicable IRS security requirements on computers that use the Microsoft Windows operating system. According to the Windows Policy Checker user manual and reports, scores of 79 percent and below are not compliant and present a serious risk to the IRS. The IRS made a risk-based decision to continue use of Windows Policy Checker past its end-of-life in May 2016. That risk-based decision was granted until July 31, 2017. We ran a second round of reports on the domain controllers with a Criminal Investigation system administrator on December 6, 2017, which resulted in the same failing average score of 63.76 percent.

Criminal Investigation personnel told us that they submit their Windows Policy Checker reports monthly to the Cybersecurity organization. Cybersecurity organization personnel collect all Windows Policy Checker reports from various business units, consolidate the information, and then report them monthly to the Treasury Cyber Analysis and Reporting Dashboard. We received the Security Assessment Report showing that the IRS is aware of deficiencies with failing Criminal Investigation Windows Policy Checker reports; however, we found no evidence that the Cybersecurity organization provided feedback or guidance to the Criminal Investigation data owners of failing systems to take remediation action. By not providing feedback based on the Windows Policy Checker reports, including how to properly configure system components to the most restrictive settings for failing Criminal Investigation domain controllers, the IRS compromised the security posture of the system. A compromise can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and data exploitation, all of which compromise the integrity, confidentiality, and availability of the system.

Further, we found that the Windows Policy Checker itself is out of date. The current version of Windows Policy Checker was released December 2014. That release of Windows Policy Checker uses Security Technical Implementation Guidelines set by the Defense Information Systems Agency that are more than three years old to evaluate IRS systems. By comparison, the most current Security Technical Implementation Guidelines for domain controllers were released October 27, 2017. The IRS cannot provide relevant and timely continuous monitoring with an application so outdated. The IRS will be unable to continuously assess or analyze security controls and security risks to support organizational risk-based decisions by using outdated standards.

For our audit of the IRS's contracted Integrated Enterprise Portal–Registered User Portal, we found that vulnerabilities ******************2**************************************
********************2**********************. From the contractor's ***2*** vulnerability scan results for October 2016 and February 2017, we identified *2* systems and system components, *e.g.*, hypervisors, firewalls, and embedded systems, that were scanned in both reports. For these *2* systems and system components, the scan reports presented information on **2** vulnerabilities, *i.e.*, critical-, high-, medium-, and low-risk severity ratings, of which **2** (*2* percent) were remediated. Figure 7 provides the remediation status of the vulnerabilities by severity rating.

Figure 7: Remediation Status of ***2* Scanned Vulnerabilities by Severity Rating for October 2016 and February 2017**

2 Scan Vulnerability Severity Ratings	Vulnerabilities	Count and Percentage of Vulnerabilities Remediated		Count and Percentage of Vulnerabilities Not Remediated	
Critical	**2**	**2**	**2**	**2**	**2**
High	**2**	**2**	**2**	**2**	**2**
Medium	**2**	**2**	**2**	**2**	**2**
Low	**2**	**2**	**2**	**2**	**2**
Total	**2**	**2**	**2**	**2**	**2**

*Source: TIGTA's analysis of **2** scan results for October 2016 and February 2017.*

While the contractor can improve on its overall *2* percent remediation rate, we found that the remediation rate for the critical and high-risk vulnerabilities was at *2* percent (*****2*****
********************2***********). The remaining **2** vulnerabilities were not remediated between the completion scan dates of the two **2** vulnerability reports, totaling **2** calendar days. *********************2**************************************
***************************************2**************************************
***************************************2**************************************

***************************************2**************************************
************2**********

Based upon our results, the contractor explained that the **2**-identified critical severity vulnerabilities were reevaluated using the Cybersecurity organization's *********2*********
**********************2**********************. The matrix is based upon seven questions, *e.g.*, Is the vulnerability widely known?, Is the exploitation of the vulnerability being reported?, How many systems are vulnerable?, *etc.*, and a numeric rating range between one and 10 was considered to determine the overall severity rating for each question. Based upon the reevaluation, the contractor changed the severity ratings to *********2*********
*****2*****, *i.e.*, ***********************2**************************************
*********2***********. While we did not conduct a comprehensive and detailed review of each of the answers and the numeric ratings, we agreed with the reasoning for changing the severity ratings for **2** of the **2** critical vulnerabilities. However, we did not agree with changing the severity rating for ************2*************************************
2.

For the *2* high-risk vulnerabilities found on both the October 2016 and the February 2017 scan results, with the oldest vulnerabilities dating back to March 2013, we believe they should have been resolved long before February 2017. These *2* vulnerabilities stemmed from six unique vulnerabilities.[45]

Based upon our results, the contractor again reevaluated the high-risk vulnerabilities using the
***************************************2***************** Based upon the reevaluation, the contractor changed the severity ratings to medium for **2** high-risk vulnerabilities and low for **2** high-risk vulnerabilities, *i.e.*, ***********2***********
****2****. While we also did not conduct a comprehensive and detailed review of each of the answers and the numeric ratings, we generally agreed with the reasoning for changing the severity ratings for **2** of the **2** high-risk vulnerabilities.

However, we did not agree with changing the severity rating for *********2**********
***************************************2********. The contractor took 223 calendar days from the time the vulnerability reappeared to the date the contractor stated that it had resolved the vulnerability in May 2017. We reviewed the October 2016 Integrated Enterprise Portal Vulnerability Assessment report and found the following explanation on the delay in resolving this vulnerability: ****************2*************************************
***************************************2***************************************
***************************************2***************** Although the contractor noted in the Vulnerability Assessment report that **********2***********, the contractor did not provide a ***********2********** for our review.

[45] The unique vulnerabilities can be identified in multiple systems or system components.

Additionally, we are concerned with the timeliness to remediate the vulnerabilities, the oldest of which was initially discovered in March 2013. While the contractor provided some ***2*** and we observed a reference to a POA&M, the contractor did not account for the length of time spent remediating these vulnerabilities.

In our private collection agency audit, we found that the IRS is not ensuring that private collection agencies are performing complete monthly vulnerability scans and reviewing the scan results. We requested three consecutive months of vulnerability scans for the months of April through June 2017 from the four private collection agencies. However, one of the four private collection agencies could not provide us scans for three consecutive months. We notified the IRS of the situation; it was not aware of the private collection agency scanning issue.

In addition, one of the four private collection agencies provided us with the scan result for only one workstation for the month of July. Although the IRS required that monthly scans be performed by the private collection agencies, we determined that the IRS is not regularly reviewing the scan results. The IRS reviewed the results of the private collection agency vulnerability scans only during its on-site annual assessments of the private collection agencies. As a result, the IRS was unaware of any of the issues we identified. Hackers find weaknesses and flaws in those devices that are connected to the network. As a result of this lapse in vulnerability scanning, taxpayer data at the private collection agencies were at risk and could have been compromised.

We also found that the IRS is not requiring and enforcing timely remediation of critical and high-risk vulnerabilities. We analyzed two consecutive months of vulnerability scans for both servers and workstations to determine if the private collection agencies were timely remediating the vulnerabilities. Figure 8 shows the unique critical and high-risk vulnerabilities identified on servers and workstations not remediated within the required 30-calendar day time frame.

Figure 8: Private Collection Agencies' Unique Critical and High-Risk Vulnerabilities Not Remediated Within 30 Calendar Days

Private Collection Agency (in random order)	Servers (Critical and High-Risk)	Workstations (Critical and High-Risk)
Private Collection Agency #1	67	260
Private Collection Agency #2	3	0
Private Collection Agency #3	85	Data Not Provided
Private Collection Agency #4	0	0

Source: TIGTA's analysis of two consecutive monthly scans for private collection agencies' servers and workstations from April to October 2017, depending on the availability of reports for each private collection agency.

Our review determined that only one of the four private collection agencies remediated all critical and high-risk vulnerability factors identified during the two months reviewed. The other three private collection agencies had vulnerabilities which were not remediated within the required 30 calendar days. Known exploits exist for a large number of these vulnerabilities, which could lead to the exposure of Personally Identifiable Information as occurred when Equifax did not patch its vulnerabilities in a timely fashion.

Additionally, we found that the IRS is not informed of the private collection agencies' security postures. During our visitations, we requested the POA&Ms from the four private collection agencies. Two of the four private collection agencies did not have a POA&M because all issues found during the IRS annual assessment were corrected prior to our request. The other two private collection agencies provided us with a POA&M. We determined that the first private collection agency had corrected its critical and high-risk vulnerabilities. The second private collection agency did not correct the critical and high-risk vulnerabilities within the required 30 calendar days, and the vulnerabilities remained on its POA&M for several months after the IRS performed its assessment.

Private collection agencies are required to perform monthly vulnerability scans as part of continuous monitoring, but identified issues are not required to be listed on a POA&M and tracked. As a result, the IRS would be unaware of any vulnerabilities identified during monthly scanning on the private collection agencies' machines until the annual or any follow-up visitations. The private collection agencies are not required to send any reports or notification of their monthly scans to the IRS nor report the vulnerabilities and the number of machines affected. Therefore, we believe the current requirements do not ensure that the IRS is adequately informed about the true security posture of the private collection agencies.

Moreover, one of the four private collection agencies initially provided us with a high-level overview presentation of vulnerabilities on its computer systems instead of its raw scan data. We compared the presentation data to the raw scan data that the private collection agency provided and identified a large discrepancy between the vulnerabilities reported to the IRS and the total number of vulnerabilities on its systems. We determined that the private collection agency was reporting the number of vulnerabilities; however, it did not detail the number of machines each vulnerability affected. For example, if the private collection agency reported one critical vulnerability, that one vulnerability could actually be present on 30 servers, which significantly increases the risk than if it was a single instance in the server environment.

Figure 9 reflects the results of our analysis of two months of private collection agency–provided raw scan data to identify the unique vulnerabilities and the actual number of instances that those vulnerabilities were present in the server environment.

Figure 9: Actual Number of Vulnerabilities for the Private Collection Agencies

Private Collection Agency (in random order)	Month One Unique Vulnerabilities	Month One Instances in the Server Environment	Month Two Unique Vulnerabilities	Month Two Instances in the Server Environment
Private Collection Agency #1	15	27	25	85
Private Collection Agency #2	9	37	1	3
Private Collection Agency #3	49	339	42	188
Private Collection Agency #4	10	19	3	5

Source: TIGTA's analysis of monthly vulnerability scans provided by the private collection agencies from April to October 2017, depending on the availability of reports for each private collection agency.

The unique vulnerabilities are a combined total of both critical and high-risk vulnerabilities that need to be corrected within 30 calendar days. Figure 9 shows a significant difference when the vulnerability is applied to the number of affected machines in the server environment. Knowing how widespread the vulnerability is throughout the components that are used for the IRS contract gives a better picture of the private collection agencies' security postures. With this information, the IRS knows the risk involved with its data at the contractor sites.

The GAO also found issues with the IRS not applying updates to software in its review of the IRS's financial statements for Fiscal Years 2017 and 2016. Specifically, the IRS did not apply vendor-supported software updates on certain databases, servers, and network equipment that support its financial systems. Such control deficiencies increase the risk that unauthorized personnel can leverage known information security vulnerabilities and gain access to key systems and network equipment.

In the GAO's review of protecting sensitive financial and taxpayer data, it found that the IRS had not installed critical patch updates to a recently upgraded database supporting an important IRS information system, nor had the IRS addressed deficiencies related to installing critical patch updates identified in prior years. Specifically, the IRS still had not applied critical security patches to databases supporting five information systems, including its personnel and payroll system, or to servers supporting eight information systems, including its general ledger system. In addition, the IRS continued to rely on database software that was no longer supported by the vendor. Such reliance is problematic because vendors generally do not provide updates for unsupported software even if vulnerabilities are known. By not installing patches and replacing unsupported software per its own requirements, the IRS has increased the risk that individuals may exploit known vulnerabilities in its systems.

Network monitoring and audit logs

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. Audit and monitoring controls can help information systems security professionals routinely assess computer security, recognize an ongoing attack, and perform investigations during and after an attack.

In Fiscal Year 2018, TIGTA and the GAO conducted four audits in the areas of network monitoring and audit logging and reviews. In the eAuthentication audit, we found that the IRS has taken a number of steps to enhance its network monitoring and audit log analysis capabilities. Specifically, the IRS enhanced its network monitoring controls at the IRS.gov portal that were needed to help identify and block malicious activity. The IRS also enhanced its capabilities to aggregate and correlate system audit logs across different systems. The IRS is able to stream the eAuthentication log data to its CSDW and hired a contractor to analyze anomalous log activity as part of its Cyber Fraud Analytics group. The scope of the work performed by the contractor includes using advanced analytic techniques to prevent and detect fraudulent activity in IRS online applications. The contractor has been tasked with conducting complex analytics on large transactional data sets to identify anomalous patterns in activity and building and refining predictive models to classify or identify anomalous transactions.

In addition, the Cyber Fraud Analytics group developed a tool that searches the log data for suspicious activities and potentially fraudulent behavior. ***************2*************** ***************************************2************************************** *********2********. Using this tool, the Cyber Fraud Analytics group identified fraudulent activity in which individuals improperly used data stolen from sources outside of the IRS to successfully perpetrate a small number of targeted attacks.

While the IRS took actions to enhance controls and security, more work is needed to fully implement the security improvements the IRS indicated were completed since the Get Transcript breach in May 2015. We found that, while the IRS has implemented the enhanced controls related to network traffic, such as network activity rate controls, increased detection via perimeter controls, and filtering of suspicious Internet Protocol addresses, it has not fully completed implementation of other controls specific to analyzing network activity in real time and identifying automated attacks. **********2************************************** ******2*******.

***************************************2************************************** ***************************************2************************************** ***************************************2************************************** *********2*********. The IRS receives weekly status reports from the contractor implementing these security improvements, but a more formalized process for identifying needed tasks, establishing milestones, and detailing required resources would be beneficial. For example, creating a POA&M, which includes these items, would ensure proper tracking and management visibility of the remaining issues that need to be addressed. A POA&M would also allow management to determine and direct the resources needed to address the issues timely. If automated attacks are not prevented, more taxpayer records could be compromised and revenue lost to identity theft refund fraud.

In addition, based on our review and analysis of the eAuthentication audit logs, we believe limitations with the log data may have contributed to the IRS's difficulty in ensuring that controls were effective. The eAuthentication audit logs contain key data, but much of it is combined into one field such that to make it usable for analysis would require extra time and effort to extract the key elements. We had to perform this work of extracting key elements prior to running our tests, which determined that the IRS's enhanced controls were not fully effective.

2*************************************
2*************************************
2*************************************
2*************************************
2*************************************
2*************************************
2*************************************
2*************************************
2*************************************
*******2******. Without adequate and readily usable audit logs or other means to sufficiently test and monitor controls, the IRS may not discover control deficiencies in a timely manner. If controls are not effective in stopping unauthorized activities, more taxpayer records could be compromised and revenue lost to identity theft refund fraud.

We also found that requirements for monitoring audit logs for suspicious activity were not being fulfilled. Although the Security Operations organization generated and e-mailed unusual activities reports of exceeded thresholds to the eAuthentication application owner and indicated that a response was required, the application owner did not review the reports or provide a response. The Security Operations organization did not follow up on why a response was not provided, indicating to us that the report generation and review process was still being developed. Our review of the unusual activity reports that were generated through the contractor identified that key data were still left combined into one field and, therefore, these reports were not readily useful for review, analysis, or after-the-fact investigations of user activity. This lack of usefulness may have contributed to the application owner's failure to review them.

In June 2017, the application owner assigned staff to begin reviewing the reports e-mailed by the Security Operations organization. However, a reviewer indicated that instructions were needed on what to do with the suspicious activity once identified. ******************************
2*************************************
*************************2************************. The lack of the capability to

generate reports from the eAuthentication audit logs that readily support on-demand audit review, analysis, and after-the-fact investigations of incidents reduces the IRS's ability to discover and address malicious activity and to determine the effectiveness of eAuthentication controls in a timely manner. In addition, not reviewing the unusual activity reports or not conducting adequate and timely follow-up on the identified suspicious activities could lead to taxpayer records being compromised.

Further, we found that the criteria used to generate certain reports was not reviewed or updated. IRS policy requires auditable events to be reviewed and updated at a minimum of every two years. However, the IRS could not demonstrate that this was done in the case of certain auditable events in the eAuthentication Audit Plan as required. It is the responsibility of various parties, including the Security Operations organization, eAuthentication's owner, and the program management office, among others, to meet and review this information. Failure to do so could result in criteria being obsolete, which would limit the effectiveness of the reports being generated.

Our analysis of approximately two months of daily unusual activity reports showed that some specific threshold amounts were not exceeded at all or by very minor amounts, while others were exceeded by very large amounts. This discrepancy indicates that the individual thresholds may be either too low or too high and, therefore, need to be reviewed to ensure their usefulness. The usefulness of the generated reports is in question given the potentially outdated thresholds and the lack of a readily available means to review the underlying data.

*************************************2************************************ **************************2*************************. The IRS indicated that it had implemented new controls to block excessive attempts in Calendar Year 2014 and further strengthened them in Calendar Year 2016. However, instances of excessive activity still appear on the unusual activity reports. This could indicate that some controls are not working as intended or that event thresholds are inappropriate and outdated. This further reinforces the need to review the unusual activity reports and ensure that the thresholds triggering report generation are appropriate and kept up to date. Without periodically reassessing which events are captured and keeping the event thresholds triggering report generation current, the reports being produced may lose their usefulness. If the reports being produced have limited usefulness, the IRS will be unable to effectively investigate and respond to suspicious activities.

In our audit of the CSDW, we found that audit trails were not implemented. At the beginning of our audit, the IRS had not implemented complete audit trails and security controls for the CSDW. The IRS must be able to monitor fraud analysts who have access to taxpayer data, as well as CSDW system administrators, for unauthorized access. According to IRS personnel, they only had the capability to capture basic information, such as who and when the user accessed the CSDW. Auditing controls were not in place for the CSDW because the system was not originally designed to process and store taxpayer data; therefore, granular auditing controls and capabilities were limited. As of December 2017, the IRS took steps to begin capturing the activities performed by Cybersecurity Fraud Analytics and Management analysts and CSDW system administrators with access to taxpayer data by deploying a tool that has the capability to record activities in searchable audit trails. The tool captures the activities data necessary for user profiling and enables full user session details for forensic investigations. However, the IRS has not established a review process for the tool-generated data, and there is currently no timeline for when monitoring will begin. In addition, although IRS executives stated that the CSDW was the only system available for immediate use at that point in time to process taxpayer data following the Get Transcript application security breach, no formal risk assessment or business case was documented, and other known systems already housing Personally Identifiable Information with built-in audit trails were not considered.

With limited audit trails in place to capture and record Cybersecurity Fraud Analytics and Management analyst and system administrator activities on the CSDW, the IRS lacks the full capability to monitor or perform periodic reviews of these activities. The IRS is at risk of being unable to identify employees who have violated the Taxpayer Browsing Protection Act[46] and the IRS's unauthorized access policy. Further, the lack of auditing controls hinders IRS management's ability to enforce unauthorized access policies.

Similarly, the GAO found continuing and additional monitoring control deficiencies involving certain key financial reporting systems in its review of the IRS's financial statements for Fiscal Years 2017 and 2016. For example, the IRS's monitoring processes had not identified user account control settings that were not in compliance with its policy. In addition, the IRS was unable to detect changes made to its mainframe systems, including changes made in a nonproduction test environment that affected controls in the mainframe production system. These deficiencies limit the IRS's ability to detect and respond to unauthorized access or unusual activity affecting its financial reporting systems.

In its review of protecting sensitive financial and taxpayer data, the GAO also found that the IRS has made limited progress in enhancing its audit and monitoring capabilities. For example, the IRS corrected three previously identified weaknesses by reconfiguring the audit trails for several of its databases supporting three applications to enable the reconstruction of specific actions. Nevertheless, deficiencies persist, and the IRS had not fully implemented seven of the 12 recommendations the GAO had previously made to correct deficiencies identified in audit and monitoring controls.[47] For example, the IRS had not enabled database logging, nor reviewed, analyzed, or reported auditable and actionable events on a database supporting a tax payment

[46] 26 U.S.C. §§ 7213, 7213A, and 7431 (2013).

[47] As of September 30, 2017, the GAO determined that the IRS had addressed four of the 12 recommendations. For seven of the remaining eight recommendations, the IRS had not completed corrective actions. As for the remaining recommendation, the GAO determined that it was no longer relevant due to the changing operating environment and issued a new specific recommendation that more accurately reflects addressing the associated deficiency in the current environment.

system. In addition, the IRS did not consistently detect improperly configured encryption settings for user and service accounts or detect configuration changes made to the mainframe.

System security documentation

The documentation of system security is an important element of information security management for an organization. During Fiscal Year 2018, TIGTA and the GAO conducted four audits with coverage on security documentation. In our eAuthentication audit, we found that the IRS completed or reassessed the eAuthentication risk assessments for its online applications. The IRS wants its online applications to use the appropriate level of assurance to conduct identity proofing that is required to protect the sensitivity of data being shared with taxpayers. The IRS implemented an eAuthentication risk assessment process that it completes for each new online application or when there is a change made to an application. The IRS indicated that it will renew all eAuthentication risk assessments annually to ensure that the identified assurance level remains consistent with the application's online risk profile and any applicable policies. The IRS completed or updated eAuthentication risk assessments for 28 of its online applications.[48]

However, in our audit of the CSDW, we found that the IRS did not conduct and document a risk assessment nor update key security documentation when it transferred taxpayer data into the CSDW. The purpose of a risk assessment is to inform decisionmakers and support risk responses by identifying threats, vulnerabilities, potential for exploiting threats, and the likelihood of harm resulting from those threats. Without a complete risk assessment document, there is an increased risk that the IRS would be unable to identify relevant threats to the organization. Further, the IRS may be unaware of internal and external vulnerabilities that could negatively impact the organization.

In addition, the IRS Security Change Advisory Board reviewed the change request for transferring taxpayer data to the CSDW and determined that additional tasks required completion prior to the data transfer. The Security Change Advisory Board specified that security artifacts, specifically the CSDW system security plan and privacy impact assessment, be updated. However, the IRS did not update either document to reflect the inclusion of taxpayer data as directed. The most recent system security plan dated March 31, 2017, states that the CSDW does not contain taxpayer data even though data transfers of Personally Identifiable Information began in April 2016. The IRS also did not update the CSDW privacy impact assessment. A privacy impact assessment should be performed before developing or procuring information systems or initiating programs or projects that collect, use, maintain, or share Personally Identifiable Information and be updated when changes create new privacy risks. During our

[48] Some of these online applications include: Affordable Care Act Information Returns; Federal Student Aid – Datashare; First Time Home Buyer Credit Account Lookup; Foreign Accounts Tax Compliance Act; Get Transcript; IRS Direct Pay; Online Account – View Payment Status/History; Where's My Amended Return?; and Where's My Refund?

fieldwork, the IRS updated its CSDW privacy impact assessment effective September 18, 2017, which now states that the system contains Personally Identifiable Information including, name, date of birth, and other tax account information.

In the GAO's review of protecting sensitive financial and taxpayer data, it found that the IRS corrected a previously identified weakness by documenting the disaster recovery steps for switching two different production system platforms to a disaster recovery environment for its payment posting system. The IRS also had updated nine of the 10 contingency plans to reflect changes to computer equipment and software supporting the information systems and the operating environment. However, it did not fully update one plan to document the existence of a server that was added to the operating environment for one of its tax processing systems. By not updating the contingency plan to reflect the change, the IRS has reduced assurance of its ability to fully restore the system in the event of a service interruption.

The GAO also identified that, while the IRS had developed and documented security plans for the 12 systems reviewed, it had not updated three of the plans to reflect changes to the information systems or their current operating environment. Specifically, the IRS did not update one plan to show that the agency had changed the system authentication mechanism to Smart ID cards, which replaced the weaker encryption that was previously used. In addition, plans for the other two systems were not updated to reflect changes in system boundaries where their interconnections to each other were removed. The IRS also did not correct a similar weakness in the plan for a system that covered multiple subsystems providing network infrastructure services to the agency, which was reported in Fiscal Year 2016. Further, the IRS did not update five system security plans to remove references to criteria the agency had rescinded. Specifically, the IRS rescinded its Information Technology Security Audit Logging Security Standard effective February 28, 2017. However, at the end of the audit, the plans still referenced the rescinded standard as audit logging criteria, which was also reported in the GAO's review of the IRS's financial statements for Fiscal Years 2017 and 2016. Without updated system security plans, the IRS has less assurance that it has documented and implemented appropriate security controls to protect its sensitive financial and taxpayer information.

Systems Development and Information Technology Operations

In carrying out its responsibilities of administering the tax laws, the IRS relies extensively on information technology investments to support its mission-related operations. For Fiscal Year 2016, the IRS's information technology portfolio contained 137 investments, of which 23 were classified as major. According to the IRS, it spent approximately $2.7 billion on its information technology investments during Fiscal Year 2016. Of the $2.7 billion, approximately $1.9 billion (70 percent) was spent for operations and maintenance activities.

TIGTA and the GAO performed several audits that assessed the operations of information technology at the IRS. These audits covered information technology acquisitions, project management, hardware and software asset management, human capital, and implementation of corrective actions.

Information technology acquisitions

In December 2014, Congress enacted the Federal Information Technology Acquisition Reform Act of 2014[49] (FITARA) to improve major Federal agencies' information technology acquisitions as well as hold CIOs accountable for reducing duplication of efforts across agencies and achieving cost savings. On November 21, 2017, Congress passed the FITARA Enhancement Act of 2017,[50] repealing and extending certain provisions of the FITARA. The Department of the Treasury is one of the Federal agencies responsible for implementing the FITARA. The IRS is responsible for implementing the FITARA to the extent that the Department of the Treasury has delegated FITARA responsibilities to it. The basic principles of the FITARA are to improve CIO approval authority over information technology purchases and to empower Government CIOs with the authority to eliminate unnecessary information technology spending.

TIGTA initiated an audit[51] to determine the IRS's effectiveness in implementing the requirements of the FITARA in relation to its information technology and information resources management responsibilities. While the applicability of the FITARA applies to the IRS's CIO only to the extent that FITARA responsibilities have been delegated by the Department of the Treasury, we reported in July 2018 that the IRS could do more to voluntarily follow the intent of the FITARA, thereby improving management of its information technology investment portfolio. Specifically, we found that the review and approval processes over major information technology acquisitions should be improved and implemented enterprise-wide. For example, the IRS's ability to voluntarily achieve one of the key guiding principles of the FITARA, which is to establish CIO authority over the review and approval of major information technology acquisitions, was weakened by the following three conditions.

- The IRS CIO does not review the acquisition and contract sections in the business cases as required by the Department of the Treasury's FITARA responsibilities assignment memorandum. To comply with this requirement, the Associate CIO, Strategy and Planning, annually presents business cases for major investments to the CIO containing high-level contract and acquisition data. However, these high-level acquisition data do not include vendors' names, the purpose of the contracts, or contract dollar amounts. We believe the high-level presentation of business cases does not satisfy the Department of the Treasury's delegation of responsibility to the IRS CIO to review the acquisition and contract sections in business cases.

[49] Pub. L. No. 113-291, Title VIII, Subtitle D.

[50] Pub. L. No. 115-88.

[51] TIGTA, Ref. No. 2018-20-045, *Information Technology Investment Management Controls Should Be Better Aligned With the Federal Information Technology Acquisition Reform Act of 2014* (July 2018).

- The IRS CIO has broadly delegated the responsibilities to review and approve major information technology acquisitions for the IT organization to subordinates. This delegation of authority as it relates to major information technology acquisitions is contrary to the basic principles of the FITARA.
- The IRS has not effectively implemented enterprise-wide the provisions of Internal Revenue Manual 2.21.1, *Requisition Processing for IT Acquisition Products and Services, Introduction to Requisition Processing for Information Technology (IT)*, dated April 11, 2017, which states that the IRS CIO has the responsibility for all purchases of information technology products and services acquired by the IRS. The controls necessary to implement Internal Revenue Manual 2.21.1 are not in place to ensure that the IT organization is actively engaged in reviewing, approving, and implementing information technology acquisitions that are initiated or funded by other business units. These controls are needed to ensure that the IT organization is engaged in the information technology product or service procurement process prior to the IRS signing the contract.

As a result, the IRS CIO's ability to exercise authority over the review and approval of major information technology acquisitions is limited.

We also found that lessons learned trends from post-implementation reviews and operational analyses should be used to improve IRS information technology investment management. Without fully using lessons learned to improve the capital planning and investment control process, IRS investment management will potentially not benefit from the experience learned by overcoming recurring problems, will repeat prior mistakes, and will not continually improve its capital planning and investment control activities.

Project management

Project management is the discipline of using established principles, procedures, and policies to manage a project from conception through completion. It is the application of knowledge, skills, tools, and techniques to activities to meet the project requirements. It is also the process of defining and achieving goals while optimizing the use of resources, such as people, time, and money, during the course of a project.

For Fiscal Year 2018, TIGTA and the GAO provided coverage of information technology project management controls in three audits. In our FITARA audit, we found that the IRS was using incremental development on major information technology projects. Incremental software development offers the benefits of: delivering capabilities to users more rapidly; increasing the likelihood that individual projects will achieve cost, schedule, and performance goals; obtaining additional feedback from users, increasing the probability that each successive increment will meet the user's needs; and terminating a poorly performing investment with fewer costs.

As of November 7, 2017, the date of the latest FITARA Scorecard,[52] the Department of the Treasury investment portfolio data reported on 38 IRS development projects, 11 of which were incrementally developing software or services at least every six months. Examples of some incremental software development projects included Modernized e-File Releases 10 and 10.1, Affordable Care Act Administration Release 6.1, Foreign Account Tax Compliance Act Releases 5.0 and 6.0, and the Individual Master File (IMF) 2017 Mid-Year Conversion.

However, during subsequent discussions with the IRS about the November 2017 FITARA Scorecard, the IRS discovered that, based on its review of actual project start and completion dates, information used in the Department of the Treasury's FITARA score for the incremental development calculation was incorrect. We recalculated the incremental development measure using the corrected information and found that the IRS was using incremental development on 16 of its 17 in-process projects as of January 30, 2018. This calculates to a 94 percent, or a grade of A. There were 12 completed projects incorrectly included in the incremental development calculation for the November 2017 FITARA Scorecard.[53] The Department of the Treasury subsequently notified the OMB of this discrepancy, to which the OMB replied that the software logic calculating the in-process indicator wasn't working properly and that a code fix was needed to properly reflect in-process and completed projects.

In our audit of the Enterprise Case Management (ECM) solution,[54] we found that the IRS's initial efforts to develop an ECM solution were unsuccessful, costing $85.4 million and approximately two and a half years of work, and other options are now being evaluated. Case management is the process that addresses the resolution of tax administration issues through the management of case creation, execution, maintenance, and closure. It describes the activities required to manage the life cycle of an individual case. The IRS's case management environment is characterized by many challenges that are driven by the complexity of the tax laws and tax administration, the diversity of the customers the IRS serves, and the large number and variety of IRS programs and services as well as the need to modernize and upgrade aging IRS case management systems. Tax administration is supported by more than 90 different case management systems that widely vary in complexity and size and how they are customized. These case management systems were implemented over many years to support the individual needs of multiple business units.

[52] The House Oversight and Government Reform Committee, working alongside the GAO, developed the scorecard to assess Federal agency FITARA implementation efforts, assigning a grade from A to F based on self-reported data at the department level.

[53] Between the time that the November 2017 Scorecard was issued and our recalculation of the incremental development score, the IRS reported that it closed 22 projects and started 13 new ones. Removing the additional 12 completed projects incorrectly included in the initial incremental development calculation results in 17 in-process projects as of January 30, 2018.

[54] TIGTA, Ref. No. 2018-20-043, *Initial Efforts to Develop an Enterprise Case Management Solution Were Unsuccessful; Other Options Are Now Being Evaluated* (July 2018).

Although the IRS established the ECM program[55] in January 2015,[56] it did not perform a search for a software product that would enable the ECM program to meet its enterprise-wide requirements. The IRS used entellitrak® to develop the ECM solution despite problems reported from prior case management projects, *e.g.*, the software product had not proven it could be scalable to the IRS's needs and did not have continuous integration capability. In November 2016, the IRS provided the vendor a list of 37 operational problems related to using entellitrak to develop the ECM solution and requested that the vendor address the problems. However, the IRS had concerns with the vendor's proposed solutions. Further, ECM requirements were not agreed upon prior to the start of the following ECM projects.

- Enterprise Fraud Case Management – This ECM project was scheduled for deployment in December 2017 and would have developed case management functionalities for fraud case management.
- ECM Tracking – This ECM project was to establish one solution to achieve the conversion of existing IRS case tracking systems to entellitrak.
- ECM Correspondence – This ECM project was to track and report on correspondence between the IRS and taxpayers in support of cases being managed.

In October 2016, the IRS reported that not having agreed-upon, baselined ECM requirements was a risk in its Item Tracking, Reporting, and Control system. Specifically, the risk statement reported that if correct ECM requirements were not consistently adopted by all ECM stakeholders, then the ECM Information Technology Program Management Office would not have a consistent understanding of the requirements and the enterprise solution architecture could require maintenance.

In February 2017, the IRS Commissioner was informed that the entellitrak software product that the IRS had selected was not viable for developing the ECM solution. The IRS suspended the last ECM project's development activities in April 2017. Because of the problems with its ECM solution effort, there will be substantial delays in migrating case management processes from legacy case management systems. As a result, for the time being, the IRS will be unable to

[55] The IRS established the ECM program to consolidate many case management systems across the IRS. The ECM program planned to: 1) standardize system design for increased taxpayer information security; 2) reduce the risk for system failures that would impede revenue collection; and 3) provide cost savings by reducing information technology hardware, software, and system maintenance costs.

[56] Prior to initiating the ECM program, the IRS had started three other case management projects: the Information Reporting and Document Matching Case Management system, the Taxpayer Advocate Service Integrated System, and the Affordable Care Act Case Management system. TIGTA conducted audits of all three case management projects and reported that all three projects were closed or suspended prior to completion. Both the Information Reporting and Document Matching Case Management project and the Taxpayer Advocate Service Integrated System project failed because of insufficient system requirements. The Affordable Care Act Case Management project was closed in order to free up resources and funding for other information technology projects. In total, the IRS spent $33,256,603 and dedicated significant resources toward development of these three systems.

realize the cost savings from reducing information technology hardware, software, and system maintenance costs for the numerous antiquated case management systems. Moreover, using antiquated systems runs the increased risk of system failures.

The IRS has taken several positive steps to address our audit findings since the IRS Commissioner was informed in February 2017 that entellitrak was not viable for the ECM solution. For example, in March 2017, the IRS initiated a commercial off-the-shelf product assessment to evaluate the industry's best case management software. By performing an assessment of current case management products in the marketplace, the IRS can identify and select the best products for the ECM solution. The IRS's current efforts show positive steps toward the development of the ECM solution because it is specifically focused on ECM development rather than a specific project under the ECM, such as the Enterprise Fraud Case Management.

In its report on IRS tax processing,[57] the GAO reported that best practices highlight the importance of monitoring the performance of projects in development by comparing actual cost, schedule, and scope to plans in order to allow appropriate corrective actions if actual performance deviates significantly from planned performance. The GAO found that the performance of select IRS information technology investments varied. Specifically, four selected investments[58] in development had spent less than planned, and most were behind schedule and had delivered less scope than planned. In addition, most of these investments had significant variances, meaning that actual cost, schedule, or scope varied from their plans by more than 10 percent. For five selected investments[59] in the operations and maintenance phase, the GAO found that most had met all of their operational performance targets and all performed operational analyses required by the OMB.[60] However, none of the analyses addressed all key factors specified in the OMB's guidance. As a result, the IRS is at risk of not having critical information needed to determine whether its investments fully meet intended objectives and whether there are alternative ways to efficiently meet its mission.

Hardware and software asset management

Hardware and software asset management controls are key to: 1) timely detect loss, theft, or misuse of Government property; 2) help mitigate unauthorized access to taxpayer or other sensitive information; 3) accurate financial statement reporting; and 4) help management make sound operating decisions and manage operations. In Fiscal Year 2018, TIGTA and the GAO

[57] GAO, GAO-18-298, *INFORMATION TECHNOLOGY: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing* (June 2018).
[58] Affordable Care Act; ECM; Customer Account Data Engine 2; and the Return Review Program.
[59] End User Systems and Services; Integrated Data Retrieval System; IMF; Mainframes and Servers Services and Support; and Telecommunications Systems and Support.
[60] According to the OMB's Fiscal Year 2016 capital planning guidance, ongoing performance of operational investments should be monitored to ensure that the investments are meeting the needs of the agency, are delivering expected value, and/or are consistent with the agency's enterprise architecture.

each issued a report covering hardware and/or software management controls. In our audit of information technology hardware asset inventory,[61] we found that the IRS has taken steps to improve its hardware asset management by revising its hardware user guide and continuing to look for opportunities to implement technologies and automation into its hardware asset inventory processes. However, despite these efforts, management controls need to be further strengthened to improve the reliability of the hardware asset inventory.

Specifically, for Fiscal Year 2017, the IRS verified 226,947 (90.6 percent) of 250,520 Class A and Class B hardware assets, which was short of its inventory objective of a 95 percent or better certification rate. While the hardware asset certifying officials returned signed Certification Letters acknowledging their commitment to make all attempts to find unverified and missing assets, they only verified an additional 7,095 (23.1 percent) of the 30,668 initially unverified and missing hardware assets, leaving a balance of 23,573 unverified and missing assets. During site visits to nine IRS locations, we were able to verify unverified and missing assets by physically locating or otherwise accounting for 54 (41.5 percent) of 130 hardware assets[62] judgmentally selected from the Knowledge Incident/Problem Service Asset Management–Asset Manager (KISAM-AM) module for review.

In addition, the IRS did not ensure that all hardware assets were timely documented or controlled in the KISAM-AM module. We identified that 12 (40 percent) of 30 judgmentally selected hardware assets were not updated in the KISAM-AM module within 10 workdays of receipt as required. We also identified that 17 (16.7 percent) of 102 judgmentally selected hardware assets from our site visits did not have a corresponding KISAM-AM module record and were not controlled in the system as required.

IRS hardware asset inventory certifying officials also did not always ensure that key KISAM-AM module fields[63] were complete, accurate, and reliable. Of 232 hardware assets,[64] we reviewed 151 that were found or selected during our site visits[65] to determine whether four of the five key fields in the KISAM-AM module were accurate. We analyzed a total of 604[66] KISAM-AM module fields by comparing the key field information captured at each of our site visits to the KISAM-AM module data provided by the Hardware Asset Management office. Our analysis

[61] TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).
[62] We physically located 49 assets and accounted for an additional five other assets by contacting the person listed in the User Name or Contact Name fields from the KISAM-AM module record.
[63] Key KISAM-AM module fields include the Assignment Code, Barcode, Serial Number, Building Code, and either the User Name or Contact Name.
[64] Our sample included 130 hardware assets judgmentally selected from the KISAM-AM module and 102 hardware assets judgmentally selected from our site visits.
[65] The 151 hardware assets that were found included 49 assets of the 130 assets selected from the KISAM-AM module and 102 of the assets selected from our site visits. We did not include five additional assets that were accounted for because the key KISAM-AM module fields were provided for the user to verify.
[66] Four key KISAM-AM module fields multiplied by 151 hardware assets reviewed.

identified that one or more of the four key KISAM-AM module fields were inaccurate for 53 (35.1 percent) of the 151 hardware assets reviewed. Further, of the 604 KISAM-AM module fields analyzed, we identified 109 (18 percent) total errors. We were unable to determine the accuracy of the remaining key KISAM-AM module fields (either the User Name or Contact Name field) because the employees listed were not always present during our site visits and/or we were unable to definitively determine whether the asset was assigned to a single user or if the asset was shared. As a result, we measured the IRS's efforts to ensure that required information was entered into either of these two fields in the KISAM-AM module by analyzing the IRS-provided KISAM-AM module data extract of all Class A and Class B hardware assets, dated October 1, 2017. We found that both the User Name and Contact Name fields did not include required information for 6,493 (4.5 percent) of the 144,296 hardware assets that had an assignment status of in use.[67]

Managing and maintaining the integrity of the KISAM-AM module asset hardware inventory requires the complete and timely updating of asset records. Incomplete or inaccurate asset records hinder management's ability to make sound operating decisions and manage operations. In addition, failure to timely update asset inventory records impedes the IRS's ability to timely detect the loss, theft, or misuse of Government property. Lack of controls over hardware assets increases the potential risk of unauthorized access to taxpayer or other sensitive information. If unverified and missing hardware assets are allowed to remain in the KISAM-AM module, this could result in the IRS overstating its financial statements by reporting amounts for assets that are no longer in its possession. Conversely, hardware assets without a KISAM-AM module record, or assets incorrectly reported as missing, lost, or stolen that are still in the IRS's possession, could result in the IRS understating the value of its assets on its financial statements.

In the GAO's review of IRS tax processing, it found that the Integrated Data Retrieval System, IMF, and Mainframes and Servers Services and Support system are facing significant risks, in part due to their reliance on legacy software programming languages and outdated hardware. Despite these risks, the GAO reported that the IRS has not fully implemented key risk management practices and may be challenged in mitigating risks effectively so that they do not affect the agency's ability to carry out its mission. These systems were originally placed into operation in the late 1960s and early 1970s and, thus, are considered legacy systems.

The GAO reported that the Integrated Data Retrieval System and the IMF rely on legacy software programming languages, resulting in increased risk to continuing operation of these investments. Specifically, the IMF is written in assembly language code and Common Business Oriented Language, and the Integrated Data Retrieval System is written in Common Business Oriented Language (both language codes were developed in the 1950s). Reliance on legacy

[67] The User Name or Contact Name fields are required to be populated only for in use assets and not for in stock or missing assets.

software programming languages has risks, such as a rise in procurement and operating costs and a decrease in the availability of individuals with the proper skill sets to maintain them.

In addition, the GAO reported that the Mainframes and Servers Services and Support system relies on a significant amount of outdated hardware exposing it to rising warranty and maintenance fees as well as equipment failures. Specifically, at the start of Fiscal Year 2017, the IRS reported an inventory of approximately $684.2 million in hardware associated with this system. Of this amount, approximately $430.3 million, or 63 percent, was for outdated hardware, with about 21 percent of that amount directly supporting tax processing. IRS officials stated that the outdated hardware associated with the Mainframes and Servers Services and Support system is expensive to maintain because it is often past the warranty. Specifically, after a warranty for hardware ends, the maintenance fees for this hardware commonly increase by approximately 25 percent per year. In addition, the officials stated that relying on this hardware has the potential to expose the IRS to equipment failures that could preclude its systems from supporting the annual tax filing season and expanding the systems and tools for enforcement approaches, among other things.

Human capital

Mission-critical skill gaps across the Federal workforce pose a high-risk to the Nation because they impede the Government from cost-effectively serving the public and achieving results. The GAO first designated strategic human capital management across the Government as a high-risk issue in 2001 because of the Federal Government's long-standing lack of a consistent approach to human capital management. In February 2011, the GAO narrowed the focus of this high-risk issue to the need for agencies to close mission-critical skill gaps.

Implementing effective information technology workforce planning practices can better position the IRS to address human capital risks. Accordingly, the GAO identified four key information technology workforce planning practices and supporting activities detailed in various laws enacted and guidance issued over the past 20 years that call for agencies to perform workforce planning activities. These key practices are 1) setting the strategic direction for workforce planning, 2) analyzing the workforce to identify skill gaps, 3) developing strategies to address skill gaps, and 4) monitoring and reporting on progress in addressing skill gaps.

In its IRS tax processing report, the GAO reported that, while the IRS has initiated information technology workforce planning efforts, it has not implemented any of the four key information technology workforce planning practices, placing tax processing and modernization efforts at risk. Specifically, the GAO found that the IRS Human Capital Office and IT organization have collaboratively developed a tool to automate the information technology workforce planning process, but the tool is in the initial stages of implementation, and the IRS has not yet performed any of the activities associated with setting the strategic direction for workforce planning. In addition, the IRS has developed an inventory of its current information technology workforce, but it has not yet developed the competency and staffing requirements nor conducted any of the activities associated with analyzing the workforce to identify skill gaps, developing strategies to address skill gaps, or monitoring and reporting on progress in addressing skill gaps for the agency.

While the IRS has not implemented key practices for information technology workforce planning at the agency level, staff working on the IMF and Customer Account Data Engine 2 provided evidence of efforts they had taken to address their workforce needs. For example,

- For the IMF, the IRS established a process in Calendar Year 2016 for continuously matching the current workforce capacity, in terms of skills and staffing, with a projected level of work. In addition, the IMF staff identified competencies and staffing requirements and assessed the gaps by assessing net available staff hours with needed staff hours for particular skill types. Lastly, the IMF staff developed strategies and implemented activities in an effort to address information technology skill gaps by creating a stabilization plan, which includes short- and long-term activities for training and realignment of resources.
- For the Customer Account Data Engine 2, the IRS conducted an assessment in Calendar Year 2015 to identify Government and contractor resource needs and utilization. The IRS also identified skill gaps and developed strategies and implemented activities such as knowledge transfer sessions to begin addressing these skill gaps. The Customer Account Data Engine 2 program manager stated that the program is waiting for additional guidance and direction from the IRS Human Capital Office, as the work in this area was a rudimentary one-time effort.

Staff for the Integrated Data Retrieval System and Return Review Program stated that they were awaiting further implementation of the IRS's agencywide workforce planning tool to address their information technology workforce planning needs. IRS officials attributed the limited progress in implementing information technology workforce planning practices to resource constraints and competing priorities. However, until the IRS implements these practices, it will continue to face challenges in assessing and addressing the gaps in knowledge and skills that are critical to the success of its key investments.

The GAO also reported that three selected IRS legacy systems, *i.e.*, the IMF, the Mainframes and Servers Services and Support system, and the Integrated Data Retrieval System, are facing risks due to the attrition of key personnel. For example, IMF program officials noted that developers are responsible for maintaining taxpayer accounts and applying business rules associated with the tax process for a given situation or tax year and thus require skills beyond creating or updating lines of code. However, according to an internal staffing report for the IMF, the IRS experienced attrition of developers skilled in legacy programming languages and tax processing, exposing the investment to increased risks of not being able to successfully process tax information. For example, according to the report, 24 developers responsible for performing work on the IMF investment retired or were transferred to other positions in the past six years. As a result of this attrition, only 32 developers were available to perform IMF system updates for the 2017 Filing Season, which was about four developers less than needed to perform the work.

Further, as of July 2017, IMF program officials projected a shortage of three developers needed for the 2018 Filing Season.

In an internal document identifying options to address the loss of knowledge caused by the attrition of staff for the IMF, the IRS reported that it has taken various actions as a result of the ongoing attrition of developers. These actions include cancelation of planned system enhancements, training and transfer of developers from other projects to perform work on the IMF, and reduction in the amount of development work being completed for the Customer Account Data Engine 2 to address a financial material weakness.

According to IMF risk logs, the investment also reported potential impacts on tax processing as a result of the attrition. These impacts include the IRS's delay in implementing modifications to the IMF for the filing season to reflect changes in the tax law, tax processing delays due to the lack of adequate institutional knowledge to resolve complex issues, and a lack of necessary data from the IMF, which the IRS uses as input for other tax processing systems.

Further, according to the IRS's CIO, it takes four to five years to train developers performing work on the IMF. The IRS, however, is facing challenges with such training and development. For example, IMF program staff stated that the IRS has historically recruited and trained future developers from within the agency, where staff had an understanding of IRS business processes and concepts. However, according to the program staff, budgetary reductions limiting travel, moving costs, or stipends have prevented the IRS from continuing such efforts. Until the IRS implements effective key workforce planning practices, it will not be best positioned to address the human capital risks it faces and ensure the timely and effective delivery of its investments.

Implementation of corrective actions

Internal controls are comprised of the plans, methods, and procedures used to accomplish an organization's mission, goals, and objectives. Internal controls protect assets, detect errors, and prevent fraud. Systems of internal controls provide reasonable assurance that the following objectives are being achieved: 1) effectiveness and efficiency of operations; 2) reliability of financial reporting; and 3) compliance with applicable laws and regulations.

The Department of the Treasury developed the Joint Audit Management Enterprise System (JAMES) to track issues, findings, and recommendations reported in the GAO, Department of the Treasury's Office of Inspector General, and TIGTA audit reports. The JAMES is used to track the current progress of Planned Corrective Actions (PCA) for material weaknesses, significant deficiencies, and existing reportable conditions as well as remediation and action plans. The information contained in the JAMES is used by the Department of the Treasury to assess the effectiveness and progress of its bureaus in correcting their internal control deficiencies and implementing audit recommendations.

The IRS has developed guidance and assigned responsibilities to managers, senior officials, and audit coordinators to help ensure that its corrective actions are completed. The Chief Financial Officer's Office of Audit Coordination supports the day-to-day internal control program and is responsible for managing the Department of the Treasury's JAMES-related activities for the IRS. In addition, IRS management is responsible for assigning individuals within the respective business units to serve as JAMES audit coordinators. The JAMES audit coordinators' responsibilities include uploading Form 13872, *Planned Corrective Action (PCA) Status Update for TIGTA/GAO/MW/SD/TAS/REM Reports*,[68] as well as sufficient documentation supporting each PCA closure into the JAMES. All IRS business units use the Form 13872 to update the status of their PCAs in the JAMES, *e.g.*, adding the PCA implementation date or extending the due date. The IRS is required to notify TIGTA if it plans to significantly revise or cancel a corrective action to a TIGTA recommendation, and TIGTA must consent to the change.

During Fiscal Year 2018, TIGTA and the GAO conducted three audits with coverage on whether the IRS's closed PCAs have been fully implemented and documented. Our PCA review of the IT organization[69] focused on a judgmental sample of 20 closed PCAs related to prior TIGTA systems development and systems operations recommendations. Our review of the sampled PCAs found that approving officials and the Office of Audit Coordination approved each PCA closure. However, the PCA closure process, including ensuring that PCAs are fully implemented, needs to be improved. For example, according to the instructions for Form 13872, the "Specific action taken" section of the form should state the specific activities taken to implement the agreed-upon action(s). Based on our review, the "Specific action taken" section did not completely describe how the IRS implemented the PCAs for two (12.5 percent) of 16 sampled PCAs.[70] The forms simply stated that the upgrades were completed. In both examples, the information on the forms did not comply with PCA closure instructions to document the specific activities taken to implement the PCAs. Without a complete description of actions taken to implement the PCAs, it is unclear how or to what extent the IRS implemented them.

In addition, we reviewed supporting documentation in the JAMES for the 16 sampled PCAs and found that the IRS did not upload sufficient documentation to support proper PCA closure for six (37.5 percent) of them. Based on the sampled PCAs we reviewed, we determined that JAMES audit coordinators and the Office of Audit Coordination did not always ensure that sufficient documentation was uploaded into the JAMES to support PCA closure. Without sufficient supporting documentation in the JAMES, there is limited evidence to support that PCAs were fully implemented.

We also found that the IRS did not fully implement four (20 percent) of the 20 sampled PCAs that it had closed as implemented on the JAMES. Of these four PCAs, three were partially

[68] MW = Material Weaknesses, SD = Significant Deficiencies, TAS = Taxpayer Advocate Service, and REM = Remediation Plans.

[69] TIGTA, Ref. No. 2018-20-063, *Improved Controls Are Needed to Ensure That Corrective Actions for Reported Information Technology Weaknesses Are Documented and Fully Implemented Prior to Closure* (Sept. 2018).

[70] Our sample was comprised of 20 closed PCAs, which included four PCAs that were closed with management's response prior to April 1, 2017. Prior to April 1, 2017, the IRS did not require personnel to upload supporting documentation to the JAMES for PCAs closed at the time of management's response.

implemented and one was not implemented at all. For these four sampled PCAs, the IRS did not provide sufficient evidence to support a conclusion that they had been fully implemented.

Our review of closed Cybersecurity organization PCAs[71] focused on a judgmental sample of 23 PCAs related to prior TIGTA cybersecurity recommendations. Our analysis showed that 10 PCAs (43 percent) were not fully implemented and should not have been closed. All 10 relate to the security of systems that contain or provide access to taxpayer data. We found one that did not address the identified weaknesses and nine that partially addressed the identified weaknesses. During our review, we found that the one PCA had not been implemented because the IRS decided to take no action on our recommendation. However, we did not find an IRS request in the JAMES to cancel this PCA.

Without an effective management control process, the IRS cannot be assured that its management control program is operating as intended, which includes assessing its effectiveness and progress in correcting internal control deficiencies and implementing corrective actions in response to audit recommendations. When this happens, the IRS cannot assure its stakeholders, which include the Department of the Treasury and Congress, that the PCAs to correct the vulnerabilities were implemented as reported and that the information in the JAMES is reliable. The Department of the Treasury produces an annual financial report and an annual performance report that serves as its congressional justification for appropriated dollars. It is imperative that the information in the JAMES is reliable and that the developed processes to assist with supporting the management control process are effective.

In its review of protecting sensitive financial and taxpayer data, the GAO also reviewed closed PCAs related to prior GAO cybersecurity recommendations to determine whether the PCAs were properly closed. The GAO made recommendations to the IRS to correct identified information security control deficiencies in access controls, configuration management, segregation of duties, contingency planning, and security management. However, the GAO found that many deficiencies in these information security control areas have not been corrected, and a large number of recommendations remained open at the conclusion of their audit. Specifically, at the beginning of the audit, the IRS stated that it had implemented 63 of the 166 recommendations that the GAO made during prior audits. However, the GAO determined that the IRS had effectively implemented only 37 (59 percent) of these 63 recommendations.

The GAO also concluded that seven[72] of the original 166 recommendations were no longer relevant due to the changes in the IRS's operating environment. Further, the GAO found that an additional five recommendations that IRS had not submitted to the GAO for validation had been adequately addressed. Collectively, the IRS had corrected or mitigated deficiencies associated

[71] TIGTA, Ref. No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* (Sept. 2018).
[72] The GAO reported that these seven recommendations will either be reissued to more closely align with the agency's current policies and environment or not be reissued due to it being covered by another recommendation.

with 49 of the 166 recommendations to resolve control weaknesses that were open at the beginning of the GAO's audit.

Although the IRS made some progress in correcting or mitigating the previously reported deficiencies, the IRS still had not fully or effectively implemented corrective actions for 117 (70 percent) of the 166 recommendations. This indicates that the IRS's corrective action verification process continues to be ineffective. Until the IRS takes additional steps to implement a more effective process, it will have limited assurance that control deficiencies are being properly mitigated or corrected. As a result, sensitive financial and taxpayer data on IRS computer systems remain vulnerable.

Filing Season Readiness

TIGTA performed three audits that assessed the IRS's readiness for the annual tax filing season. Our audits covered the implementation of the Tax Cuts and Jobs Act of 2017,[73] implementation of Section 201 of the Protecting Americans from Tax Hikes Act of 2015 (PATH Act),[74] and the systems outage on Tax Day, April 17, 2018.

Tax Cuts and Jobs Act of 2017

On December 22, 2017, the President signed into law the Tax Cuts and Jobs Act of 2017 (hereafter referred to as the Act). The Act made significant changes to the tax code affecting individuals, businesses, and tax-exempt organizations. The Act contains 119 tax provisions administered by the IRS that affect both domestic and international taxes and is the first major tax reform legislation in more than 30 years. The IRS estimates that implementation will require creating or revising about 450 forms, publications, and instructions and modifying about 140 information technology systems (for tax return processing and compliance activities) to ensure that it can accommodate the newly revised tax forms and respond to an estimated 4 million additional telephone calls and taxpayer correspondence. The IRS is continuing to assess its systems to determine the ones that are affected by the Act.

TIGTA initiated an audit[75] to provide a status of the IT organization's progress to make system modifications required by the Act for the 2019 Filing Season. We found that missed deadlines could increase the risk of not timely completing system modifications. The IT organization's normal deadline for business units requesting information technology products and services for the next filing season is January 31. For example, requests for system changes for the 2019 Filing Season would have been due by January 31, 2018. With the passage of the Act in

[73] Pub. L. No. 115-97. Officially known as "An act to provide for reconciliation pursuant to titles II and V of the concurrent resolution on the budget for Fiscal Year 2018."
[74] Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, Div. Q (2015).
[75] TIGTA, Ref. No. 2018-24-064, *A Shortened Delivery Cycle, High Volume of Changes, and Missed Deadlines Increase the Risk of a Delayed Start of the 2019 Filing Season* (Sept. 2018).

December 2017, the IT organization established several interim deadlines to facilitate timely implementation of the Act's tax provisions. However, the business units missed the deadlines for submitting work request notifications and business requirements. Subsequently, the IT organization set a new deadline of June 1, 2018, for submitting final work request notifications. The most recent deadline shortened the time frame for making system changes for the 2019 Filing Season by four months. As of July 5, 2018, the IT organization had not received all final work request notifications and business requirements. Delays in receiving this information will result in less time for modifying and testing systems and increases the risk of a delayed start of the 2019 Filing Season.

Another area of concern that could affect the timely implementation of the Act's tax provisions for the 2019 Filing Season is the IRS's ability to quickly fill critical positions that were vacated by employees or contractor employees. If the process to hire employees or the process to procure contractor employees is lengthy, the positions might not be quickly filled, causing risk to the timeliness of the information technology updates.

We also found that the IT organization is fully funded to implement the Act. The IRS received $320 million to implement the Act, allocating $291 million for the hours it estimated would be needed for the information technology and ancillary operations support work. TIGTA calculated it will take more than 1.1 million hours based on the IRS's estimate of 542 full-time equivalents to implement the Act's tax provisions. The IRS plans to use current and new employees to meet these needs. As of June 2018, 117 current and new employees have been hired and entered on duty. However, the IRS used standard position descriptions for hiring efforts and has not defined specific knowledge, skills, abilities, and other requirements necessary for positions it expects to hire for work on the Act and/or back-filling existing positions due to personnel performing the work. This information is necessary to ensure that hiring efforts support successful implementation of the Act with limited impact on existing IT organization work.

In addition, we found that the scope of system changes and impact to existing projects is unclear. The IT organization is planning to identify any potential negative impact on existing programs and projects caused by implementing the Act. As of July 16, 2018, the IRS had not provided documentation of any ongoing projects or programs that will be negatively affected by the implementation of the Act. TIGTA is continuing to review the IT organization's efforts to implement the Act.

Protecting Americans from Tax Hikes Act of 2015

On December 18, 2015, Congress enacted the PATH Act, which includes program integrity provisions specifically intended to reduce certain fraudulent and improper payments. The integrity provisions expanded the IRS's ability to verify earned income before refunds are paid. One of the program integrity provisions in the PATH Act is in Section 201.[76]

[76] Codified into Internal Revenue Code § 6071 and § 6402.

Section 201 of the PATH Act modifies the filing due dates of Form W-2, *Wage and Tax Statement*, and Form 1099-MISC, *Miscellaneous Income*. It requires returns and statements related to employee wage information and nonemployee compensation[77] be filed on or before January 31. Prior to the 2017 Filing Season, the due date for a paper Form W-2 and Form 1099-MISC was February 28; for an electronically filed Form W-2 and Form 1099-MISC, the due date was previously March 31. Section 201 of the PATH Act also specifies that no credit or refund can be made to taxpayers who claimed the Earned Income Tax Credit or the Additional Child Tax Credit until the 15th day of the second month following the close of the taxable year, *i.e.*, February 15, 2017, for the 2017 Filing Season. This change allows the IRS to take additional time to review refund claims before issuing refunds with the Earned Income Tax Credit or the Additional Child Tax Credit in order to reduce fraud and improper payments.

The Filing Information Returns Electronically system is an Internet-based system through which filers transmit information returns and other forms electronically to the IRS. According to the IRS, this system performs preliminary checks of submitted files, manages the file transfer of data to downstream systems, and receives statuses from the downstream systems. It also receives Form 1099-MISC and Form 8809, *Application for Extension of Time To File Information Returns*.

TIGTA initiated an audit[78] to ensure that the IRS was in compliance with the filing requirement changes in Section 201 of the PATH Act and reported that the Filing Information Returns Electronically system was ready for the 2017 Filing Season. Based on our analysis and discussions with the IRS, we concluded that the Wage and Investment Division and the IT organization worked together to trace 18 business requirements to 13 information technology requirements needed to comply with the legislative changes. We also reviewed requirements testing documentation to ensure that all 13 requirements were tested and system functionality met expectations prior to implementing the changes into the production environment. Based on our analysis, we concluded that each of the 13 requirements were successfully tested (actual results matched expected results) for acceptance prior to being placed into production.

IRS systems outage on Tax Day

The IRS relies extensively on information technology systems to annually collect taxes, distribute refunds, and carry out its mission of providing service to America's taxpayers in meeting their tax obligations. During Calendar Year 2018, the IRS expects to receive approximately 153.7 million individual income tax returns, with more than 89 percent of those filed electronically.

[77] Or self-employment income.

[78] TIGTA, Ref. No. 2018-20-019, *System Changes Resulted in Successfully Processed Third-Party Income Documents, but Processes for Using the Information Need Improvement* (Mar. 2018).

TIGTA initiated an audit[79] to review the IRS systems outage that occurred on Tax Day, April 17, 2018, and identify solutions to prevent such disruptions in the future. We found that the IRS experienced a storage outage due to a firmware bug on one of the IRS's high-availability storage arrays. Because of the outage, 59 tax processing systems, including Modernized e-File, were unavailable for approximately 11 hours between 2:57 a.m. and 1:40 p.m.[80] The IRS Computer Security Incident Response Center concluded that the outage fit the pattern of a previously known firmware bug and determined that there was no evidence of any breach or cyber threat activity related to this outage. The timing and severity of the outage prompted the IRS to allow an additional day to file to April 18, 2018.

Established contingency tools, processes, and procedures for mainframe outages served the IRS well during the Tax Day outage. The IRS detected, assessed, repaired, and restored mainframe operations by the afternoon of the day the outage occurred and processed almost 4 million tax returns before midnight within acceptable performance time frames for acknowledgement and receipt.

While the IRS effectively responded to the Tax Day outage and resumed tax processing operations, the major outage process needs improvement to reduce risk and response times for future outages. To reduce these risks, the IRS needs to 1) better track lessons learned and vulnerabilities to ensure that remediation and other corrective actions are implemented in full; 2) require sufficient information from contractors about microcode upgrades in order to facilitate better decisionmaking by IRS management regarding microcode bundle implementation; and 3) improve the resiliency and availability of the Tier I architecture.

[79] TIGTA, Ref. No. 2018-20-065, *Review of the System Failure That Led to the Tax Day Outage* (Sept. 2018).
[80] All times are reported in Eastern Standard Time.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the adequacy and security of the IRS's information technology program. This review is required by the IRS Restructuring and Reform Act of 1998.[1] To accomplish our objective, we:

I. Obtained information on the IRS budget and staffing to provide context on the size of the IT organization.[2]

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

A. Obtained and reviewed the Security and Information Technology Services' Systems Security Directorate audit reports issued during Fiscal Year 2018. During the review, we analyzed and prepared an assessment of the systems security and privacy issues.

B. Identified and summarized relevant non–Security and Information Technology Services and/or external oversight assessments dealing with systems security and privacy.

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 the Security and Information Technology Services' Systems Development Directorate audit reports issued during Fiscal Year 2018. During the review, we analyzed and prepared an assessment of the systems development issues.

B. Identified and summarized relevant non–Security and Information Technology Services and/or external oversight assessments dealing with 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 the Security and Information Technology Services' Systems Operations Directorate audit reports issued during Fiscal Year 2018. During the review, we analyzed and prepared an assessment of the systems operations issues.

B. Identified and summarized relevant non–Security and Information Technology Services and/or external oversight assessments dealing with systems operations.

[1] Pub. L. No. 105-206, 112 Stat. 685.

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

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's information technology program based on a compilation of the audit results reported during Fiscal Year 2018. 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)
Bryce Kisler, Director
Louis Lee, Audit Manager
David Allen, Lead Auditor
Ashley Weaver, Senior Auditor
Jason Rosenberg, Auditor

Appendix III

Report Distribution List

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

Appendix IV

List of Treasury Inspector General for Tax Administration and Government Accountability Office Reports Reviewed

No.	Report Reference Number	Audit Title	Report Issuance Date
1	2018-10-004	*Improved Controls Are Needed to Account for the Return of Contractor Employee Identification Cards*	November 1, 2017
2	GAO-18-165	*FINANCIAL AUDIT: IRS's Fiscal Years 2017 and 2016 Financial Statements*	November 9, 2017
3	2018-20-007	*Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented*	February 5, 2018
4	2018-40-014	*Transcript Delivery System Authentication and Authorization Processes Do Not Adequately Protect Against Unauthorized Release of Tax Information*	March 20, 2018
5	2018-20-019	*System Changes Resulted in Successfully Processed Third-Party Income Documents, but Processes for Using the Information Need Improvement*	March 26, 2018
6	2018-40-031	*Proactive Processes to Identify and Mitigate Potential Misuse of Electronic Payment Systems Are Needed*	April 23, 2018
7	2018-20-029	*Security Over High Value Assets Should Be Strengthened*	May 18, 2018
8	2018-20-030	*The Cybersecurity Data Warehouse Needs Improved Security Controls*	June 21, 2018
9	GAO-18-418	*IDENTITY THEFT: IRS Needs to Strengthen Taxpayer Authentication Efforts*	June 22, 2018
10	2018-20-034	*Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls*	June 27, 2018

No.	Report Reference Number	Audit Title	Report Issuance Date
11	GAO-18-298	*INFORMATION TECHNOLOGY: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing*	June 28, 2018
12	2018-20-041	*Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability*	July 13, 2018
13	2018-20-036	*The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved*	July 18, 2018
14	2018-20-043	*Initial Efforts to Develop an Enterprise Case Management Solution Were Unsuccessful; Other Options Are Now Being Evaluated*	July 27, 2018
15	2018-20-045	*Information Technology Investment Management Controls Should Be Better Aligned With the Federal Information Technology Acquisition Reform Act of 2014*	July 27, 2018
16	2018-20-039	*Private Collection Agency Security Over Taxpayer Data Needs Improvement*	July 30, 2018
17	GAO-18-391	*INFORMATION SECURITY: IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data*	July 31, 2018
18	2018-20-063	*Improved Controls Are Needed to Ensure That Corrective Actions for Reported Information Technology Weaknesses Are Documented and Fully Implemented Prior to Closure*	September 19, 2018
19	2018-20-065	*Review of the System Failure That Led to the Tax Day Outage*	September 19, 2018
20	2018-24-064	*A Shortened Delivery Cycle, High Volume of Changes, and Missed Deadlines Increase the Risk of a Delayed Start of the 2019 Filing Season*	September xx, 2018
21	2018-20-066	*Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented*	September xx, 2018
22	2018-20-082	*Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018*	September 21, 2018

Appendix V

Glossary of Terms

Term	Definition
Access Controls	A policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: 1) passing the information to unauthorized subjects or objects; 2) granting its privileges to other subjects; 3) changing one or more security attributes on subjects, objects, the information system, or system components; 4) choosing the security attributes to be associated with newly created or modified objects; or 5) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges, *i.e.*, they are trusted subjects, such that they are not limited by some or all of the above constraints.
Additional Child Tax Credit	A refundable credit designed to help low-income taxpayers. It is used to adjust the individual income tax structure to reflect a family's reduced ability to pay taxes as the family size increases. Refundable tax credits can be used to reduce a taxpayer's tax liability to zero. Any excess of the credit beyond the tax liability can be refunded to the taxpayer.
Antivirus	Detects, prevents, and removes viruses, worms, and other malware from a computer. Antivirus programs include an automatic update feature that permits the program to download profiled or new viruses, enabling the system to check for new threats.
Application	A software program hosted by an information system.
Appropriation	Statutory authority to incur obligations and make payments out of Treasury funds for specified purposes.
Arbitrary File Download	Abusing the download functionality of a web application, which fails to restrict the user input to a specific directory. The user input goes beyond the directory and is able to download other critical files of the system.
Artifact	The output of an activity performed in a process/procedure, which is created throughout the life cycle of a project.
Assembly Language Code	A low-level computer language initially used in the1950s.
Asset Manager	KISAM module that tracks information technology and non–information technology equipment used throughout the IRS.

Term	Definition
Assignment Code	There are five assignments in the KISAM-AM module that identify the status of an asset at any given time: In Use, In Stock, Missing, Retired, and Awaiting Receipt.
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
Audit Plan	Used as guidance for the implementation of configuration-specific audit settings for the operating systems and software for which they are intended.
Audit Trail	A record showing who has accessed an information technology system and what operations the user has performed during a given period.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official; excludes separately authorized systems to which the information system is connected.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Barcode	A unique series of alphanumeric characters for each asset record in the KISAM-AM module that are associated with a unique series of varying width lines. The unique series of varying width lines are printed on a tag and affixed to the associated asset for identification by an optical scanner.
Buffer	Temporary data storage area.
Buffer Overflow	A condition wherein the data transferred to a buffer exceed the storage capacity of the buffer and some of the data "overflow" into another buffer, one that the data were not intended to go into.
Bug	An error or defect in software or hardware that causes a program to malfunction.
Building Code	Identifies the building location of an asset.

Term	Definition
Business Case	Structured proposal for business improvement that functions as a decision package for organizational decisionmakers. It includes an analysis of business process performance and associated needs or problems, proposed alternative solutions, assumptions, constraints, and a risk-adjusted cost-benefit analysis.
Business Master File	The IRS database that consists of Federal tax-related transactions and accounts for businesses. These include employment taxes, income taxes on businesses, and excise taxes.
Business Process	The method that the enterprise must follow to conduct its business successfully.
Business Unit	A title for major IRS organizations such as Appeals, Wage and Investment, the Office of Professional Responsibility, Information Technology, *etc*.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.
Capacity Management	The process responsible for ensuring that the capacity of information technology services and the information technology infrastructure is able to meet agreed capacity and performance-related requirements in a cost-effective and timely manner. Capacity Management considers all resources required to deliver an information technology service and is concerned with meeting both the current and future capacity and performance needs of the business. Capacity Management includes three subprocesses: business capacity management, service capacity management, and component capacity management.
Capital Planning and Investment Control Process	A management process for the ongoing identification, selection, control, and evaluation of investments in information resources focused on agency missions and achieving specific program outcomes.
Certifying Official	The official held accountable and responsible for verifying and certifying assets under his or her respective control and stewardship. The official is responsible for ensuring that proper action is taken to research, resolve, and correct anomalous asset records in the KISAM-AM module.
Change Control	The procedures to ensure that all changes are controlled, including the submission, recording, analysis, decisionmaking, approval, implementation, and post-implementation review of the change.

Term	Definition
Chief Information Officer	Leads the 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.
Cipher Lock	Makes use of a feature keypad in place of a standard keyhole. This type of lock provides easy access to any building by the use of a numerical pin code in place of a key.
Civil Service	Branches of public service concerned with all Government functions outside the armed services.
Class A Hardware Asset	Capital high-end assets that include mainframe computers, desktop and laptop computers, servers, routers, firewalls, and network printers.
Class B Hardware Asset	Assets that include personal digital assistants, smartphones, and stick personal computers.
Common Business Oriented Language	A computer programming language that reads like regular English and is often used for business and administrative purposes.
Common Vulnerability Scoring System	Provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities.
Computer Security Incident Response Center	Part of the IRS's Information Technology Cybersecurity organization. The Computer Security Incident Response Center's mission is to ensure that the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify and eradicate cyber threats or cyberattacks. One of its primary duties is to perform 24-hour monitoring and support to IRS operations.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Contingency Planning	The process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively affects the organization.
Continuous Integration	A software development practice in which developers integrate working copies of software into a shared repository one time or more each day, verifying code check-ins through an automated build process.

Term	Definition
Continuous Monitoring	The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) developing a strategy to regularly evaluate selected Information Assurance controls/metrics; 2) recording and evaluating relevant events and the effectiveness of the enterprise in dealing with those events; 3) recording changes to controls or changes that affect risks; and 4) publishing the current security status to enable information-sharing decisions involving the enterprise.
Contractor	An organization external to the IRS that supplies goods and services according to a formal contract or task order.
Corrective Action	Identification and elimination of the causes of a problem, thus preventing their recurrence.
Council of the Inspectors General on Integrity and Efficiency	An independent entity established within the Executive Branch to address integrity, economy, and effectiveness of issues that transcend individual Government agencies and aid in the establishment of a professional, well-trained, and highly skilled workforce in the Offices of Inspectors General.
Criminal Investigation	An IRS business unit that serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.
Customer Account Data Engine 2	Establishes a single database that houses all individual taxpayer accounts, including IMF data, which provides IRS employees the ability to view updated account information online.
Data at Rest	In the context of data handling systems, data at rest refers to data that are being stored in stable destination systems. Data at rest are frequently defined as data that are not in use and are not traveling to system endpoints, such as mobile devices or workstations.
Data Breach	An incident in which sensitive, protected, or confidential data have potentially been viewed, stolen, or used by an individual unauthorized to do so.
Data Exfiltration	The unauthorized transfer of data from a computer.
Data Loss Prevention	A strategy for ensuring that end users do not send sensitive or critical information outside the organization's network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

Term	Definition
Data Retrieval Tool	Accessible from the FAFSA.gov[1] 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.
Database	A computer system with a means of storing information in such a way that information can be retrieved.
Defense Information Systems Agency	A combat support agency that provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations.
Department of the Treasury's Financial Agent	A bank that operates the EFTPS. It is responsible for moving taxpayer payments from the taxpayer to the Treasury General Account as well as reconciling payment data with the Federal Reserve System and transmitting the EFTPS payment and deposit information electronically to the IRS.
Desktop Computer	A computer that is designed to stay in a single location, cannot be powered from an internal battery, and therefore must remain connected to a wall outlet.
Digital Assistant	A portable device that functions as a personal information manager and is used for web browsing, office applications, watching videos, viewing photos, or as a mobile phone.
Direct Pay System	A system that can be accessed through IRS.gov where individual taxpayers can make payments to the IRS from their bank account.
Disaster Recovery Server	A server dedicated to testing the ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.
Domain Controller	A server that is running a version of the Windows® Server operating system and has Active Directory Domain Services installed.

[1] FAFSA = Free Application for Federal Student Aid.

Term	Definition
Drive	A computer component used to store data; may be a static storage device or may use removable media.
Earned Income Tax Credit	A tax credit for certain people who work and have income under established limits.
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.
Electronic Federal Payment Posting System	Used by the IRS to process and record payments received through the Department of the Treasury's EFTPS and payments received via paper check converted into electronic payments.
Electronic Federal Tax Payment System	Provides a free service for taxpayers to make Federal tax payments and for the IRS to process these payments.
Electronic Return Originator	The authorized IRS electronic filing provider that originates the electronic submission of a return to the IRS.
Embedded Systems	Some combination of computer hardware and software, either fixed in capability or programmable, that is designed for a specific function(s) within a larger system. Embedded systems are computing systems, but they can range from having no user interface to complex graphical user interfaces, such as in mobile devices.
Employer Identification Number	Also known as a Federal Tax Identification Number, it is used to identify a business entity.
Encryption	Conversion of plain text to cipher text through the use of a cryptographic algorithm.
End-to-End Encryption	A method of secure communication that prevents third parties from accessing data while it's transferred from one end system or device to another.
Entellitrak®	A commercial off-the-shelf software consisting of preconfigured applications that reflect best practices, business rules, and terminology for case management solutions.
Enterprise Case Management Solution	Designed to provide core case management capabilities that are commonly used, *e.g.*, create case, assign case, close case, across all IRS business units.
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.

Term	Definition
Enterprise Service Desk	Made up of a dedicated number of staff responsible for dealing with a variety of service activities, usually made via telephone calls, web interface, or automatically reported infrastructure events.
Equifax®	One of the three largest nationwide credit bureaus that provide lenders, employers, and other entities with reports that are commonly used to determine eligibility for credit, employment, and insurance. Equifax also provides services to organizations, including income and employment verification, risk-based authentication tools, and identity validation.
eServices	Provides a set of web-based business products as incentives to third parties to increase electronic filing; also provides electronic customer account management capabilities to all businesses, individuals, and other customers.
Executable Files	Files that are used to perform various functions or operations on a computer.
Exploit	A general term for any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.
Facilities Management and Security Services	Provides IRS nationwide facilities and security services.
Federal Chief Information Officer Council	As the principal interagency forum on Federal information technology, the purpose of the Federal CIO Council is to foster collaboration among Federal Government CIOs in strengthening Governmentwide information technology management practices.
Federal Information Processing Standard	A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by the NIST. A Federal Information Processing Standard covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.
File Permissions	System settings that determine who can access specified files and what they can do with those files.
File Transfer Protocol	A standard set of rules used to exchange and manipulate files over a network, such as the Internet.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.

Term	Definition
Firewall	A gateway that limits access between networks in accordance with local security policy.
Firmware Component	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
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.
Forest	A complete instance of active directory. Each forest acts as a top-level container in that it houses all domain containers for that particular active directory instance.
Full-Time Equivalent	A measure of labor hours in which one full-time equivalent is equal to eight hours multiplied by the number of compensable days in a particular fiscal year.
Gateway	Serves as the entry and exit point of a network; all data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths. Generally, a router is configured to work as a gateway device in computer networks.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Get Transcript	Allows taxpayers to view and download their tax information, such as account transactions, line-by-line tax return information, and income reported to the IRS. Taxpayers can download or print five distinct transcript types: tax account, tax return, record of account, wage and income, and verification of nonfiling.
Hackers	Unauthorized users who attempt to gain or do gain access to an information system.
Hardware	The physical parts of a computer and related devices. It includes motherboards, hard drives, monitors, keyboards, mice, printers, and scanners.
Hash	A hash value (or simply hash) is a number generated from a string of text. Hashing produces hash values for accessing data or for security.

Term	Definition
High Value Assets	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical Federal operations or house unique collections of data (by size or content), making them of particular interest to criminal, politically-motivated, or State-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the Government.
Host	A workstation or server.
Hypervisor	The virtualization component that manages the guest operating systems on a host and controls the flow of instructions between the guest operating systems and the physical hardware. It is also described as software that allows a single host to run one or more guest operating systems as well as can be referred to as a virtual machine manager.
Income and Verification Express Services	Used by mortgage lenders and others within the financial community to confirm the income of a borrower during the processing of a loan application. The IRS provides return, Form W-2, *Wage and Tax Statement*, and Form 1099-MISC, *Miscellaneous Income*, transcript information to a third party with the consent of the taxpayer.
Incremental Development	For the development of software or services, it is defined as planned and actual delivery of new or modified technical functionality to users occurring at least every six months.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Individual Taxpayer Identification Number	A tax processing number issued by the IRS to individuals who are required to have a U.S. TIN but who do not have and are not eligible to obtain a Social Security Number from the Social Security Administration.
Information System Component Inventory	An inventory of information system components that accurately reflects the current information system, includes all components within the authorization boundary of the information system, and includes all IRS-defined information deemed necessary to achieve effective information system component accountability.
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 Hardware Asset Inventory	Equipment or property that are part of the information technology infrastructure in use, in stock, or awaiting disposal.
Information Technology Investment	The expenditure of resources on selected information technology or information technology–related initiatives with the expectation that the benefits from the expenditure will exceed the value of the resources expended.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Information Technology Project	An organizational initiative that employs or produces information technology assets. Each project has or will incur costs, expects or will realize benefits, has a schedule of project activities and deadlines, and has or will incur risks.
Integrated Data Retrieval System	IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.
Integrated Enterprise Portal	The IRS Internet portal that allows registered individuals to access selected tax data and other sensitive applications.
Interactive Voice Response System	A service provided by each of the credit and debit card processors to allow taxpayers to make payments by telephone using a voice prompt system.
Internal Revenue Manual	The IRS's primary source of instructions to its employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Internal Revenue Service Strategic Plan	The IRS designed this plan to allow employees to see their contribution to the IRS mission and to set forth key goals to guide the agency over the next four years. The IRS will use this plan to guide operations across its organization. The IRS will monitor its progress against the plan on a recurring basis, review its organizational performance, study changes in its environment, and update the plan as needed.
Internet Protocol	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Internet Protocol Address	A 32-bit number that uniquely identifies a host, *e.g.*, computer or other device, such as a printer or router, on a Transmission Control Protocol/Internet Protocol network.
Inventory	To take stock of assets. A detailed list of assets.

Term	Definition
Item Tracking, Reporting, and Control System	IRS system used to track and report on issues, risks, and action items.
Knowledge Incident/Problem Service Asset Management	A system that maintains the complete inventory of information technology and non–information technology organizational assets as well as computer hardware and software. It is also the reporting tool for problem management with all IRS-developed applications and shares information with the IRS Enterprise Service Desk.
Knowledge Incident/Problem Service Asset Management Record	An asset record in the KISAM-AM module that includes fields such as Assignment Code, Barcode, Serial Number, Building Code, User Name, Contact Name, Purchase Price, Inventory Date, Model, Manufacturer, and other information used to identify the asset.
Laptop Computer	A portable computer that can be carried and used in different environments and has a battery that allows it to operate without being plugged in to a power outlet.
Legacy System	A computer system that has been in existence for a long period of time.
Limited Area	An area in a building to which access is limited to authorized personnel only. All who access a limited area must have a verified official business need to enter.
Lockbox Site	In the Lockbox program, the Department of the Treasury agrees to let certain financial institutions process individual and business tax payments. Financial institutions, or sites, deposit the taxpayer's payment and forward any tax forms or documentation to the IRS as quickly and efficiently as possible. The nationwide Lockbox Network was established on behalf of the Department of the Treasury, the IRS, and the Bureau of the Fiscal Service. As a fiduciary of the IRS, the Lockbox Network processes sensitive, private information pertaining to U.S. citizens, financial information, proprietary information, and mission-critical information. The Lockbox Network has a legal obligation to protect the confidentiality of tax returns and related information.
Mainframe	A powerful, multiuser computer capable of supporting many hundreds of thousands of users simultaneously.
Mainframes and Servers Services and Support System	Represents approximately 73 percent of the IRS's information technology infrastructure and encompasses the design, development, and deployment of servers, and middleware and large systems as well as enterprise storage infrastructures, including systems software products, databases, and operating systems.

Term	Definition
Major Incident	Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
Major Investment	Department of the Treasury criteria states that major information technology investments have an annual cost equal to or greater than $5 million, have total costs exceeding $50 million for a five-year rolling period of performance, or significantly affect more than one bureau.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. It includes a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Master File	A computer record containing information about taxpayers' filing of returns and related documents for both individual tax returns, *i.e.*, IMF, and business tax returns, *i.e.*, Business Master File. The Master File contains information on the current year plus all years that have had activity within the two previous years. In addition, the Master File maintains retention register files on taxpayers for two additional years.
MD5	A hashing algorithm that is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.
Microcode	The lowest specified level of processor and machine instruction sets. It is a layer comprised of small instruction sets, which are derived from machine language. Microcode performs short, control-level register operations, including multiple micro instructions, each of which performs one or more micro operations.
Modernization	Modernization is the process of updating, improving, and bringing processes and technology in line with modern standards. Modernization is an IRS program that includes Organization Modernization and Business System Modernization.
Modernized e-File	The IRS's electronic filing system that enables real-time processing of tax returns while improving error detection, standardizing business rules, and expediting acknowledgements to taxpayers. The system serves to streamline filing processes and reduce the costs associated with a paper-based process.

Term	Definition
Multifactor Authentication	A characteristic of an authentication system or a token that uses two or more authentication factors to achieve authentication. The three types of authentication factors are something you know, something you have, and something you are.
National Institute of Standards and Technology	Part of the Department of Commerce. The NIST develops management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of "other than national security"–related information in Federal information systems.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Office of Management and Budget	The OMB's predominant mission is to assist the President in overseeing the preparation of the Federal budget and to supervise administration in Executive Branch agencies. The OMB evaluates the effectiveness of agency programs, policies, and procedures and oversees and coordinates the Administration's procurement, financial management, information, and regulatory policies.
Office of Personnel Management	Serves as the chief human resources agency and personnel policy manager for the Federal Government.
Online 5081 System	A web-based application that allows users to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems. The application also allows the IRS to track user access history, generate reports, and document an audit trail of user actions.
Operating System	The software that serves as the user interface and communicates with computer hardware to allocate memory, process tasks, and access disks and peripherals.
Operational Analysis	The process of reviewing the performance of an operational, *i.e.*, steady-state, investment and measuring its performance against cost, schedule, and performance goals. The operational analysis should trigger considerations of how the investment's objectives could be better met, how costs could be reduced, and whether the organization should continue performing a particular function.
Oracle®	A relational database management system produced by the Oracle Corporation, which is the largest software company whose primary business is database products.

Term	Definition
Packet	A message that is broken into smaller units and may be addressed and routed through a computer network.
Partitioned Server	A reserved part of a storage drive that is treated as a separate server.
Patches	Updates to an operating system, application, or other software issued specifically to correct particular problems with the software.
Path	In disk operating systems and Windows systems, a path is a list of directories where the operating system looks for executable files if it is unable to find the file in the working directory.
Personal Identification Number	A password consisting only of numbers.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, *etc.*, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, *etc*.
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
Physical Server	A server on which an operating system, like Windows or Linux, runs just as on any other computer. The physical servers are in almost all aspects like desktop computers.
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.
Portal	The web-based infrastructure, *e.g.*, hardware and software, that serves as the entry point for web access to IRS applications and data.
Portfolio	The combination of all information technology assets, resources, and investments owned or planned by an organization in order to achieve its strategic goals, objectives, and mission.

Term	Definition
Post-Implementation Review	The process of reviewing information technology investments to determine whether the expected performance and financial benefits anticipated in the business case have been realized. A post-implementation review provides decisionmakers with lessons learned so they can improve investment decisionmaking processes. One of the primary objectives of a post-implementation review is to ensure continual improvement of an agency's capital programming processes based on lessons learned.
Privacy Impact Assessment	An analysis of how information is handled: 1) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged Access/Account/User	Any user right assignment that is above the organization's baseline for regular users. Sometimes referred to as system or network administrative accounts.
Privileges	Rights granted to an individual, a program, or a process.
Production Environment	The location where the real-time staging of programs that run an organization are executed; this includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
********2*******	***********************2******************************* ***********************2******************************* ***********************2******************************* ***********************2*******************************.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Requirement	The formalization of a need and the statement of a capability or condition that a system, subsystem, or system component must have or meet to satisfy a contract, standard, or specification.
Return Review Program	An IRS system used to identify potentially fraudulent electronically filed tax returns. It enhances the IRS's capabilities to detect, resolve, and prevent criminal and civil noncompliance and reduces issuance of fraudulent tax refunds.

Term	Definition
Risk	A potential event that could have an unwanted impact on the cost, schedule, business, or technical performance of an information technology program, project, or organization.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation arising through the operation of an information system.
Risk-Based Decision	A decision made when meeting a requirement is technically or operationally not possible or is not cost-effective. It is required for any situation in which the system will be operating outside of IRS information technology security policy or the NIST guidelines, whether related to a technical, operational, or management control.
Router	A device or, in some cases, software on a computer, that determines the best way for a packet to be forwarded to its destination.
Security Accounts Manager	A database in the Windows operating system that contains user names and passwords.
Security Assessment Report	Provides the stakeholders with an assessment of the adequacy of the security and privacy controls used to protect the confidentiality, integrity, and availability of the system and the data it stores, transmits, or processes.
Security Breach	Any incident that results in unauthorized access of data, applications, services, networks, or devices by bypassing their underlying security mechanisms. A security breach is also known as a security violation.
Security Change Advisory Board	Meets weekly to review all IRS security change requests and collaborates to determine the FISMA Inventory Level of a system. During these meetings, the current status of each security change request is reviewed and updated, with next steps determined and any open issues discussed.
Security Patch	A fix to a program that eliminates a vulnerability exploited by malicious hackers.
Serial Number	A unique combination of alpha characters and numeric digits affixed to an asset.
Server	A system capable of managing and running virtual machines. It is also a process capable of accepting and running instructions from another process.

Term	Definition
Session	The period of time a user interfaces with an application. The user session begins when the user accesses the application and ends when the user quits the application.
Severity Rating	One of five levels on a ratings scale to describe the risk associated with a vulnerability. The complete scale from the lowest risk to the highest risk is: Informational, Low, Medium, High, and Critical.
Shares	Resources such as files, folders, or printers that have been made available (sharable) to other users on the network.
Smart ID Card	A plastic card that contains a microprocessor and a memory chip or just a memory chip. The microprocessor card has the ability to add, delete, and manipulate information on the card.
Smartphone	A mobile telephone with highly advanced features that typically has a high-resolution touch screen display, wireless connectivity, web browsing capabilities, and the ability to accept sophisticated applications.
Social Security Number	Assigned at birth, the Social Security Number enables Government agencies to identify individuals in their records and businesses to track an individual's financial information.
Software	A general term that describes computer programs and consists of lines of code written by computer programmers that have been compiled into a computer program.
Solution	An aggregation of products and services, as opposed to a single discreet system or piece of software, that helps solve a particular problem.
Steady-State	Investments that include all routine maintenance and operational costs at a current capability and performance level, including costs for personnel, maintenance of existing information systems, corrective software maintenance, voice and data communications maintenance, and replacement of broken information technology equipment.
Stick Personal Computer	A type of device that puts all the performance of a personal computer into a small drive that looks similar to a slightly larger version of standard flash drives and universal serial bus storage drives.
Storage Array	A hardware element that contains a large group of hard disk drives. It may contain several disk drive trays and has an architecture that improves speed and increases data protection.
Switches	Small hardware devices that join multiple computers together with local area networks.

Term	Definition
System	A set of interdependent components that perform a specific function and are operational. It may also include software, hardware, and processes.
System Boundary	The physical or logical perimeter of a system.
System Log	System or device-related entries consisting of the message type and severity, a timestamp, the hostname or Internet Protocol address of the source of the log, and log content.
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Systems Development Server	A type of server that is designed to facilitate the development and testing of programs, websites, software, or applications for software programmers.
Task Order	An order for services placed against an established contract or with Government sources.
Tax Day	The annual deadline to file tax returns and pay income taxes with the IRS. The date is typically on or around April 15.
Tax Transcript	Shows most line items, *e.g.*, marital status, the type of return filed, adjusted gross income, and taxable income, from an original filed tax return, including items from any accompanying forms and schedules.
Tax Year	A 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.
Taxpayer Assistance Center	Local IRS office where taxpayers can meet face-to-face with an IRS representative and ask questions, make payments, and get copies of tax returns and tax account transcripts.
Taxpayer Identification Number	A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is either an Employer Identification Number, a Social Security Number, or an Individual Taxpayer Identification Number.
Testing Server	A type of server that allows safe testing of dynamic software code without impacting a live environment.
Tier I Environment	A computing infrastructure consisting of mainframe computers that handle a high volume of critical operational data.

Term	Definition
Tier II Environment	A computing infrastructure consisting of nonmainframe servers. These servers run various operating systems. The servers may also operate as database, web, e-mail, and file servers and provide a host of other important functions supporting the IRS network infrastructure.
Transmission Control Protocol	A communications protocol based on the U.S. Department of Defense's standards for reliable internetwork delivery of data.
Treasury Cyber Analysis and Reporting Dashboard	A product of the Department of the Treasury's Cyber Security Dashboard, which provides an executive overview of the Department of the Treasury's security posture to its stakeholders.
********2*******	***********************2*************************** ***********************2*************************** ***********************2*************************** ***********************2*************************** ***********************2*************************** ***********************2*******.
********2*******	***********************2*************************** *******2*******.
Trivial File Transfer Protocol	An Internet software utility for transferring files that is simpler to use than the File Transfer Protocol but less capable. It is used where user authentication and directory visibility are not required.
Two-Factor Authentication	A method of confirming a user's claimed identity by utilizing a combination of two different components. These components may be something that the user knows, something that the user possesses, or something that is inseparable from the user.
U.S. Computer Emergency Readiness Team	This team acts as the Federal information security incident center for the Federal Government per the FISMA.
********2*******	***********************2*************************** ***********************2*************************** *******2*******.
USAccess	Provides Federal Government agencies with identity credential solutions. This shared service provides an efficient, economical, and secure infrastructure to support agencies' credentialing needs.
Virtual Machine/Virtual Server	A simulated environment created by virtualization, also described as a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer.

Term	Definition
Volunteer Income Tax Assistance program	Specially trained IRS volunteers who offer free assistance with tax return preparation and tax counseling to individuals with low to moderate incomes, those with disabilities, and those for whom English is a second language.
Vulnerability	A flaw or weakness in an information system's design, implementation, or operation and management that could potentially be exploited by a threat to gain unauthorized access to information, disrupt critical processing, or otherwise violate the system's security policy.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten the network's security.
Wage and Investment Division	IRS organization that serves taxpayers whose only income is derived from wages and investments.
Windows Policy Checker	An application that validates applicable Internal Revenue Manual security requirements on computers that use the Microsoft® Windows operating system.