TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the Internal Revenue Service's Information Technology Program for Fiscal Year 2019

September 27, 2019

Reference Number: 2019-20-083

Redaction Legend:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions
11 = Disclosure of the Information is Prohibited by Statute or Federal Regulation

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

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.

ANNUAL ASSESSMENT OF THE INTERNAL REVENUE SERVICE'S INFORMATION TECHNOLOGY PROGRAM FOR FISCAL YEAR 2019

Highlights

Final Report issued on September 27, 2019

Highlights of Reference Number: 2019-20-083 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

In Fiscal Year 2018, the IRS collected approximately $3.5 trillion in Federal tax payments, processed approximately 253 million tax returns and other forms, and paid approximately $464 billion in refunds to taxpayers. In addition, the IRS employs approximately 78,700 people in its Washington, D.C., headquarters and its more than 530 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. 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the IRS's information technology program could result in computer operations that become compromised, disrupted, or outdated, which could adversely affect the IRS's ability to meet its mission of providing America's taxpayers with top-quality service by helping them understand and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 information technology program 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 rated three of five *Cybersecurity Framework* functions as "effective." 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 in compliance with the requirements of the Federal Information Security Modernization Act of 2014.

Problems were also reported in the IRS's handling of the privacy of taxpayer data, system access controls, system environment security, disaster recovery, separation of duties, system security and privacy training, and system security documentation.

In our reviews of systems development and information technology operations, TIGTA found that the IRS completed extensive programming and systems changes in a compressed time frame and started the 2019 Filing Season on January 28, 2019, which is within the normal time frame.

However, TIGTA also found that inadequate governance of the Solaris® to Linux® migration project contributed to significant delays with total project costs of $56.2 million. Problems were also reported with the IRS's information technology acquisitions, hardware and software asset management, governance and project management, information technology service and helpdesk requests, and risk management.

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 2019, TIGTA did not make any further recommendations.

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

September 27, 2019

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 2019 (Audit # 201920007)

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 2019. This review is required by the IRS Restructuring and Reform Act of 1998.[1] This audit is included in our Fiscal Year 2019 Annual Audit Plan and addresses the major management challenges of *Security Over Taxpayer Data and Protection of IRS Resources*; *Implementing the Tax Cuts and Jobs Act and Other Tax Law Changes*; *Identity Theft and Impersonation Fraud*; *Improving Tax Reporting and Payment Compliance*; 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 (codified as amended in scattered sections of 2 U.S.C., 5 U.S.C. app., 16 U.S.C., 19 U.S.C., 22 U.S.C., 23 U.S.C., 26 U.S.C., 31 U.S.C., 38 U.S.C., and 49 U.S.C.).

Table of Contents

Appendices

Abbreviations

BYOD	Bring Your Own Device
CI	Criminal Investigation
CIO	Chief Information Officer
DLP	Data Loss Prevention
EEU	Enterprise Exchange Upgrade
e-file(d); e-filing	Electronically file(d); Electronic Filing
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act of 2014
GAO	Government Accountability Office
GSS	General Support System
IBM	International Business Machines®
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
P	Priority
PCLIA	Privacy and Civil Liberties Impact Assessment
PGLD	Privacy, Governmental Liaison and Disclosure
PII	Personally Identifiable Information
RAFT	Risk Acceptance Form and Tool
TIGTA	Treasury Inspector General for Tax Administration

Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998[1] requires the Treasury Inspector General for Tax Administration (TIGTA) to annually evaluate the adequacy and security of the IRS's information technology program.[2] TIGTA's Security and Information Technology Services business 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 2019.

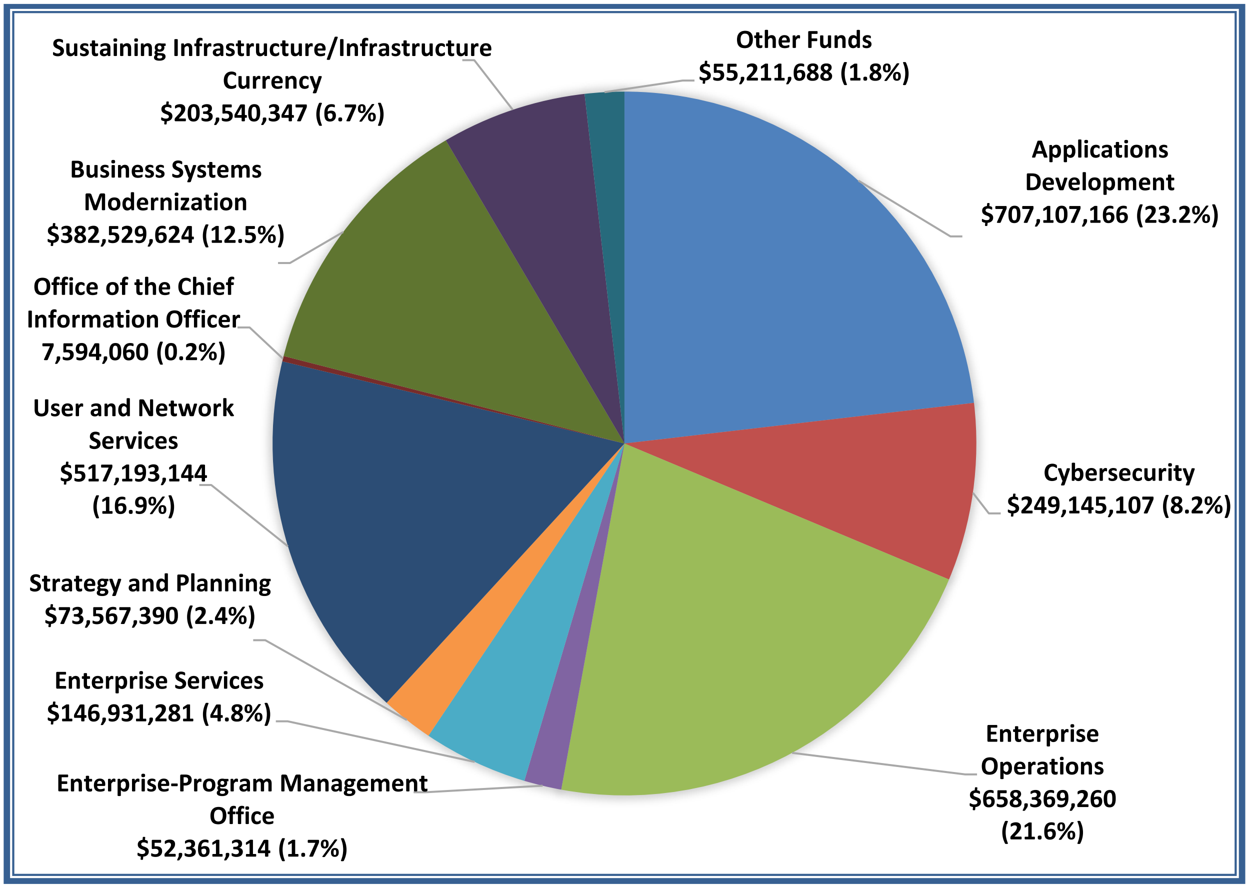
The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In Fiscal Year 2018, the IRS collected approximately $3.5 trillion in Federal tax payments, processed approximately 253 million tax returns and other forms, and paid approximately $464 billion in refunds to taxpayers. Further, the size and complexity of the IRS add unique operational challenges. The IRS employs approximately 78,700 people in its Washington, D.C., headquarters and its more than 530 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 taxpayers.

In Fiscal Year 2019, the IRS's appropriations decreased by $100 million to $11.3 billion, of which $77 million designated for taxpayer services, enforcement, and operations support was to be used for implementing the Tax Cuts and Jobs Act of 2017.[3] However, the Information Technology (IT) organization did not receive a portion of this designated funding amount.[4]

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 2019 projected available funds included about $3.1 billion for information technology investments, representing 27.4 percent of the total IRS budget, down from approximately $3.2 billion in Fiscal Year 2018. Figure 1 illustrates the IRS's Fiscal Year 2019 information technology funding by IT organization function and major program.

[1] Pub. L. No. 105-206, 112 Stat. 685.
[2] See Appendix V for a glossary of terms.
[3] Pub. L. No. 115-97.
[4] In Fiscal Year 2018, the IT organization received $275 million for implementing the Tax Cuts and Jobs Act of 2017.

Figure 1: Fiscal Year 2019 Information Technology Funding by IT Organization Function and Major Program[5]

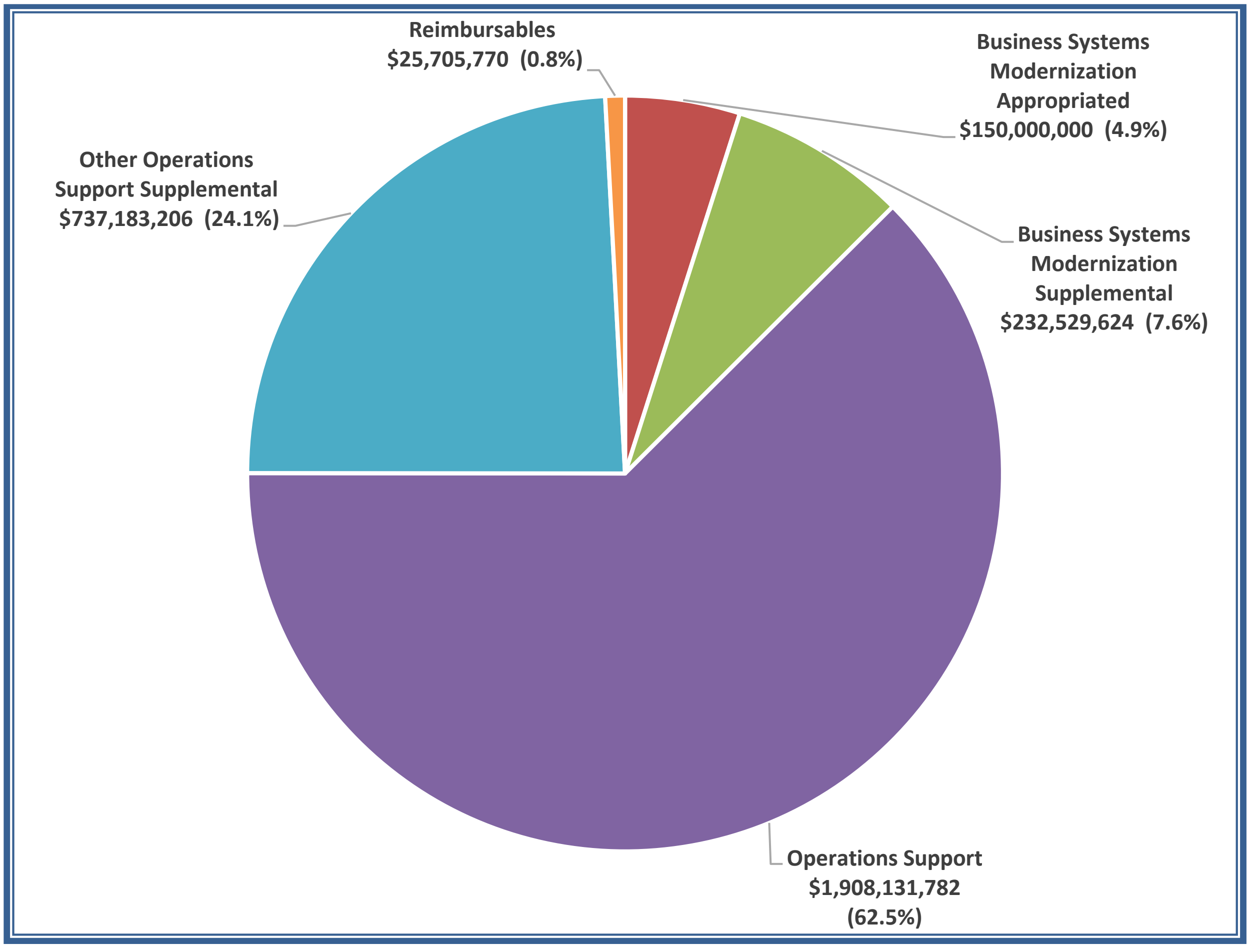


Source: The IT organization budget data as of May 2019, based on information provided by the Strategy and Planning function's Office of Financial Management Services. The Other Funds category includes Shared Support and multiyear funds.

Figure 2 shows the IT organization funding for Fiscal Year 2019 by funding source.

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

Figure 2: Fiscal Year 2019 Total Available Funding by Funding Source[6]



Source: The IT organization budget data as of May 2019, based on information provided by the Strategy and Planning function's Office of Financial Management Services.

Figure 3 illustrates that, as of May 2019, the IRS had a total of 7,096 employees working across eight different IT organization functions, 585 more employees than in Fiscal Year 2018.

[6] The percentages do not add up to 100 percent due to rounding.

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

IT Organization Function	Number of Employees
Applications Development	2,015
Enterprise Operations	1,933
User and Network Services	1,321
Enterprise Services	753
Cybersecurity	457
Strategy and Planning	310
Enterprise-Program Management Office	290
Office of the Chief Information Officer (CIO)	17
Total	7,096

Source: IRS Human Resources Reporting Center as of May 2019.

- **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** provides crosscutting services and support functions that help bring coordination and assistance to programs and projects within the IRS.
- **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, 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 as well as implementing new information system functional capabilities.
- **The Office of the CIO** includes the CIO, three Deputy CIOs, and their staff. Deputy CIOs serve as principal advisors to the CIO and provide 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 2019. The information presented is derived from TIGTA and Government Accountability Office (GAO) reports issued during Fiscal Year 2019 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 development, operations, and security as required by the IRS Restructuring and Reform Act of 1998. During Fiscal Year 2019, TIGTA audits of the information technology program addressed the IRS major management challenges of *Security Over Taxpayer Data and Protection of IRS Resources*; *Implementing the Tax Cuts and Jobs Act and Other Tax Law Changes*; *Identity Theft and Impersonation Fraud*; and *Achieving Program Efficiencies and Cost Savings*. This report presents a summary of TIGTA and GAO audit results for Fiscal Year 2019.

The IRS has made progress in many information technology program 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.

Integrated Modernization Business Plan

Successful modernization of IRS systems and the development and implementation of new information technology applications are critical to meeting the IRS's evolving business needs and enhancing services provided to taxpayers. The reliance on legacy systems, aged hardware and software, and use of outdated programming languages pose significant risks to the IRS's ability to deliver its mission. The cost to operate the current information technology infrastructure now exceeds $2.2 billion annually and is expected to exceed $3 billion annually by Fiscal Year 2026 if current trends continue. Modernization is necessary to deliver efficient taxpayer services and enforcement with enhanced user experiences, and to curtail the rising operational costs. Modernizing the computer systems has been a persistent challenge for many years and will likely remain a challenge for the foreseeable future. To address the modernization challenge, the IRS developed the *IRS Integrated Modernization Business Plan* (hereafter referred to as the *Business Plan*), dated April 2019.

The *Business Plan* provides a six-year roadmap for achieving necessary modernization of IRS systems and taxpayer services in two three-year phases beginning in Fiscal Year 2019. The IRS organized the plan around four "Modernization Pillars" that are critical to its mission and future development: 1) *Taxpayer Experience*, 2) *Core Taxpayer Services and Enforcement*, 3) *Modernized IRS Operations*,; and 4) *Cybersecurity and Data Protection*. The IRS budgeted $300 million for this effort in Fiscal Year 2019 and an equivalent amount in Fiscal Year 2020. The IRS estimates costs of approximately $2.3 billion to $2.7 billion over six years to fully implement this plan. Annual funding levels will, in part, determine the speed at which the IRS delivers modernization of its systems and taxpayer services.

The IRS reported that it will deliver incremental value each year after implementing the modernization technology and transitioning it into operations. Once the *Business Plan* is fully executed, the IRS also reported it will:

- Promote ease and simplicity in taxpayer interactions as well as deliver a customer experience in line with its priority goal, *e.g.*, increase on the American Customer Satisfaction Index score and the Enterprise Self-Assistance Participation Rate.
- Protect revenue by improving the ability to identify fraudulent returns and assisting victims of identity theft, *e.g.*, reduce unprotected identity theft refunds paid by 2 percent.
- Expand opportunities and assistance for voluntary compliance and enhance systemic identification of noncompliance and fraud, *e.g.*, increase taxes collected as a percentage of taxes owed and audit efficiency.
- Stabilize operations and maintenance costs in line with industry standards, *e.g.*, reduce and then sustain aged infrastructure at 25 percent, and retire 50 percent of the legacy programming code.
- Minimize the risk of catastrophic system failure and data breaches, *e.g.*, ensure high service availability with 100 percent of critical systems at the appropriate level of redundancy, and protect systems with 100 percent of applications at assessed level of risk, *e.g.*, systems have completed annual security and change-event driven security assessments, or mitigated with compensating controls.

The IRS further reported that delivering the *Business Plan* will enable the IRS to:

- Significantly improve the taxpayer experience by standardizing customer workflows and expanding access to information.
- Reduce call wait and case resolution times with customer callback technology, online notices, and live online customer support.
- Expedite return and refund processing with real-time return processing and taxpayer error correction.
- Simplify identity verification to expand access to online services while protecting data.
- Increase systems availability for taxpayers and practitioners.
- Implement new tax provisions enacted by Congress by eliminating millions of lines of legacy code based on historical provisions and customizations.
- Consistently provide superior service to taxpayers and deliver long-term budget efficiencies as the IRS decommissions legacy applications, automates manual processes,

and expands advanced analytics programs to more effectively serve and bring taxpayers into compliance.

- Stabilize the rising cost (hundreds of millions of dollars) associated with maintaining legacy applications and infrastructure, creating opportunities to reinvest savings to keep technology current and grow digital services consistent with similar trends in the private sector.

Success of the *Business Plan* will be dependent on a number of special legislative proposals and regulatory authorities that the IRS believes are appropriate for an effort of this scope and importance. This includes:

- Engaging the Office of Personnel Management to use existing direct hire authority for information technology modernization positions and broadening Governmentwide critical pay authority. As of July 20, 2019, the IRS stated it has used an IT organization-wide direct hiring authority to onboard 371 candidates through Fiscal Year 2019 and plans to continue the onboarding efforts until it meets its approved allocation of 426 candidates. In addition, the IRS received a separate approval for direct hiring authority in support of cybersecurity.
- Ensuring funding is available for multiple fiscal years at somewhat predictable intervals.[7]

<u>Legislation affecting the IT organization</u>

During the past few calendar years, two pieces of major legislation were passed that affects the IT organization. The Taxpayer First Act[8] amended the Internal Revenue Code of 1986 to modernize and improve the IRS. From an information technology perspective, it revised provisions related to the IRS's:

- Cybersecurity and identity protection, *e.g.*, must work collaboratively with the public and private sectors to protect taxpayers from identity theft refund fraud, notify taxpayers of suspected identity theft.
- Development of information technology, *e.g.*, establishes the position of the CIO in the IRS and makes the CIO responsible for the development, implementation, and maintenance of information technology for the IRS, provides for streamlined critical pay authority for IRS information technology positions.
- Modernization of its consent-based income verification system, *e.g.*, must implement a program that ensures that any disclosure of tax information for third-party income verification is fully automated and accomplished through the Internet in as close to real-time as practicable, and prohibit persons who are granted consent by a taxpayer to

[7] As of August 16, 2019, the IRS stated it has submitted its funding requests for Fiscal Years 2020 and 2021 and is awaiting their approval.

[8] Pub. L. No. 116-25.

receive return information from using it for a purpose other than the purpose for which consent was granted.

- Expanded use of electronic systems, *e.g.*, must verify the identity of any individual opening an e-Services account with the IRS before such individual may use e-Service tools, expands the use of electronic systems for filing tax returns.

Further, the sunset dates on several provisions of the Federal Information Technology Acquisition Reform Act of 2014 (FITARA)[9] were reset with the enactment of the FITARA Enhancement Act of 2017.[10] Specifically, the FITARA Enhancement Act extends three provisions that were set to expire in Calendar Years 2018 and 2019 related to:

- Federal data center consolidation – Agencies are required to provide the Office of Management and Budget (OMB) with a data center inventory, the number of data center closures, projected cost savings, and quarterly updates on progress.[11]
- Transparency and risk management of major information technology systems – The OMB and agencies must make publicly available detailed information on Federal information technology investments and require agency CIOs to categorize information technology investments by risk.
- Information technology portfolio, program, and resource reviews – Agencies must annually review information technology investment portfolios in order to increase efficiency and effectiveness and identify potential waste and duplication.

System Security and Privacy of Taxpayer Data

Federal agencies are dependent on information technology systems and electronic data to carry out operations and to process, maintain, and report essential information. Virtually all Federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information technology assets. Hence, the security of these systems and data is vital to public confidence and the Nation's safety, prosperity, and well-being. Ineffective security controls to protect these systems and data could have a significant impact on a broad array of Government operations and assets.

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

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

[11] The FITARA required the Federal Government to consolidate and optimize its data centers by October 1, 2018. The FITARA Enhancement Act of 2017 extended the data center requirements of the FITARA until October 1, 2020. On June 25, 2019, the OMB issued Memorandum M-19-19, *Update to Data Center Optimization Initiative*, to highlight the requirements for the consolidation and optimization of Federal data centers in accordance with the FITARA. It also established targets and metrics for Federal agencies' consolidation and optimization efforts as well as reporting requirements on their progress.

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 that wish to do harm to an organization's systems or steal an organization's data.

For Fiscal Year 2019, TIGTA designated *Security Over Taxpayer Data and Protection of IRS Resources* as the number one major management challenge area for the ninth consecutive year. The IRS faces the daunting task of securing its computer systems against the growing threat of cyberattacks.

In addition to TIGTA's annual Federal Information Security Modernization Act of 2014[12] (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, system access controls, system environment security, disaster recovery, separation of duties, system security and privacy training, and system security documentation.

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 other sources. 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 Fiscal Year 2019 Inspector General FISMA Reporting Metrics were developed as a collaborative effort among 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 2019 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* (hereafter referred to as the *Cybersecurity Framework*)[13]

[12] Pub. L. No. 113-283, 128 Stat. 3703. This bill amends chapter 35 of title 44 of the U.S.C. to provide for reform to Federal information security.

[13] Version 1.1 (April 16, 2018).

and transition the evaluation of all the function areas to the maturity model approach. 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.

Figure 4 shows the alignment of the five *Cybersecurity Framework* function areas to eight Fiscal Year 2019 Inspector General FISMA domains, *i.e.*, security program areas.

Figure 4: Alignment of the NIST Cybersecurity Framework's Function Areas to the Fiscal Year 2019 Inspector General FISMA Domains

Cybersecurity Framework Function Area	Fiscal Year 2019 Inspector General FISMA Domain
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 2019 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 2019 Inspector General FISMA Reporting Metrics specify that, within the context of the maturity model, *Managed and Measurable* (Maturity Level 4), or above, represents an "effective" level of security.[14]

Figure 5: Inspectors General Assessment Maturity Model Spectrum

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 2019 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.[15] We based our Fiscal Year 2019 FISMA review[16] 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 2019 FISMA evaluation period.

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,

[14] NIST, Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 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.

[15] Version 1.3 (April 9, 2019).

[16] TIGTA, Ref. No. 2019-20-082, *Fiscal Year 2019 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act* (Sept. 2019).

due to program components that were not at an acceptable maturity level, the Cybersecurity program was not fully effective.

Based on the Department of Homeland Security's scoring methodology for the Fiscal Year 2019 FISMA evaluation period, we rated three *Cybersecurity Framework* functions as "effective" and two as "not effective," as shown in Figure 6.

Figure 6: Maturity Levels by Function Area

Framework Foundation Function	Assessed Maturity Level	Effective?
IDENTIFY – Risk Management	***Managed and Measurable* (Level 4)**	**Yes**
PROTECT – **Configuration Management** **Identity and Access Management** **Data Protection and Privacy** **Security Training**	 ***Defined* (Level 2)** ***Consistently Implemented* (Level 3)** ***Consistently Implemented* (Level 3)** ***Managed and Measurable* (Level 4)**	**No**
DETECT – Information Security Continuous Monitoring	***Defined* (Level 2)**	**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, were *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 was rated at *Managed and Measurable* (Maturity Level 4) and was therefore considered "effective." However, we determined that the security program component of Configuration Management was rated at *Defined* (Maturity Level 2), and the security program components of Identity and Access Management, and Data Protection and Privacy were rated at *Consistently Implemented* (Maturity Level 3). As a result, these three program components were considered "not effective." Because three of the four program components were "not effective" with the overall result at *Consistently Implemented* (Maturity Level 3), we rated the entire function area as "not effective."

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

- Specifically address the allocation of resources, *e.g.*, people, processes, and technology, in a risk-based manner and accountability for effectively carrying out roles and responsibilities for configuration management.
- Ensure that policy and procedures for maintaining baseline configurations or component inventories, secure configurations settings, flaw remediation and patching, and configuration change control are consistently implemented across the enterprise.
- Specifically address the allocation of resources in a risk-based manner for identity, credential, and access management.
- Ensure that all nonprivileged and privileged accounts use strong authentication to access IRS information systems.
- Ensure that privileged accounts are provisioned, managed, and reviewed.
- Ensure that the encryption solutions are compliant with Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules,*[17] on all of its remote access connections.
- Review and remove unnecessary Personally Identifiable Information (PII) collections on a regular basis.
- Fully implement all elements of the Data Loss Prevention (DLP) solution, specifically those related to Data-at-Rest.
- Conduct exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.
- Make updates to its privacy program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.

The *Cybersecurity Framework* function area of DETECT

We found that the function area DETECT and its security program component, Information Security Continuous Monitoring, was rated at *Defined* (Maturity Level 2). 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 to:

[17] Dated May 25, 2001 (Change Notice 2, December 3, 2002).

- Continue to implement components to support Continuous Diagnostic and Mitigation.
- Ensure that adequate resources are allocated to cover Information Security Continuous Monitoring positions.
- Continue to deploy automated capabilities to provide a view of the organizational security posture.
- Continue to implement its data collection/analysis tool and reporting system to support its Information Security Continuous Monitoring dashboard for improved data collection, storage, analysis, retrieval, and reporting of performance measures.

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 PII has become readily available as a result of large-scale cyberattacks on entities including Equifax® and Capital One Bank®. In September 2017, Equifax announced that criminals had exploited a vulnerability in its systems and obtained PII, including names, Social Security Numbers, birth dates, addresses, and in some cases, driver's license information, on approximately 147 million individuals. Equifax agreed to a global settlement with the Federal Trade Commission of up to $700 million to help individuals affected by the data breach. In July 2019, the U.S. Department of Justice announced that a hacker exploited a misconfigured web application firewall and gained access to more than 100 million Capital One Bank customers' accounts and credit card applications. PII exposed included Social Security Numbers and bank account numbers as well as individuals' names, addresses, credit scores, credit limits, balances, and other information. The proliferation of stolen PII 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 *Identity Theft and Impersonation Fraud* as the number three major management challenge facing the IRS. The IRS's ability to continuously monitor and improve its approach to identity theft and data loss prevention is a critical step in defending the agency against evolving cyberthreats and fraud schemes and in protecting billions of taxpayer dollars.

Identity theft prevention

During Fiscal Year 2019, TIGTA and the GAO conducted three audits evaluating IRS identity theft prevention measures. We initiated an audit[18] to determine the effectiveness of the IRS's ongoing efforts to detect and prevent identity theft. We found that the IRS continues to work with its Security Summit partners to refine sharing and coordination processes in an effort to continually improve the detection and prevention of tax-related identity theft. The Security Summit convened in Calendar Year 2015 and includes IRS officials, representatives from State Departments of Revenue, the Chief Executive Officers of leading tax preparation firms, software developers, and payroll and tax financial product processors. A primary initiative of the Security Summit is the creation of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center. The IRS reports that the Information Sharing and Analysis Center is a highly secure web-based portal operated by a trusted third party for States, industry, and the IRS to share and exchange cyberthreat information, and effective security policies and practices. The Information Sharing and Analysis Center facilitates the sharing of information among participating organizations for the purpose of detecting, deterring, and preventing tax-related identity theft. In April 2018, the IRS reported that more than 60 organizations were participating in the Information Sharing and Analysis Center with more than 400 users.

In January 2017, the IRS partnered with a Security Summit industry provider of debit cards to implement and test an initiative called the *Deposit Account Verification Tool*. As part of this initiative, the IRS sends limited information to the debit card partner related to refunds claimed on identified potentially fraudulent tax returns that have a bank routing number belonging to a debit card issued by this partner's organization. The debit card provider then evaluates the information it has for the individual associated with the debit card account to provide the risk level associated with the recipient's account. For example, the debit card provider would indicate whether the recipient's account has been verified and is in good standing at the time of the IRS inquiry or whether additional verification is suggested.

As of April 25, 2018, the debit card provider responded to 158,447 IRS inquiries and indicated that it would accept the deposit for 142,110 (89.7 percent) refunds and reject the deposit for 13,656 (8.6 percent) refunds.[19] Reasons the debit card provider rejects a deposit include that an existing bank account was not located, the taxpayer's last name and last four digits of the Social Security Number did not match, the account is blocked or closed, the account type is not eligible to receive deposits, or the debit card is expired. According to the IRS, participation in the *Deposit Account Verification Tool* initiative was expanded in Processing Year 2018, making the tool available to 12 States and two financial institutions. IRS management indicated that the Security Summit plans to further expand the use of this tool for Processing Year 2019 to

[18] TIGTA, Ref. No. 2019-40-012, *Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft* (Dec. 2018).

[19] At the time of our reporting, the remaining 2,681 (1.7 percent) refunds were still being verified by the debit card provider.

additional Security Summit participants as well as expanding the number of financial institutions that participate.

Moreover, we also found during this review that the IRS's use of a dollar tolerance and programming efforts resulted in some potentially fraudulent returns not being identified. For example, an IRS filter selects potentially fraudulent tax returns for review if the refund meets specific dollar tolerances. However, the 27,566 potentially fraudulent tax returns with refunds totaling almost $1.3 million we identified were below the refund dollar tolerances. It should be noted that between May 23, 2017, and August 7, 2017, six alerts were posted to the Information Sharing and Analysis Center alerting the IRS and other users to an identity theft scheme involving refund amounts below the IRS's refund dollar tolerance amount.

In addition, the IRS modified its identity theft filters to no longer exclude returns with foreign addresses. Our review of tax returns filed during Processing Year 2017 found that its identity theft filters no longer exclude returns with foreign addresses from potential identity theft detection. The IRS reports that 20,299 returns with a foreign address were selected for review as of December 31, 2017. As a result, the IRS protected more than $71.2 million in revenue. However, the exclusionary criteria associated with a filter as well as programming errors associated with another, resulted in 28,092 potentially fraudulent Tax Year 2016 tax returns, as of May 25, 2017, with refunds totaling more than $4.4 million, not being identified.

Further, we found that adding Social Security Administration records to the Death Master File could further reduce the risk of misuse of deceased individuals' identities to file fraudulent tax returns. In September 2016, the Social Security Administration Office of the Inspector General reported that the Social Security Administration excluded approximately 8.7 million individuals for whom it has a date of death from its Death Master File.[20] The Social Security Administration explained that these records were not previously added to the Death Master File because of its concerns regarding the accuracy of the information used to create death claim records prior to the creation of the electronic Numident Database[21] in the early 1970s.

The IRS obtains and uses the Death Master File to identify tax accounts associated with deceased individuals. In fact, the Death Master File is the basis for one of the IRS's key efforts to prevent identity theft tax return filings using the Taxpayer Identification Number of a deceased individual, *e.g.*, locking of the deceased individual's tax account. As of May 15, 2017, the IRS locked approximately 33.9 million tax accounts of deceased individuals. The locking of a tax account results in the rejection of an electronically filed (e-filed) tax return and the prevention of a paper-filed tax return from posting to the IRS's Individual Master File if the Social Security

[20] Social Security Administration Office of the Inspector General, A-06-16-50069, *Numident Death Information Not Included on the Death Master File* (Sept. 2016).

[21] The Social Security Administration Numident Database is a record of applications for a Social Security Card, from which a unique life-long Social Security Number is assigned to an individual. The database includes information on the name, date and place of birth, parent's name and Social Security Numbers, and death date. It is used to create the Death Master File.

Number associated with a locked tax account is used to file a tax return. However, the IRS's efforts to detect and prevent tax-related identity theft using deceased individuals' identities may be substantially incomplete as a result of incomplete Death Master File data.

On April 9, 2018, the Social Security Administration confirmed that it is undertaking an initiative to confirm the date of death information for individuals included on the Numident Database and to update the Death Master File with these records. On May 30, 2018, we received more than 7.7 million Social Security Numbers from the Social Security Administration Office of the Inspector General of individuals for whom the Social Security Administration has a date of death on the Numident Database, but the date of death was omitted from the Death Master File. Our analysis of tax returns filed in Processing Years 2015 through 2018 found that 2,807 of the 7.7 million Social Security Numbers were used 3,783 times on 3,596 tax returns. Of the 3,596 returns, 2,490 (69 percent) claimed refunds totaling more than $8 million.

The GAO initiated an audit[22] of the IRS's financial statements for Fiscal Years 2017 and 2018 to determine whether the financial statements are fairly presented and IRS management maintained effective internal control over financial reporting. As part of this review, the GAO found that the IRS continues to face an ongoing management challenge associated with identity theft. Identity theft tax refund fraud is an evolving and costly problem that causes hardship for legitimate taxpayers who are victims of the crime and demands an increasing amount of the IRS's resources. Taxpayer authentication has become more difficult for the IRS with the wide availability of PII and perpetrators' ability to develop more complex and sophisticated methods to commit fraud undetected. Over the years, the IRS has taken several actions to help combat identity theft tax refund fraud. More recently, because of earlier access to Form W-2, *Wage and Tax Statement*, data, the IRS has been able to conduct systemic verification checks before issuing billions of dollars in potentially fraudulent refunds. Further, to address a sharp increase in the number of fraudulent business and partnership tax returns in recent years, the IRS has been working to develop rules, models, and filters in its Return Review Program to better detect fraud in these returns.

While systemic verification shows promise for preventing fraudulent tax refunds, the IRS has faced challenges that limited success in its implementation, *e.g.*, limitations with its information technology systems and issues with employers filing Forms W-2 after the filing deadline. Although the Return Review Program provides opportunities to combat refund fraud, the IRS has not fully examined opportunities to improve the availability of information on which the Return Review Program's analytic tools rely. Even as the IRS has adapted its identity theft defenses, perpetrators create new schemes in an effort to obtain fraudulent tax refunds despite the IRS's ongoing efforts. Therefore, it is important that the IRS continue its efforts to effectively identify, design, and implement the most effective systems, processes, and internal controls to prevent and

[22] GAO, GAO-19-150, *FINANCIAL AUDIT: IRS's Fiscal Years 2018 and 2017 Financial Statements* (Nov. 2018).

detect identity theft tax refund fraud and thereby minimize the effects on taxpayers and the associated losses to the Federal Government.

The GAO also initiated an audit[23] to review the IRS's efforts to track, monitor, and deter theft of taxpayer information from third parties' cybersecurity practices. The GAO reported that the IRS uses various outreach techniques to encourage third-party providers, *e.g.*, paid preparers and tax software providers, to protect taxpayer information. The IRS tries to educate these tax professionals about ways to improve information security practices and the benefits of doing so. For example, the IRS informs paid preparers, tax software providers, and others about the importance of reporting security incidents in a timely manner to help ensure that action can be taken quickly to help protect their clients and avoid fraudulent returns being filed.

Though the IRS has various ways to disseminate information to tax professionals, it faces a challenge reaching paid preparers who are not affiliated with larger industry groups or who do not visit the www.IRS.gov website, according to both IRS and industry group officials. According to Return Preparer office officials, many paid preparers are not linked to standard tax communication channels, *e.g.*, direct communications from the IRS through news releases or e-mail alerts. The IRS and industry group officials told the GAO that one barrier to reaching these paid preparers is the preparers' belief that their businesses are too small to be a target for fraudsters. IRS officials recognize the challenges and stated that they continue to address them by speaking with tax professionals about how to increase paid preparers' awareness of information security risks, such as by making materials easy for preparers to read.

Data loss prevention

During Fiscal Year 2019, TIGTA and the GAO conducted four audits to evaluate IRS efforts to prevent data loss. We initiated an audit[24] of the DLP solution to determine whether the IRS properly implemented controls to prevent data loss, including data exfiltration of PII. We found that the Data-in-Motion component of the DLP solution has been implemented and is working as intended.[25] The Data-in-Motion component was deployed to a production environment in May 2015. The current screening process includes reviewing unencrypted e-mails and attachments, file transfers, and web traffic for the most common types of PII used by the IRS. Our testing indicated that the component generally identified and blocked common PII types from being sent by e-mail as designed, and that potential incidents identified by the DLP solution were reviewed and resolved as required.

For internal e-mails with PII, the IRS uses the Secure Enterprise Messaging System, which enables the IRS to digitally encrypt e-mail messages and attachments sent between IRS

[23] GAO, GAO-19-340, *TAXPAYER INFORMATION: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices* (May 2019).

[24] TIGTA, Ref. No. 2019-20-049, *The First Phase of the Data Loss Prevention Solution Is Working As Intended, but the Remaining Phases Continue to Experience Delays* (Aug. 2019).

[25] The DLP solution has two other components: Data-at-Rest and Data-in-Use.

employees. Accordingly, IRS policy provides that employees may not e-mail PII outside the IRS unless there is an approved exception from the IT organization.[26] The Data-in-Motion component is a control to ensure that this policy is followed and is currently the only operational component of the DLP solution. If the Data-in-Motion component identifies potential unencrypted PII, it will take action to prevent the PII from leaving the internal network. For example, an e-mail meeting specific criteria found in the DLP system policies will be blocked and the sending employee will receive a warning e-mail explaining why his or her e-mail was not sent. The e-mail will also be manually reviewed to determine if the circumstances were suspicious and if further action is warranted.

To test whether the Data-in-Motion component was working as intended, we created test e-mails containing various types of common PII that are supposed to be identified and blocked based on current DLP policies. We created 30 test e-mails that contained examples of test PII related to 12 common policy rules, with multiple variations of some rules, *e.g.*, PII in the body of the e-mail versus included in an e-mail attachment. We coordinated with an IRS employee, who attempted to send the test e-mails to an external e-mail address, and we documented in real time whether the DLP solution blocked the unencrypted e-mails containing PII based on the related policy rule. Based on this determination and for the specific policy rules tested (including certain Taxpayer Identification Numbers, keywords, and password terms), the DLP solution identified and blocked our test e-mails as expected.

When the DLP solution identifies and blocks data that meet certain exception criteria as designated in the system policies, the identified traffic is referred to the DLP Operations team, who receives the event information in the form of a potential incident. The DLP Operations team analyzes each potential incident to determine if a PII disclosure or attempted disclosure occurred. If a potential incident is confirmed, the DLP Operations team escalates it to one or more parties depending on its categorization, *e.g.*, Business System Process Liaison Event Responders receive event alerts and the Computer Security Incident Response Center receives notice of events that could substantially increase the risk of exposure to IRS systems. If the party receiving the potential incident disagrees with the initial assessment, the potential incident should be sent back to the DLP Operations team for further review.

To test whether potential incidents were reviewed, classified, and referred or otherwise resolved correctly, we reviewed a judgmental sample[27] of incidents on the DLP system. We selected 56 out of 1,561 incidents that were generated during the two-week period from May 1 through May 14, 2018, and reviewed them to determine whether they were triaged and remediated in accordance with IRS policy. Incidents are classified by a severity rating of high, medium, or low as determined by the policy set in use. For example, the severity for the Social Security Number

[26] The IRS is testing a type of secure communication with taxpayers through the Taxpayer Digital Communications program. This provides a way for selected taxpayers and their representatives to exchange secure messages with IRS employees for a variety of reasons, including providing requested documentation for examinations.

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

policy is based on the number of criteria matches identified for that incident. For each of the 14 days, we judgmentally selected two high, one medium, and one low severity incident, *i.e.*, four per day.[28] We determined that all of the sampled incidents were reviewed and resolved correctly.

We also initiated an audit[29] to evaluate the management and security of the Bring Your Own Device (BYOD) program to ensure that data are protected while maintaining program cost efficiencies. The IRS's BYOD program allows registered users to access select IRS applications and data through their personal mobile devices using secure managed mobile applications provided by the program. We found that users with personally owned iPhones® have screenshot capabilities that could allow data leakage to occur. We tested 23 iPhones and determined that all 23 devices had the capability to take a screenshot of the information on the display and save the image on the device. For example, **********2************************************
***************************************2************************************
***************************************2************************************
***************************************2************************************
******************2****************. To our knowledge, this capability has been in effect for more than three years. The IRS has deactivated the screenshot feature on its Government-issued iPhones. However, personally owned iPhones cannot be configured to disallow the screenshot function without completely rendering the function disabled for all of the device applications.

In addition, we initiated an audit of the Privacy program[30] to determine its maturity level. We reviewed the effectiveness of the *Data Breach Response Plan* used to respond to privacy events and found that it is not fully integrated with information security continuous monitoring efforts. The Privacy, Governmental Liaison and Disclosure (PGLD) office monitors and analyzes quantitative performance metrics for the effectiveness of its *Data Breach Response Plan*, *e.g.*, total number of breaches and median cycle time from breach to sending a data loss notification letter. The IRS conducts annual tabletop exercises of the *Data Breach Response Plan* to practice a coordinated response to a breach, to further refine and validate the plan, and to identify potential weaknesses. The PGLD office also tracks performance metrics as part of the annual tabletop exercise, *e.g.*, internal communication processes, third-party response procedures, and the overall effectiveness of the breach response exercise.

[28] For two of the days, there were no Medium severity incidents generated. In their place, we substituted two High severity incidents selected at random that were generated on the same days. Therefore, the severity incidents by category were 30 High, 12 Medium, and 14 Low for a total of 56 severity incidents reviewed.

[29] TIGTA, Ref. No. 2019-20-046, *The Bring Your Own Device Program's Security Controls Need Improvement* (Sept. 2019).

[30] TIGTA, Ref. No. 2019-20-062, *Some Components of the Privacy Program Are Effective; However, Improvements Are Needed* (Sept. 2019).

We reported in Fiscal Year 2018[31] that the Privacy program's *Data Breach Response Plan* was operating at the FISMA Maturity Level 4 (*Managed and Measurable*), which is considered an effective level of security. However, a FISMA Level 5 (*Optimized*) maturity requires a fully integrated continuous monitoring solution between the Cybersecurity function and the PGLD office that incorporates privacy and data breach response to provide ongoing, near real-time monitoring of privacy risks. Because information security continuous monitoring is a security control, the Cybersecurity function is primarily responsible for its development. Cybersecurity function officials stated that privacy and security are two separate but parallel data processes that are not fully coordinated within the IRS.

When a breach is identified, an e-mail is sent to the PGLD office and a breach response team is assembled to assess the severity of the risk; however, continuous monitoring technology is not available to be used by the PGLD office to determine the location and nature of the breach. The PGLD office reported that the number of data loss breaches in Fiscal Years 2017 and 2018 were 3,348 and 3,373, respectively. It currently takes 19 calendar days to notify individuals affected by a breach. The implementation of continuous monitoring of privacy risks would assist the PGLD office's ability to dynamically identify and measure the security implications for privacy and breach response, and more timely notify breach victims.

The Calendar Year 2019 *IRS Information Security Continuous Monitoring Program Plan*[32] states that in the event of the loss or theft of an information technology asset, the Cybersecurity function sends a summary notification to the PGLD office. The plan also states the PGLD office relies upon the Cybersecurity function for lost or stolen information technology assets only; all other incidents are reported online and automatically uploaded into the e-trak system. The e-trak system is used to input and track incidents of disclosures, losses, and thefts and has no systemic monitoring capability. However, until the Information Security Continuous Monitoring program is fully integrated between the Cybersecurity function and the PGLD office, the PGLD office is unable to monitor controls on an ongoing basis or assess its effectiveness against internal or external threats to privacy in its environment.

We also found during this review that while the Privacy and Civil Liberties Impact Assessments (PCLIA) process allows the IRS to categorize, minimize, and apply the appropriate safeguards regarding the use of PII, the IRS does not have an effective inventory of the systems that contain or use PII. According to the NIST,[33] organizations should identify all PII residing in their environment because an organization cannot properly protect PII it does not know about. In addition, NIST Special Publication 800-53 states that organizations should take due care to update the inventories by identifying linkable data that could create PII.

[31] TIGTA, Ref. No. 2018-20-082, *Federal Information Security Modernization Act Report for Fiscal Year 2018* (Sept. 2018).

[32] IRS, *IRS Information Security Continuous Monitoring Program Plan* (June 2019).

[33] NIST, Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (Apr. 2010).

According to PGLD office officials, in Calendar Year 2014, the Department of the Treasury (hereafter referred to as the Treasury Department) requested an inventory of PII from the PGLD office. However, the inventory provided has not been maintained or updated.

An inventory of systems containing PII would allow the PGLD office and the Cybersecurity function to know which systems could affect the public in the event of a breach. An inventory could also support the *Data Breach Response Plan* efforts to help identify which systems and PII are affected by a particular breach. Without a PII inventory, an organization might struggle to implement effective administrative, technical, and physical security policies and procedures to protect PII and to mitigate risks of PII exposure.

In addition, we found that the PCLIAs are not being reassessed timely. We determined the management system contained 441 system PCLIAs at the end of Fiscal Year 2018. Of these PCLIAs, 173 were due to expire by the end of Fiscal Year 2018. Of these 173 PCLIAs due to expire, we determined that:

- 123 (71 percent) were updated timely.
- 37 (21 percent) were not updated timely.
- 13 (8 percent) were retired.

By not ensuring that systems remain current, the IRS cannot ensure that protections for privacy and other civil liberties are being enforced on its systems that collect and disseminate PII.

Further, we found that the PGLD office does not actively review PII collections on a regular basis to remove unnecessary PII. The PGLD office relies on the business units to conduct reviews of the PCLIAs in the Privacy Impact Assessment Management System every three years to ensure that the information is current, to identify and remove unnecessary PII collections, and to meet FISMA requirements. These PCLIAs are collected in the Privacy Impact Assessment Management System, but we determined that the management system itself is not a complete PII inventory of systems that currently contain or use PII that aligns with NIST inventory guidance. Without a PII inventory, an organization might struggle to implement effective administrative, technical, and physical security policies and procedures to protect PII and to mitigate risks of PII exposure.

In its review of the oversight of third-party cybersecurity practices, the GAO reported that the IRS's security requirements for third-party providers do not provide assurance that information is being protected. Specifically, the GAO reported that different types of third parties have varying responsibilities for safeguarding taxpayer information under the IRS's Authorized e-file Provider program. The IRS seeks to help safeguard taxpayers' information and the e-filing system by prescribing requirements for various types of third-party providers through its Authorized e-file Provider program. These requirements are outlined in Revenue Procedure 2007-40[34] and in IRS

[34] Revenue Procedure 2007-40 § 5.03 (June 25, 2007).

Publication 1345[35] and provide that the security of taxpayer accounts and personal information is a top priority. Further, the Revenue Procedure states that it is the responsibility of each IRS authorized e-file provider to have security systems in place to prevent unauthorized access to taxpayer information by third parties. Some of the requirements included in this program are applicable to all types of authorized e-file providers, while others are applicable to one group or another.

According to the IRS, in 2018 there were more than 325,000 authorized e-file providers, some of which were paid preparers. More than 790,000 paid preparers had registered with the IRS as of 2018; accordingly, not all paid preparers are authorized e-file providers and are therefore not covered by the requirements of the Authorized e-file Provider program. However, a business that has been approved as an electronic return originator may employ multiple paid preparers who are not authorized e-file providers. Those paid preparers would be allowed to e-file returns under the supervision of their electronic return originator employer. According to IRS Publication 3112,[36] the activities and responsibilities for return preparation and e-filing are distinct and different from each other.

Further, the GAO reported that the IRS has not fully incorporated the Federal Trade Commission Safeguards Rule[37] into its requirements for all provider types under the Authorized e-file Provider program. The Safeguards Rule applies to financial institutions, including third-party providers that help taxpayers file tax returns, *e.g.*, paid preparers and providers of software that allows individuals to prepare their own tax returns.[38] The Safeguards Rule requires those institutions to develop, implement, and maintain a comprehensive written information security program. The program must contain administrative, technical, and physical safeguards that are appropriate to the provider's size and complexity, the nature and scope of the provider's activities, and the sensitivity of any customer information at issue.[39]

The IRS addresses the Safeguards Rule through Revenue Procedure 2007-40. It provides the procedures for the Authorized e-file Provider program, and states that violations in implementing the rules and regulations of the Federal Trade Commission are considered violations of the Revenue Procedure. It also states that violations may subject an authorized e-file provider to

[35] Publication 1345, *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns* (Feb. 2019).
[36] Publication 3112, *IRS e-file Application and Participation* (Apr. 2017).
[37] The Safeguard Rule was the result of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801(b), 6804, which provides the Federal Trade Commission the authority to require financial institutions, subject to its jurisdiction, to ensure the security and confidentiality of customer records and nonpublic personal information.
[38] Under 16 C.F.R. pt. 314, the Federal Trade Commission regulates the protection of customer information at all financial institutions over which it has jurisdiction. 16 C.F.R § 313.3(k)(2)(viii) identifies accountants or other tax preparation services as financial institutions for this purpose.
[39] On April 4, 2019, the Federal Trade Commission issued a proposed amendment to the Safeguards Rule that, if finalized without modification, would include more detailed requirements for the comprehensive information security program required by the rule. Standards for Safeguarding Customer Information, 84 Fed. Reg. 13,158 (proposed April 4, 2019) (to be codified at 16 C.F.R. pt. 314).

penalties or sanctions, including suspension or removal from the Authorized e-file Provider program. However, IRS publications that provide further information on the Authorized e-file Provider program only briefly discuss the Safeguards Rule and do not provide details on the required elements of an information security program. For example, IRS Publication 3112 states that providers should become familiar with the privacy and security rules and with other important information regarding the safeguarding of personal information available on the Federal Trade Commission website. The publication does not detail each of the required elements of an information security program.

Most paid preparers do not know about the Safeguards Rule and likely do not have information security plans for their places of business, according to officials from several tax preparation industry groups. Industry group officials stated that there are misconceptions about who should be responsible for implementing information security. For example, one industry group official said that paid preparers and electronic return originators often think that their tax software providers will provide security services or that their computer firewall or antivirus software will be enough protection.

In addition, the GAO reported that the IRS lacks explicit authority to require minimum security standards for paid preparers' or authorized e-file providers' systems. The IRS's Authorized e-file Provider program does not outline a set of minimum information security standards for systems used by paid preparers or authorized e-file providers. The GAO reviewed IRS publications for authorized e-file providers and found that specific information security standards were outlined for online providers, but there were no specific standards for other types of authorized e-file providers or paid preparers.

Officials from tax preparation groups and the IRS raised issues that relate to paid preparers' system risks. First, the tax preparation industry groups that were interviewed stated that most paid preparers, especially small firms or individual preparers, did not know the steps that they should take to protect taxpayer information on their systems. IRS officials reported that paid preparers often do not know that they experienced a security incident until the IRS informs them something is wrong with their filing patterns. Second, according to officials from several tax preparation industry groups, paid preparers often have several misconceptions as to what is required of them in protecting taxpayer data, causing confusion. Industry group officials stated that the IRS's current publications are not clear about requirements versus leading practices. For example, IRS Publication 4557[40] provides paid preparers with some leading practices to protect taxpayer data, but the leading practices are not legal requirements, with the exception of the Safeguards Rule.

In addition, the GAO reported that the IRS does not have a robust set of information security requirements for all tax software providers in the Authorized e-file Provider program. Instead, the IRS has limited security requirements for the subset of tax software providers designated as

[40] Publication 4557, *Safeguarding Taxpayer Data: A Guide for Your Business* (Oct. 2015).

online providers. In IRS Publication 4164,[41] the IRS provides some information on "security directive rules of behavior for accessing IRS business systems" while transmitting returns to the IRS; however, it does not provide a specific list of controls for these providers to follow.

Another issue raised by the GAO is that the IRS's monitoring efforts for electronic return originators have limited focus on cybersecurity. The IRS's monitoring program is primarily focused on electronic return originators' adherence with multiple aspects of the Authorized e-file Provider program, *e.g.*, requirements for earned income tax credit due diligence, advertising, and electronic signatures. The Internal Revenue Manual[42] details mechanisms and practices for monitoring authorized e-file providers, including electronic return originators and online providers. However, it provides little direction for the monitoring of information security standards from IRS Publication 1345. The Internal Revenue Manual also lists monitoring techniques for security, but they largely focus on physical security rather than cybersecurity controls for the electronic aspects of information security. For example, it suggests that agents ask about access to physical files or office keys rather than about how providers send e-mails containing taxpayer information.

Similarly, the IRS does not consistently monitor Authorized e-file Providers' cybersecurity controls. The IRS conducts limited monitoring of the online provider subset of tax software providers enrolled in the Authorized e-file Provider program. However, these monitoring efforts are not part of the systematic Authorized e-file Provider monitoring program for electronic return originators, nor are they documented in the Internal Revenue Manual or relevant job aids. According to Electronic Products and Services Support officials, the IRS does not currently monitor all of the standards for online providers, but can remotely monitor three of the six security, privacy, and business standards for online providers through electronic means.[43] However, for two of the three standards that cannot be monitored remotely,[44] Electronic Products and Services Support officials stated that it would be feasible for online providers to send the results of the external vulnerability scans and the certification of information privacy and safeguard policies to the IRS for monitoring purposes.

Further, the GAO found that the IRS may not have a complete picture of third-party provider security incidents because its reporting requirements are not comprehensive. The IRS has primarily tracked information on security incidents in its Return Integrity and Compliance Services Incident Management Database since December 2016, according to Return Integrity and Compliance Services officials. Security incidents can be categorized in a number of ways, *e.g.*, when hackers infiltrate third-party providers' systems. Between 2017 and 2018, there was

[41] Publication 4164, *Modernized e-File Guide for Software Developers and Transmitters* (Oct. 2018).
[42] Internal Revenue Manual 4.21.1, *Monitoring the IRS e-file Program* (Aug. 12, 2011).
[43] The three standards that can be monitored remotely are Extended Validation Secure Sockets Layer Certificate, Website Challenge-Response Test, and Public Domain Name Registration.
[44] The three standards that cannot be monitored remotely are External Vulnerability Scan, Information Privacy and Safeguard Policies, and Reporting of Security Incidents.

an overall decrease in the number of reported high-risk security incidents that led to confirmed identity theft victims across all types of security incidents. However, the number of reported security incidents from third-party providers increased about 50 percent during this same period. In turn, the number of taxpayers affected by the security incidents at third-party providers also increased.

The IRS also does not have comprehensive information about the incidents because, in part, its reporting requirements do not apply to all third-party providers. For example, the Authorized e-file Provider program requires only online providers to report security incidents to the IRS as soon as possible, but no later than the next business day after confirmation of the incident. The information that online providers are to report includes details about the security incident and the affected taxpayers' accounts. If paid preparers or electronic return originators experience a security incident at their place of business, they are not required to report any information about the incident; instead, the IRS encourages paid preparers to share security incident information with the IRS through its stakeholder liaison.[45] According to IRS officials, the IRS cannot track incidents that third-party providers do not report. IRS officials and industry representatives stated that some third-party providers may not report security incidents for fear of punishment from the IRS, *e.g.*, penalties, sanctions, or removal from the Authorized e-file Provider program, or negative impacts to their business reputation.[46]

The IRS has other voluntary reporting mechanisms for tax software providers or other members of the tax preparation industry. For example, members of the Security Summit can use a voluntary reporting mechanism to submit information to the Return Integrity and Compliance Services group. Some members of the Security Summit can use an additional voluntary reporting system in the Information Sharing and Analysis Center online platform, which sends alerts about security incidents to others in the platform.

The IRS also recently revised some of its requirements that could affect paid preparers reporting security incidents while using other IRS services. For example, in October 2018, the IRS updated its user agreement for e-Services, a suite of web-based tools that allow paid preparers, among others, to complete transactions online with the IRS. This update included a requirement to report any unauthorized use of an e-Services account or any other breach of security as soon as the user becomes aware of the incident.[47]

[45] A stakeholder liaison typically takes information about the circumstances of the security incident and information about the affected taxpayer accounts.
[46] Additional information about the Authorized e-file Provider program and sanctions for violation of program requirements can be found in IRS Publications 1345 and 3112.
[47] e-Services users who use an intermediate service provider to obtain information from e-Services must report vulnerabilities, breaches, or compromised e-Services accounts to the IRS within one business day of the discovery. The user agreement states that these users may also report the incident to the stakeholder liaison.

System 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. Although we did not evaluate any physical access controls, the system security access controls reviewed by TIGTA and the GAO in Fiscal Year 2019 included authorization, authentication and identity proofing, and cryptography.

Authorization

Authorization is the process of granting access rights and privileges to a system or a file. Access rights and privileges specify what a user can do after being authenticated to the information system, allowing the authorized user to read or write to files and directories. A key component of authorization is the concept of "least privilege," which means that users should be granted the least amount of privileges necessary to perform their duties. Maintaining access rights and privileges is one of the most important aspects of administering systems security. Effectively designed and implemented authorization controls limit the files and other resources that authenticated users can access and the actions that they can execute based on a valid need that is determined by assigned official duties.

In Fiscal Year 2019, TIGTA and the GAO provided coverage on system authorization in two audits. We initiated an audit[48] to determine whether the firewall environment is administered effectively to protect internal networks from external threats. The Internal Revenue Manual[49] provides that the Computer Security Incident Response Center establishes and manages the minimum firewall administration requirements as well as oversees and approves all rulesets for the IRS network perimeter firewall environments. In conjunction with the Computer Security Incident Response Center, the User and Network Services function's Engineering office designs the network perimeter demilitarized zones, including firewall requirements, and is responsible for firewall implementation and maintenance.

We found that of *11* General Support System (GSS)-1 and *11* Criminal Investigation (CI)-2 firewall system administrator accounts, one GSS-1 account was not properly authorized.[50] We also reviewed login activity reports that showed this system administrator accessed the GSS-1

[48] TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019).

[49] Internal Revenue Manual 10.8.54, *Information Technology Security, Minimum Firewall Administration Requirements* (November 15, 2018).

[50] The IRS has *11* FISMA reportable firewalls. According to the FISMA, GSSs are "reportable" systems. Appendix III to OMB, Circular No. A-130 (Revised), *Security of Federal Automated Information Resources* (July 2016), defines GSS as an interconnected set of information resources under the same direct management control that shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. Each of the *11* firewalls are located within one of the following two IRS GSSs: GSS-1 or CI-2.

firewalls on three occasions without proper authorization. However, we determined the administrator's actions were valid for his or her role and responsibilities. We notified the User and Network Services function's Firewall Support team and they took corrective action to ensure that the system administrator authorization was properly completed. Improper account management increases the risk of an unauthorized user gaining access to sensitive and privileged data within the information systems.

The GAO initiated an audit[51] to evaluate whether information system security controls over the IRS's financial reporting systems were effective in ensuring the confidentiality, integrity, and availability of financial reporting and sensitive taxpayer data, as well as to determine the status of the IRS's corrective actions to address security control deficiencies and associated recommendations contained in previous GAO reports. The GAO reported that it identified two access control deficiencies regarding authorization. The IRS did not:

- Disable a function within one application that allows certain user accounts to download the application's entire database of information or portions thereof, even though the function is not needed for business purposes.
- Prevent individual user accounts from having unnecessary access to certain databases supporting tax processing systems.

Authentication and identity proofing

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 using knowledge-based information, *e.g.*, credit or tax return information, are typically implemented. Similarly, identity proofing is the process of verifying that a person who is attempting to interact with an organization, such as a Federal agency or a business, is the individual he or she claims to be. When remote identity proofing is used, there is no way to confirm an individual's identity through his or her physical presence. Instead, the individual provides information electronically, or performs other electronically verifiable actions that demonstrate his or her identity. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators, *e.g.*, an assertion generated and issued by a credential service provider based on the applicant successfully authenticating to the credential service provider, associated with that subject's digital identity.

[51] GAO, GAO-19-474R, *MANAGEMENT REPORT: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (July 2019).

TIGTA and the GAO conducted three audits covering authentication and identity proofing during our review period. We initiated an audit[52] to evaluate the effectiveness of electronic authentication (hereafter referred to as e-authentication) controls over public access to online systems. We found that the IRS continues to take steps to mitigate risks that relate to e-authentication of its public-facing applications. In May 2017, the IRS began the E-Authentication Risk Assessment Compliance Initiative. The initiative is an ongoing effort to help secure the IRS's public-facing applications. As part of this effort, an E-Authentication Risk Assessment Compliance Initiative team performed an analysis on every IRS public-facing application to determine the security risks and impact of the application if a breach was to occur and the technical and business impact of integrating the application with e-authentication. The IRS completed this process for all 52 public-facing applications (compared to 28 completed during our prior review).[53]

We also found that high-risk applications had secure e-authentication based on existing guidance prior to June 2017. After performing an analysis of the 52 public-facing applications, the IRS secured 14 high-risk, *e.g.*, Get Transcript Online, Taxpayer Protection Program IDVerify, and eight moderate-risk applications at their assessed (or at a higher) e-authentication level of assurance.[54] Conversely, 26 applications, *e.g.*, Filing Information Returns Electronically, Get Transcript by Mail, IRS Direct Pay, were not at the assessed e-authentication level of assurance and thus not in compliance with NIST guidelines.[55] The remaining four applications were either offline or retired. The IRS is accepting the risks associated with applications not at the assessed e-authentication level of assurance. We found that the IRS's rationale for maintaining them at the current authentication method was reasonable based on our review of their risk acceptance documents.

In addition, the IRS completed mitigation plans to address the risks of applications not operating at the assessed level of assurance in order to implement appropriate mitigation controls.[56] **2**
***************************************2************************************
***************************************2************************************
***************************************2************************************
***************************************2************************************

[52] TIGTA, Ref. No. 2019-20-017, *Electronic Authentication Security Controls Have Improved, but Continued Progress Is Needed to Ensure the Protection of Public-Facing Applications* (Apr. 2019).
[53] TIGTA, Ref. No. 2018-20-007, *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented* (Feb. 2018).
[54] TIGTA assigned high- and moderate-risk levels to the applications based on our evaluation of the IRS's implemented e-authentication level of assurances.
[55] NIST, Special Publication 800-63-2, *Electronic Authentication Guideline* (Aug. 2013).
[56] TIGTA did not evaluate whether the IRS implemented the mitigation controls for applications that did not meet the assessed levels of assurance, nor did we test the effectiveness of any mitigation controls.

**************2************.[57] ********2**********************************
************************************2***************.

However, we also found that e-authentication risk assessments were not timely updated and over one-half of them did not meet IRS guidance requirements. Specifically, the IRS did not timely update the e-authentication risk assessments for four public-facing applications: *****2******
************************************2*********************************
************************************2*********************************
*****2*****. The IRS should have conducted a full e-authentication risk assessment on these applications *********2********* to determine the effect of any changes to e-authentication. Prior to the end of our audit fieldwork, the IRS updated the e-authentication risk assessments for these four public-facing applications. In addition, we evaluated the e-authentication risk assessments of all 52 public-facing applications and found that the e-authentication risk assessments generally complied with NIST and OMB guidelines.[58] However, the e-authentication risk assessments did not always meet the IRS e-authentication risk assessment guidance. We found one or more issues on 27 (52 percent) of the 52 e-authentication risk assessments that included:

- Pre-Assessment Worksheets were not consistently completed. For example, the IRS did not always include mitigation options.
- Meeting minutes were not included with the e-authentication risk assessment or the minutes that were included lacked the necessary details for risk-related decisions.
- A business owner's vote was not captured in the e-authentication risk assessment report for the e-authentication level of assurance.

These conditions occurred because the controls in place were not adequate. Without a review process to ensure the full implementation of existing controls and timely updates to the e-authentication risk assessments, the IRS increases the risk that taxpayer records could be compromised and revenue lost due to identity theft.

In addition, we found that the IRS has not fully implemented all NIST requirements[59] on its 52 public-facing applications. The new NIST guidance substantially overhauled the previous guidance, including the elimination of the level of assurance model previously used by Federal agencies, instead requiring agencies to individually select levels corresponding to each function

[57] **2**
***2**
***2**
***2**
***2**
2****************************.

[58] OMB, M-04-04, *E-Authentication Guidance for Federal Agencies* (Dec. 2003).

[59] NIST, Special Publication 800-63-3, *Digital Identity Guidelines* (June 2017).

being performed. For legacy systems, the OMB expected agencies to meet the requirements and comply with NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by the OMB.[60] The one-year compliance date for revisions to NIST publications applies only to new or updated material in the publications. While the IRS is currently developing its compliance plan, it is past the one-year mark of implementing NIST requirements.

Further, the IRS has also taken steps to mitigate risks related to using the Short Messaging Service as part of the authentication process. Evolving threat vectors have rendered the use of the Short Messaging Service as a less secure means to authenticate individuals. Smartphones, which are typically used to receive verifying texts during the authentication process, are prone to theft and undetected redirection of text messages. In December 2017, the IRS launched an authentication module within its IRS2Go mobile application. The IRS2Go mobile application provides an alternative means for users to authenticate rather than using the Short Messaging Service. Next to providing users a security token, use of an authentication application provides the best available means of authentication.

The GAO initiated an audit[61] to review Federal agencies' remote identity proofing practices in light of the recent Equifax breach and the potential for fraud. The GAO reported that the IRS has taken steps to enhance the effectiveness of its remote identity proofing processes. NIST guidance[62] prohibits the use of knowledge-based verification for sensitive applications because of the security risks associated with this technique. While the IRS used knowledge-based verification on its Get Transcript service in the past, now it conducts independent verification of an applicant's possession of a mobile device and uses mobile device confirmation codes. Further, IRS officials responsible for the Get Transcript's authentication and identity proofing services stated that they plan to continue to add alternative verification methods to Get Transcript in the future. They stated that in June 2017, a task force was started to examine the updated NIST requirements and make recommendations on possible changes to its processes to meet the updated guidance. According to the officials, the task force developed a digital identity risk assessment process that it started using to assess external facing online transactions in October 2018. The IRS's recent elimination of knowledge-based verification from its Get Transcript identity proofing process and the additional enhancements that the agency is working on, if successful, will likely further improve the effectiveness of its remote identity proofing processes.

In its audit of the IRS's information system security controls, the GAO reported that it found three access control deficiencies in authentication. The IRS did not:

[60] OMB, Circular No. A-130 (Revised), *Managing Information as a Strategic Resource* (July 2016).

[61] GAO, GAO-19-288, *DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes* (May 2019).

[62] NIST, Special Publication 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing* (June 2017).

- Enforce the requirement for using the appropriate certificates to electronically sign portable document format documents, including certain tax documents.
- Consistently enforce necessary limits for maximum password age for user accounts on certain Oracle® databases in accordance with its policies.
- Use multifactor authentication for accessing certain applications in accordance with OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*, dated February 3, 2011.

Cryptography

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted or stored without unauthorized entities decoding it back into a readable format, thus compromising the data. The information cannot be read without a key to decrypt it.

In its audit of the IRS's information system security controls, the GAO reported that it found three access control deficiencies regarding cryptography, *i.e.*, encryption. The IRS did not:

- Encrypt certain servers in accordance with its policies.
- Encrypt the e-mail service in accordance with its policies.
- Enforce certain encrypted database connections.

System environment security

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.

During Fiscal Year 2019, TIGTA and the GAO conducted three audits of system configuration and change management controls. In our audit of firewalls, we found that the IRS is meeting minimum firewall administration requirements for both the GSS-1 and CI-2. With ***11***, the GSS-********************************11************************************

11************************************
******************11*********************. With ****11****, the CI-2 ******11******
******************11**************************. Minimum firewall administration requirements are guided by three fundamental objectives.

- To ensure that no traffic is admitted into or out of IRS-protected networks unless it is expressly permitted.
- The perimeter firewall environments are installed so that all traffic between IRS-protected networks and the outside must pass through these firewall environments.
- All traffic between systems in a security zone and the intranet shall traverse a firewall, including all systems administration traffic, portal application traffic, and backup system traffic.

However, we found that the GSS-1 annual firewall ruleset reviews are not being performed. We reviewed *11* GSS-1 firewall rulesets and found extraneous rules in the firewalls. Alternately, CI-2 firewall rulesets are being reviewed on an annual basis. We reviewed *11* CI-2 firewall rulesets and did not find extraneous rules in the firewalls.

The Computer Security Incident Response Center and the User and Network Services function's Firewall Support team stated that the required annual reviews were not completed due to lack of adequate staffing and the absence of a network security management tool with the ability to perform automated reviews. In February 2019, the Firewall Support team completed an initial manual review of all *11* GSS-1 rulesets associated with all ***********11************* firewalls. The results from the review showed that *11* (39 percent) of the GSS-1 firewall rulesets were not used within the previous 90 days. The Firewall Support team is testing a new network security management tool that will allow for automated reviews and testing of all firewall rulesets, and they planned for the new tool to be implemented prior to the 2020 Filing Season.

We also found that all 11 of CI-2's firewall change requests were properly approved and correctly implemented. Of the 153 GSS-1 firewall change requests, we determined that five (3 percent) change requests associated with four rulesets were implemented without approvals authorizing deployment in the GSS-1 firewall environment. The firewall change request process uses a form that requires manual data entry, and there is no IRS requirement to assign an expiration date to either the firewall change request or firewall ruleset. By not ensuring that all firewall rulesets have an approved change request and by not implementing expiration dates, there is an increased risk that network traffic flowing through the firewalls is not included in the approved services, protocols, and ports listing. As a result, IRS networks are potentially exposed to unauthorized accesses as well as unnecessary and unmanaged risks that could result in the loss of sensitive taxpayer data.

In addition, we reviewed the password expiration configuration settings for the GSS-1 and CI-2 firewalls. We found no issues with GSS-1 firewall password settings; however, the CI-2 firewall password settings were not configured to enforce password expiration. The Internal Revenue Manual[63] requires a maximum password age or expiration for application and operating systems to be set at 90 days. During our review, CI management officials initiated a corrective action to remove all local firewall administrator accounts and configure all CI-2 firewalls to use an authentication protocol authorizing access to the firewalls. This action ensures compliance with the manual's maximum password age requirements for users and administrators. Failure to properly manage passwords could result in unauthorized access to information systems, which could compromise the confidentiality, integrity, and availability of the system.

In our audit of the BYOD program, we requested the application change log for the six-month period of February through July 2018 for the BYOD application configurations. However, the IRS stated that it does not maintain a change log for administrator configuration changes to the BYOD ***********2************* application. The administrators never created a change log for the BYOD program. Without the application change log, there is no record of the events pertaining to any changes made to configurations, including what was changed in the system. Any misconfiguration that might cause an outage or potential data compromise or data loss cannot be fully diagnosed to ensure that it does not occur again.

In its audit of the IRS's information system security controls, the GAO reported that it found four configuration management control deficiencies. The IRS did not:

- Implement mandatory access controls for an application.
- Update unsupported database software and apply vendor-supplied patches for certain applications.
- Update third-party software on workstations consistently.
- Upgrade certain outdated and unsupported software network devices.

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.

In Fiscal Year 2019, TIGTA conducted two audits involving system scanning and vulnerability patching of IRS systems. In our audit of the BYOD program, we found servers that have critical-risk and high-risk vulnerabilities. The IRS scans the BYOD servers for vulnerabilities on

[63] Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance* (May 9, 2019).

a weekly basis. We analyzed the January through October 2018 vulnerability scans. The scans from January through July 2018 showed little to no high-risk vulnerabilities. However, the August through October 2018 scans had an increase in critical-risk and high-risk vulnerabilities. These vulnerabilities appear on the same servers in two or more consecutive months, which indicates that the IRS is not timely remediating the critical-risk or high-risk vulnerabilities. According to the Internal Revenue Manual,[64] critical-risk and high-risk vulnerabilities are to be patched within 30 calendar days. The software vendor regularly posts vulnerabilities with suggested corrective actions to assist in remediating the vulnerabilities. Figure 7 shows the number of critical-risk and high-risk vulnerabilities for each of the three months.

Figure 7: Critical-Risk and High-Risk Vulnerabilities on the BYOD Servers for August Through October 2018

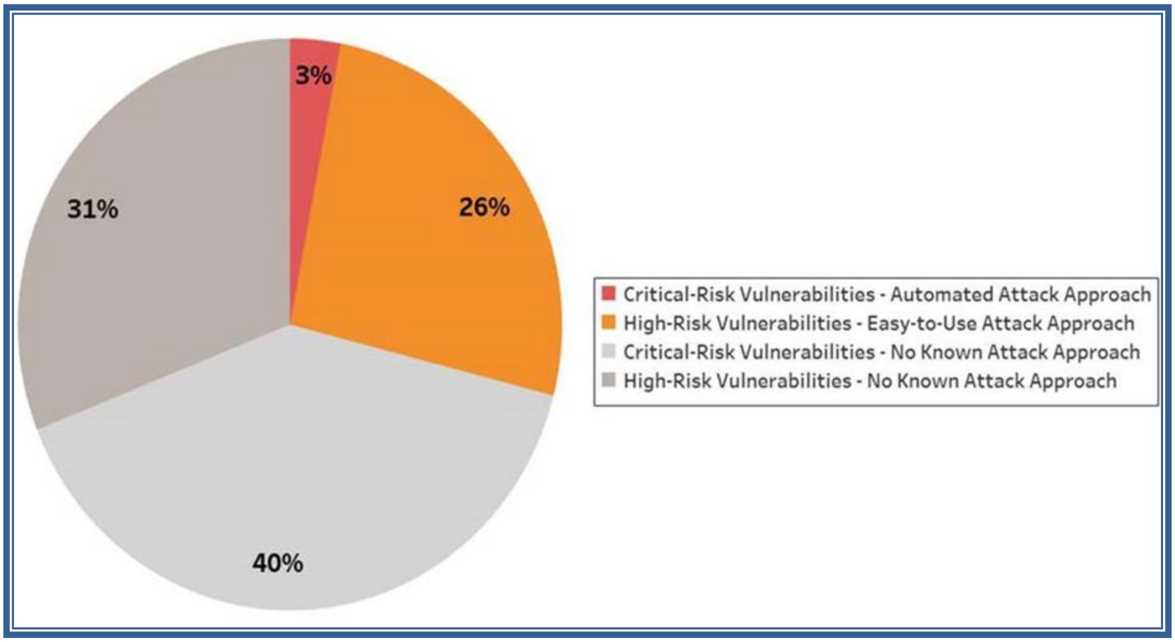
Vulnerability	August 2018	September 2018	October 2018
Critical-Risk	28	27	29
High-Risk	38	29	39
Totals	66	56	68

Source: TIGTA analysis of BYOD servers.

Hackers use different attack approaches to exploit vulnerabilities. Many of the vulnerabilities are public knowledge, making them exploitable to hackers or persons with malicious intent. Public availability of an easy-to-use attack approach increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability and the risk to the system. The risk rating levels from the ****2**** scans used by the IRS take into consideration the likelihood of an exploit based on the availability and skill level of exploit methods and tools. **********************2************************************
************************************2***********************************
*****2*****. Figure 8 shows the percentage of attack approaches for the IRS's critical-risk and high-risk vulnerabilities in October 2018, which had the highest number of vulnerabilities. For instance, 18 (26 percent) high-risk vulnerabilities had the "easy-to-use" attack approach and two critical-risk vulnerabilities (3 percent) had an "automated" attack approach. The remainder did not have a "known" attack approach.

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

Figure 8: Types of Possible Attack Approaches for Exploiting Vulnerabilities on the BYOD Servers in October 2018



Source: TIGTA analysis of BYOD servers for October 2018.

In our audit of firewalls, we reviewed security vulnerability scans for the GSS-1 and the CI-2 firewalls from August 2018 through February 2019 and did not find any issues related to the timely remediation of security vulnerabilities. However, we determined that vulnerability scans were not being performed on *11* (40 percent) of *11*[65] CI-2 firewalls. Failure to perform vulnerability scans can compromise the security posture of the system and can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and data exploitation.

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.

During Fiscal Year 2019, TIGTA's BYOD program audit also evaluated network monitoring and audit logging. We found that application audit logs files are neither retained nor reviewed as

[65] *11* of CI-2's *11* firewalls are in a separate development environment and are not subject to agency security vulnerability scanning requirements.

required. We previously reported[66] that IRS management agreed to ensure that existing IRS policy related to audit trails is followed, including retaining the audit trails for at least 90 days and reviewing the audit trails daily to identify anomalies that could indicate unauthorized access attempts or security breaches. The IRS's planned corrective action was to retain three-year "rolling" audit log files. Based on the completion of this corrective action, we requested the three-year log files for the Good for Enterprise® application. However, the IRS could not provide the log files as the application had stopped logging data in January 2016. The IRS was unaware that the application log files had stopped logging data until we requested this information. We concluded that, if the log files had been reviewed on a regular basis, the IRS would have known that its BYOD servers had stopped logging prior to our request.

We also requested the application audit log files from the ***********2************* BYOD servers for the migration period of September through November 2018. However, the IRS stated that it does not have the server capacity to retain the logs for longer than two weeks. The current process requires that the administrators of the Secure Enterprise Messaging Systems group receive notification when the disk capacity on the BYOD servers reaches their 90 percent threshold. When that occurs, a member of the group deletes the log files. As a result, only approximately two weeks of audit logs are retained from the BYOD servers. Therefore, even though the review of the BYOD audit log files did not show any risk to the BYOD systems, we only analyzed 11 days of data before the logs were deleted. The IRS does not archive these log files because it does not have the server capacity, so there is no way to recover this deleted information.

By not reviewing audit log files, the IRS cannot detect suspicious activities or inappropriate accesses on its BYOD servers. Without maintaining audit log files longer than two weeks, the IRS may have a very difficult time investigating questionable activities or potential incidents after two weeks have passed.

Disaster recovery

Disaster recovery is part of security planning and developed in conjunction with a business continuity plan. Disaster recovery is a set of policies and procedures, which focus on protecting an organization from any significant effects in case of a negative event, which may include cyberattacks, natural disasters, or building or device failures. Disaster recovery helps in designing strategies that can restore hardware, applications, and data quickly for business continuity.

In Fiscal Year 2019, TIGTA and the GAO provided coverage of disaster recovery in two audits. We initiated an audit[67] to review the IRS's migration from Oracle Solaris® to International

[66] TIGTA, Ref. No. 2013-20-108, *Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot* (Sept. 2013).

[67] TIGTA, Ref. No. 2019-20-008, *The Solaris to Linux Migration Project Was Delayed and Needs Improved Governance* (Dec. 2018).

Business Machines' (IBM) zLinux operating system. We found that the project has not fully implemented its planned backup or disaster recovery strategy. The IRS has the zLinux production mainframe located in Martinsburg, West Virginia, and its backup mainframe located in Memphis, Tennessee. The Linux® Migration project's backup mainframe was significantly unused while the project focused on the production mainframe environment. The IRS activated six of 121 central processing units from the date the backup mainframe was purchased in September 2016 to December 2017.

As of February 2018, the recovery process involved activating the backup mainframe and using data replication and tape backups to restore applications. This strategy meets the recovery goal of 36 hours. While the Linux Migration project has a disaster recovery strategy in place, it is working to implement an improved disaster recovery and business continuity strategy that should reduce the expected recovery time. As of March 2018, the zLinux backup mainframe environment in Memphis, Tennessee, was being setup to run the IRS backup and disaster recovery strategy for the production applications in Martinsburg, West Virginia. The migration team plans to improve backup and disaster recovery functionality by utilizing alternate site processing as its disaster recovery strategy.

In its audit of the IRS's information system security controls, the GAO reported one contingency planning deficiency. The GAO found that the IRS had assigned only one individual to administer the e-mail service.

Separation of duties

Separation of duties helps to ensure that no single individual has authorization to control all key aspects of a process or computer-related operation. Effective separation of duties also increases the likelihood that errors and wrongful acts will be detected because the activities of one individual or group will serve as a check on the activities of another. Conversely, inadequate separation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

During Fiscal Year 2019, TIGTA and the GAO conducted two audits in the area of separation of duties. In our audit of the BYOD program, *****************2*********************
**************************************2***********************************
**************************************2***********************************
**************************************2***********************************
**************************************2***********************************
**************************************2***********************************
**************************************2***********************************
**************************************2***********.

In its audit of the IRS's information system security controls, the GAO reported one separation of duties deficiency; the IRS allowed a non-administrator account to be included in an administrator group of accounts for one of its databases.

System security and privacy training

An agency-wide information security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. The FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes security awareness training. The training should inform personnel of the information security risks and of their responsibilities to comply with agency policies and procedures. The IRS further requires all personnel to complete an annual, role-based, information protection and disclosure training.

In Fiscal Year 2019, TIGTA and the GAO conducted two audits in the areas of system security and privacy training. In our audit of the BYOD program, we found that security training should be taken annually. We previously recommended during our prior BYOD program audit that the IRS should provide periodic refresher training to BYOD participants that clearly explains the risks associated with personal mobile devices, how these risks can potentially expose the IRS network to unauthorized accesses and malware, the consequences of such breaches, and how to prevent or reduce the possibility of causing such a security breach. The IRS agreed with our recommendation. Currently, the BYOD program has a Security Risk Awareness and Guidance presentation that BYOD program applicants must take and acknowledge prior to joining the program. The presentation makes the participant aware of the risks and consequences of using a personally owned device to access Government information. It also informs the participants how to prevent or reduce security breaches.

However, we determined that employees were not taking the required annual refresher training because BYOD program management was not enforcing the existing policy and was not following up on employee compliance. During our review, BYOD program management stated that they are negotiating implementation of the required annual training to be included on the Enterprise Learning Management System, where the annual training will be enforceable and monitored. Without annual refresher training, the user may forget the regulations or claim that they were unaware of the security guidance, which can lead to data leakage or expose the IRS network to unauthorized access.

In our audit of the Privacy program, we found that although the IRS provides privacy awareness training to employees, it does not ensure that all employees have taken the training. The mandatory privacy awareness training educates employees on privacy principles. In Fiscal Year 2018, the Human Capital office identified 88,410 instances in which employees were required to take the mandatory privacy awareness training. However, based on a comparison of the Human Capital office list of full-time and full-time seasonal employees and those who completed the mandatory privacy awareness training in Fiscal Year 2018, we found

468 employees delinquent in completing the mandatory training by more than 80 calendar days. We also found 1,313 individuals who completed the training but were not included in the initial list of employees required to take the mandatory privacy awareness training. Protecting taxpayer privacy and safeguarding confidential tax information is a public trust. By not ensuring that all employees complete the mandatory privacy awareness training, the IRS cannot maintain the public's trust for safeguarding taxpayer information.

Further, we also found during this review that PCLIA preparers are not adequately trained. In our Fiscal Year 2015 report,[68] we recommended that the PGLD office provide training to stakeholders involved in the assessment process to ensure that no sensitive information is documented in the assessments. In Calendar Year 2015, the PGLD office developed Course 61760, *Privacy Training for Privacy and Civil Liberties Impact Assessment Preparers*, and Course 61922, *Privacy Training for Adaptive Privacy Impact Assessment Preparers*. Both training courses provide an overview of the Privacy Impact Assessment Management System. However, these courses have not been updated since their implementation, even though the system itself has undergone several enhancements.

In addition, the IRS has not made the Privacy Impact Assessment Management System-specific courses mandatory for PCLIA preparers. We found that of the 117 rejected PCLIAs we reviewed, 102 (87 percent) submitting employees did not take Course 61760 and 110 (94 percent) had not taken Course 61922. We also found one employee who took one of the training courses and still had five rejected Privacy Impact Assessment Management System submissions.

System security documentation

The documentation of system security is an important element of information management for an organization. A system security policy identifies the rules and procedures that all individuals accessing and using an organization's information technology assets and resources must follow. The goal of security policies is to address security threats and implement strategies to mitigate information technology security vulnerabilities. Policies and procedures are also an essential component of any organization. Policies are important because they address pertinent issues, such as what constitutes acceptable behavior by employees. Procedures, on the other hand, clearly define a sequence of steps to be followed in a consistent manner.

During Fiscal Year 2019, TIGTA and the GAO conducted three audits with coverage on system security documentation. We initiated an audit[69] to determine the effectiveness and efficiency of the IRS's implementation of the software tools acquired by the IT organization to address its software development and software asset management needs. We found that the IRS met its

[68] TIGTA, Ref. No. 2015-20-079, *Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program* (Sept. 2015).

[69] TIGTA, Ref. No. 2019-20-005, *Management and Implementation of Information Technology Software Tools Needs Improvement* (Feb. 2019).

deadline for completing the migration of projects from Rational® RequisitePro to Rational DOORS Next Generation, which can be attributed to the IRS developing policies and procedures for the migration of projects and effective communication with employees. However, we also found that even though the IRS is successfully migrating from Rational RequisitePro to Rational DOORS Next Generation, it has not developed and issued policy directives to employees requiring its use and defining any exceptions as recommended in COBIT® 5.

According to Rational Tools Initiative[70] management, it may not be efficient for smaller projects to use Rational DOORS Next Generation. For example, the cost of the software licenses and their associated subscription and support may not be justified when other, less expensive alternatives, such as the Requirement Engineering Program office spreadsheet, would meet the requirement traceability needs. Additionally, there are times when contractors are working on projects and it is not feasible for them to use Rational DOORS Next Generation, *e.g.*, contractors working off-site without access to IRS laptops containing the software. Policy directives addressing these types of issues will ensure that the project owners are aware of when and under what circumstances they must use Rational DOORS Next Generation.

In our audit of the BYOD program, we found that program procedures and guidelines need updating. NIST requirements[71] provide that a mobile device security policy should define which types of the organization's resources may be accessed via mobile devices, which types of mobile devices are permitted to access the organization's resources, the degree of access that various classes of mobile devices may have, and how provisioning should be handled. It should also cover how the organization's centralized mobile device management servers are administered, how policies in those servers are updated, and all other requirements for mobile device management technologies.

During our review, we compared NIST requirements for a BYOD program against IRS BYOD policy. IRS BYOD policy is predominantly in the Internal Revenue Manual.[72] We identified the following areas in which the IRS BYOD policy is silent, particularly in comparison to NIST requirements:

- BYOD user procedures for downloading an antivirus software to the mobile device.
- Procedures for manually wiping, *i.e.*, deleting, a lost or stolen BYOD participant's application data.

[70] The mission of the Initiative is to implement standard processes and automated bidirectional traceability to enable consistent, integrated usage of the IBM Rational Collaborative Lifecycle Management tools solution throughout the IT organization.
[71] NIST, Special Publication 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (June 2013).
[72] Internal Revenue Manual 10.8.26, *Information Technology Security, Government Furnished and Personally Owned Mobile Device Security Policy* (Feb. 28, 2017).

We also identified Internal Revenue Manual policy, procedures, and guidelines that were not clear or needed updating to address the following:

- How and when to report lost or stolen BYOD mobile devices to the Computer Security Incident Response Center.
- How long to retain application audit logs and how often to review these logs because the Internal Revenue Manual[73] section that defined this information is now obsolete.
- Documentation for mobile device baseline configurations[74] (the last updates were from December 2015 and January 2016).

In addition, wiping procedures for lost or stolen devices need clarification. The ******2****** **********2********** system remotely wipes the application data if there is no device activity for 30 calendar days. The system also wipes the application data if the device is jailbroken or rooted. A systemic e-mail is generated to notify the BYOD team of these events. However, we did not identify any procedures requiring a manual wipe of the device application data if the device was reported lost or stolen or any procedures for tracking manual or systemic application wipes.

If mobile devices are lost or stolen and are not wiped of IRS sensitive information, the IRS is at risk of having its data recovered by a malicious party. We identified two employees who reported their personally owned BYODs lost or stolen to TIGTA's Office of Investigations during January 2017 through December 2018. However, the BYOD team could not provide a wipe report for that period. As such, we had no assurance that the BYOD program wiped the devices' application data when the devices were reported lost or stolen. These devices could have contained PII or taxpayer data.

Updating the IRS BYOD security policy ensures that all information technology users within the BYOD program comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority. The IRS should protect its data and control how it is distributed both within and outside the organization.

In its review of oversight of third-party cybersecurity practices, the GAO reported that the IRS has not updated the Authorized e-file Provider program's information security standards for online providers since 2010. Online providers, *e.g.*, tax software providers that allow individuals to prepare their own tax returns, have additional requirements for security and privacy that they must follow, as outlined in IRS Publication 1345. The IRS established six security, privacy, and business standards for online providers, including requirements for developing information privacy and security policies and reporting security incidents. Compliance with these six

[73] Internal Revenue Manual 10.8.3, *Information Technology Security, Audit Logging Security Controls* (Apr. 10, 2017).
[74] Referred to in Internal Revenue Manual 10.8.26, Exhibits 1 and 2.

standards for online providers became mandatory on January 1, 2010; however, the IRS has not substantially updated them since then. These additional requirements do not apply to paid preparers, electronic return originators, or providers of tax software used by paid preparers. Without updating standards regularly, the standards can become outdated and lose their ability to protect information from known vulnerabilities as technology changes.

The GAO also reported that the IRS has not documented the processes for third-party provider security incident or data storage. Security incident information can be reported to the IRS through various channels from the public to IRS offices, and the data are ultimately stored in the Return Integrity and Compliance Services Incident Management Database regardless of the office that initially received the information.

While the Return Integrity and Compliance Services group has documented its information intake, tracking, and storage processes in the *Return Integrity and Compliance Services Incident Management Plan*, the IRS does not have a comprehensive document that describes these processes across the different IRS offices. For example, incident information submitted to the Electronic Products and Services Support group and stakeholder liaison eventually moves to the Return Integrity and Compliance Services function to be tracked in the incident management database. Additionally, Return Integrity and Compliance Services officials stated that they track each of these reported incidents separately and that the main repository should not contain duplicate reports of the same incidents, though multiple databases may contain information about the same incident. Return Integrity and Compliance Services officials added that, before a new incident is added to the incident management database, the staff conducts a query in the database to ensure that the incident was not already added. However, the IRS has not documented how the security incident data processes should flow, relying instead on informal communication efforts of the staff and the assumption that the staff knows where the data belong and will provide that information to the appropriate offices.

While these processes may still be evolving, documenting them can help the IRS combat identity theft by helping to ensure that security incidents are properly recorded and monitored in IRS systems. Documenting the processes may also allow for more complete data, as the data would follow a specific routing and review process. This would reduce the risk of the data not following the various channels they go through now. Such documentation can also help the IRS retain organizational knowledge, mitigate the risk of having that knowledge limited to a few personnel, and ensure that the agency implements these processes effectively in the future.

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. The IRS's ability to provide high-quality taxpayer service and maintain the integrity of the tax system requires modern, secure, and nimble operations as well as a sustained and talented workforce. Many emerging trends offer challenges and opportunities for the IRS, including changes in the taxpaying public and their expectations, technological disruptions, shifts in the workforce, an increasingly globalized and interconnected world, and changes to the tax law.

TIGTA and the GAO performed several audits that assessed the systems development and operations of information technology at the IRS. These audits covered information technology acquisitions, hardware and software asset management, governance and project management, data retention, information technology service and helpdesk requests, and risk management.

Information technology acquisitions

The mission of the Office of the Chief Procurement Officer is to deliver top-quality acquisition services to ensure that the IRS can meet its mission of effective tax administration. Within the Office of the Chief Procurement Officer, the Office of Information Technology Acquisitions is primarily responsible, along with the Office of Business Operations to a lesser extent,[75] for planning, negotiating, executing, and managing the procurement of information technology products and services. The Office of Information Technology Acquisitions is responsible for ensuring that the acquisition process is properly and efficiently managed and is conducted with integrity, fairness, and openness. Information technology products and services remain one of the largest costs for Federal agencies. Without proper controls, the IRS cannot assure that it secured the lowest cost, increasing the risk of overpayments for products and services as well as the potential waste of taxpayer dollars.

For Fiscal Year 2019, TIGTA and the GAO provided coverage of information technology acquisition in three audits. We initiated an audit[76] to assess the various procurement methods the IRS uses to obtain information technology hardware and software to determine whether it followed established policies and procedures and that the procurements were the most cost effective for the Federal Government. To assess the various procurement methods the IRS uses to obtain information technology hardware and software, we selected and reviewed a stratified statistical sample of information technology purchases made between October 1, 2016, and March 31, 2018. We selected 43 awarded contracts and 22 executed delivery orders from a population of 106 awarded contracts and 77 executed delivery orders for information technology hardware and software during that period. The 183 awarded contracts and executed delivery orders had combined obligations of approximately $94.9 million, of which our stratified statistical sample comprised approximately $26.2 million, or about 28 percent of the total population obligations.

[75] The Office of Business Operations is primarily responsible for planning, negotiating, executing, and managing the procurement of non-information technology products and services.

[76] TIGTA, Ref. No. 2019-20-038, *Controls Over Information Technology Procurements Need Improvement* (June 2019).

We examined the documentation of hardware and software products purchased through all the awarded contracts and some of the executed delivery orders[77] and found that information technology hardware purchases were not always the most cost effective for the Federal Government. For 56 of the awarded contracts and executed delivery orders in our stratified statistical sample, we were unable to find the same or similar product at a better price than what the IRS had obtained. A number of those products required specific features or specifications, making them a unique product not largely available in the common marketplace and not identified in our search. However, we identified nine executed delivery orders for which the IRS could have procured its information technology hardware at a lower cost. We estimate that the IRS could have saved $122,803 had it used a General Services Administration Federal Supply Schedule to purchase the hardware.[78]

In addition, we reviewed the electronic contract files for our stratified statistical sample of 43 awarded contracts and 22 executed delivery orders for information technology hardware and software products purchased by the IRS to determine whether the preaward and award documents were stored as required. We found that the documentation was not readily available or was missing from some of the electronic contract files. Projecting our stratified statistical sample results to the population, we estimate that 91 preaward and award documents are missing.[79] Although we did not identify a large number of instances in which the IRS overpaid for a particular information technology hardware or software product, we believe that improvements can be made to the procurement process as well as to ensure that preaward and award documentation is made more readily available to decrease the risk of overpayment for products and services and the potential waste or misuse of taxpayer dollars.

In our audit of the IRS's implementation of software tools, we found that the IRS did not follow the Federal Acquisition Regulations[80] and IRS guidance[81] when purchasing the IBM BigFix® product. For example, the IRS did not follow established planning procedures, such as preparing a requisition checklist, prior to the purchase of the BigFix product as required by the Internal Revenue Manual and recommended by the Federal Acquisition Regulations and COBIT 5

[77] Due to the large variety and volume of products purchased through the executed delivery orders, we examined all software purchases but limited our review to hardware purchases with a minimum cost of $300 or more per unit. In addition, we were unable to review two awarded contracts with total obligations of approximately $67,000 because the IRS could not provide any of the preaward documentation, and the contracting officers who worked on the contracts had left the IRS. As a result, we were able to review only 41 of the 43 awarded contracts selected as part of our stratified statistical sample.

[78] 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 $59,582 and $186,024.

[79] 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 46 and 135 preaward and award documents missing.

[80] 48 C.F.R. (2017).

[81] Internal Revenue Manual 2.21.1, *Requisition Processing for IT Acquisition Products and Services, Introduction to Requisition Processing for Information Technology* (Apr. 11, 2017).

industry best practices. As a result, the IRS improperly identified the BigFix product as a viable solution to meet its need for a software asset management tool.

While in 2012 the IRS did a limited comparison of BigFix and a product from Hewlett-Packard®, the IRS did not conduct significant analysis of BigFix nor was any testing performed prior to implementation of any BigFix component. Testing the BigFix product prior to purchasing and implementing the software, as required by IRS guidance, would have allowed the IRS to determine if it would meet its software asset management needs. As a result, the IRS is still searching for a tool capable of performing software asset management nearly three years after the IRS's initial planned implementation date of May 31, 2015.

We also found that the IRS had no formal acquisition process for using software credits to purchase the BigFix product, and the process used lacked internal controls. In Fiscal Year 2015, management from the Strategic Supplier Management office developed two guidance documents for using IBM credits. One document is for software credits and only applies to software tools. The other document is for service credits and applies to service contracts for software or hardware. These documents require the same information, but only the service credit document requires any preapproval by a manager. The IRS was unable to provide final approved and signed versions of these documents. Management from the Strategic Supplier Management office stated that these documents simply serve as standard operating procedure guidelines for the contract submitters to either use or reference when submitting their contract requests to the Strategic Supplier Management office for review. However, these documents are not included in any authorized formal IRS policies and procedures. This lack of control can cause the IRS to purchase software tools that are not sufficient to meet its needs.

In addition, the GAO initiated an audit[82] to determine whether the CIO's information technology budgeting practices are consistent with the FITARA and the OMB's related implementing guidance.[83] In December 2014, Congress enacted the FITARA, which was intended to improve covered agencies' acquisitions of information technology and to assist Congress in holding covered agencies accountable for their progress towards reducing duplication and achieving cost savings. The FITARA also enhanced the CIO's authority in covered agencies for the formulation and approval of their agency's information technology budgets. In this regard, the FITARA requires the CIOs to have a significant role in the decision processes for all annual and multiyear planning, and to approve the information technology budget requests of the agency.

The GAO selected four departments to review including the Treasury Department. These departments had the two highest and the two lowest average initial self-assessments scores of compliance with OMB's FITARA guidance, as well as a Fiscal Year 2017 information technology budget of at least $1 billion. Within each of the departments, the GAO also selected

[82] GAO, GAO-19-49, *INFORMATION TECHNOLOGY: Departments Need to Improve Chief Information Officers' Review and Approval of IT Budgets* (Nov. 2018).
[83] OMB, M-15-14, *Management and Oversight of Federal Information Technology* (June 10, 2015).

the component agencies, including the IRS for the Treasury Department, with the largest Fiscal Year 2017 information technology budget. For each selected department and component agency, the GAO reviewed relevant information technology budget policies and procedures, analyzed a sample of major and non-major investment proposals against key OMB requirements, and determined whether selected departments captured Government labor costs, among other things.

The OMB's guidance on implementing the FITARA requires departments to develop policies and procedures to address a number of requirements identified in the basic set of roles and responsibilities, *e.g.*, the common baseline, for the CIOs. These include eight selected common baseline requirements related to the CIO's responsibility for information technology budgeting. The GAO reported that four of the eight selected OMB common baseline requirements are not applicable for the IRS,[84] and that the IRS satisfied the remaining four to:

- Include the CIO in the planning and budgeting stages for programs that are fully or partially supported with information technology resources.
- Include the CIO as a member of governance boards that make informed decisions regarding all information technology resources, including component-level boards.
- Ensure that the CIO has reviewed and approved the major information technology investments portion of the budget request.
- Ensure that the CIO has reviewed whether the information technology portfolio includes appropriate estimates of all information technology resources included in the budget request.

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 2019, TIGTA conducted four audits covering hardware and/or software management controls. We initiated an audit[85] to evaluate the strategy and processes to manage and control commercial-off-the-shelf software versions running on the IRS infrastructure and

[84] The four OMB common baseline requirements not applicable to the IRS include to: 1) establish the level of detail with which information technology resources are to be described in order to inform the CIO during the planning and budgeting processes, 2) establish agency-wide policy for the level of detail with which planned expenditures for all transactions that include information technology resources are to be reported to the CIO,
3) document the processes by which program leadership works with the CIO to plan an overall portfolio of information technology resources, and 4) ensure that the CIO has reviewed information technology resources that are to support major program objectives and significant increases and decreases in information technology resources.

[85] TIGTA, Ref. No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019).

ensure that software versions are up to date. We found that the IRS has made progress in automating its review of software versions through the use of tools. For example, by using the Flexera® Technopedia® catalog and BigFix 9.2, the IRS can determine the vendor's most recent released version. However, the IRS is not effectively managing or controlling software versions on systems and applications to ensure that software is approved and up to date. We identified instances in which software versions running on IRS systems were not listed in its official software product catalog or were shown as outdated and unapproved.

For example, we reviewed 110 software versions installed on 12 Tier I environments as of February 2017 and discovered that 55 (50 percent) of them were not listed in the software product catalog. This situation could be potentially dangerous to the IRS environment because these software versions were running on systems and may not have been reviewed, approved, and authorized prior to installation. Of the 110 versions reviewed, we also identified 13 software versions installed on the mainframe environment that were showing a sunset date of 2017 or earlier in the enterprise standards profile product catalog. In addition, the IRS had 28 software versions installed and running that were listed as archived/retired on the enterprise standards profile site. Users are permitted to use archived products if vendor maintenance or community support is provided and permission is obtained from the authorizing official and documented with a risk-based decision document. Currently, no mechanism is in place to reconcile the software versions installed on Tier I environments to the enterprise standards profile.

We also found that software versions not listed in the approved enterprise standards profile product catalog are running on servers. The IRS provided an ad hoc list of the software installed on approximately 3,000 servers. We reviewed the software installed on the servers to determine whether the software versions were in the enterprise standards profile product catalog as approved software. Our analysis determined that there were 156 unique software versions in the Tier II environment, of which 32 (21 percent) were not approved in the enterprise standards profile product catalog, and 50 (32 percent) were shown as archived/retired.

In addition, we found that the IRS had unauthorized software installed on workstations. We reviewed a list of 6,970 Tier III software applications installed on IRS workstations. The list identified 6,533,792 software version instances installed in each operating division of the IRS. Due to the substantial volume of Tier III software versions recorded by the IRS, we limited our analysis to 5,697,421 software version instances installed on 10,000 or more workstations. This represented 87 percent of the entire population of software version installs. From this subset, we identified 146 unique major software versions for review. Of these 146 software versions, we found seven (5 percent) that are not listed on the enterprise standards profile product catalog.

Moreover, we found that the IRS does not efficiently remove old versions of software from the Tier III environment when a newer version of software is installed. For example, the IRS currently shows ******************2******************** installed and in use, ranging from *************************2*****************************, even though these older versions have been identified to include high vulnerabilities and a Max Common Vulnerability Scoring of 10.

The IRS has a decentralized software version control process with insufficient oversight of potentially unapproved, outdated, or archived/retired software running on IRS systems that could result in unacceptable risks to overall operations and taxpayer data. Effective centralized accountability in monitoring software versions running across the entire IRS network can allow for more effective decisions on cost, risk, and compatibility. Running outdated or unapproved software versions significantly increases the risk of poor system performance and the exploitation of known software vulnerabilities by cybercriminals.

In our audit of the implementation of software tools, we found that the IRS did not effectively manage the IBM Legacy Rational tools software licenses and did not actively monitor the costs associated with purchasing the software licenses and subscription and support. As a result, the IRS purchased software licenses that it never deployed and purchased software subscription and support for licenses it did not use. We estimate that the IRS wasted approximately $3.4 million between Fiscal Years 2015 and 2017 on unused software licenses and support. The IRS may also have violated the bona fide needs rule by not using licenses purchased in Fiscal Years 2015 and 2016. In addition, we estimate that the IRS over used software licenses and support worth between $851,708 and $2.8 million between Fiscal Years 2015 and 2017.

In our audit of firewalls, we found that firewall inventories and reporting tools are inaccurate and incomplete. The IRS uses multiple inventory and reporting tools to assist in providing administrative oversight of all FISMA reportable firewalls. We reviewed multiple ********2******** firewall inventory reports and the Treasury Department Cybersecurity Analysis and Reporting Dashboard monthly inputs. Figure 9 provides a summary of the total FISMA reportable firewalls using the various inventory and reporting tools, and compares it to the correct number of firewalls in the inventory.

************************11**************************
*********************11***********************

**********11********	****11**** ****11**** ****11****	****11**** ****11**** ****11****	****11**** ****11**** ****11****	****11**** ****11**** ****11****	****11**** ****11**** ****11**** ****11*****
**********11******** **********11********	*11*	*11*	*11*	*11*	*11*
**********11******** **********11********	*11*	*11*	*11*	*11*	*11*
**********11******** **********11******** **********11******** **********11********	*11*	*11*	*11*	*11*	*11*

11
****11****.

We determined that each of the firewall inventory and reporting tools were not only inaccurate and incomplete, but also reported conflicting numbers of FISMA reportable firewalls.

During our review, we evaluated the ***********11************ inventory specific to the GSS-1 and CI-2 firewalls. ***********11************ is a component of the Knowledge Incident/Problem Service Asset Management system, which is the IRS's official financial asset inventory system. We determined that the November 2018, February 2019, and April 2019 inventories were both inaccurate and incomplete and did not contain the level of granularity required for timely and up-to-date tracking and reporting of IRS firewalls. However, throughout the course of the audit, the User and Network Services function's Asset Management program completed multiple updates to the GSS-1 and CI-2 firewall inventories. As a result, the May 2019 ***********11************ GSS-1 and CI-2 firewall inventories provided an accurate and current snapshot. Without accurate firewall inventories, the IRS cannot ensure that it is properly monitoring and maintaining perimeter supporting components in a secure manner.

We also found that the Treasury Department's Cybersecurity Analysis and Reporting Dashboard reports were inaccurate and incomplete. From July 2017 through February 2019, the IRS's monthly submission for the Dashboard reported the same incorrect number of firewalls *11* connected to unclassified networks. As previously illustrated, the IRS employs *11* FISMA reportable firewalls that are connected to unclassified networks. Without accurate firewall inventory and reporting, the IRS does not know what it has deployed and therefore what it should be protecting, as well as external stakeholders will not have accurate information for making decisions.

In addition, we found that none of the ******11******* firewalls were correctly categorized in the appropriate information technology asset group. The initial GSS-1 security vulnerability reports did not contain results for any of the GSS-1 firewalls because their Internet Protocol addresses were not correctly categorized as belonging to the GSS-1's information technology asset group. Without ensuring accurate information technology asset group lists, there is a risk that unknown or undetected security vulnerabilities could compromise the network security perimeter and potentially lead to unauthorized access, unauthorized data sharing, and unauthorized data exploitation.

In our audit of the DLP solution, we found that further project delays to the Data-at-Rest and Data-in-Use components of the DLP solution could result in inefficient use of resources. As part of the Safeguarding Personally Identifiable Information Data Extracts project's responsibility for implementing the DLP solution, the IRS originally contracted for the software in early Calendar Year 2011. At that time, the IRS purchased 110,000 licenses when its workforce was about 104,000 employees (extra licenses were needed for contractors), and another 30,000 licenses for the Treasury Department to use, for a total of 140,000 licenses. However, the IRS workforce subsequently decreased, and by Calendar Year 2015, the total number of employees was substantially smaller, about 90,000. Recognizing this reduction, in Calendar Year 2015, the Treasury Department took over the administration of the DLP license renewal contract, including the Data-in-Motion, Data-at-Rest, and Data-in-Use components and transitioned to a department-wide contract for the same 140,000 licenses, all of which were then made available for use to all Treasury Department agencies.

The IRS remained the largest user of the licenses. Because of the Treasury Department's actions, the IRS stopped contracting directly for the DLP license renewals and began acquiring them using an interagency agreement with the Treasury Department under its Franchise Fund Shared Services program. The Treasury Department uses the Franchise Fund to assign and allocate shared costs to the requesting agency. The Treasury Department then bills the agency monthly for its share of the services. In Fiscal Year 2019, the Treasury Department Franchise Fund estimated the overall DLP cost was $692,700, and the IRS share was set at about 80 percent of that amount.

We obtained and analyzed the contract documents pertinent to the DLP solution software license costs, which provided separate license information for the three individual components. We limited our analysis to the costs incurred for the three components from Fiscal Years 2016 through 2019. We used the IRS's Fiscal Year 2019 Treasury Department Franchise Fund share to determine the cost allocated to the IRS for each component for prior fiscal years.

The significant delays with the deployment of the Data-at-Rest and Data-in-Use components of the DLP solution resulted in the inability to use the capabilities associated with these two components. However, the IRS continued to pay for DLP license renewal costs for these two components per the terms of the interagency agreement. During this period, a cost of about $1.5 million was incurred by the Treasury Department for license renewals associated with the

Data-at-Rest and Data-in-Use components. The IRS was responsible for about 80 percent of this cost based on the terms of the interagency agreement with the Treasury Department. Therefore, the IRS was responsible for paying approximately $1.2 million for software that was not deployed into production, *i.e.*, not in use, over a four-year period. We did not include the costs incurred under these contracts for remote assistance/technical support for the DLP solution that was allocated to the IRS. The IRS estimates that the Data-at-Rest and the Data-in-Use components will be implemented by June 15, 2021.

Governance and project management

Governance

Governance is a process of putting structure around how an information technology strategy aligns with an organization's business strategy. It also ensures that the information technology strategy stays on track to achieve its goals and implements ways to measure the organization's performance. The primary objective of the IRS governance is to ensure that assigned investment, program, and project objectives are met, risks are managed appropriately, and enterprise expenditures are fiscally sound. IRS governance boards provide direction on the information technology scope and schedule based on established funding and targeted business results.

During Fiscal Year 2019, TIGTA provided coverage of information technology governance in two audits. We initiated an audit[86] to determine whether the IRS is adequately managing its temporary and permanent e-mail records in compliance with OMB's *Managing Government Records Directive*.[87] We found that the IRS's temporary and permanent e-mail records management efforts generally complied with the Directive. Specifically, the IT organization and the PGLD office established a governance structure over the Enterprise Exchange Upgrade (EEU) project. The EEU project was initiated to comply with the Directive's requirements. The Infrastructure Executive Steering Committee was selected to govern the EEU project; members of the IT organization and the PGLD office's eRecords Committee met biweekly to act as the Infrastructure Executive Steering Committee's proxy for eRecords decisions. The Enterprise Operations Governance Board provided oversight over each phase of the EEU project. The Enterprise Operations function's Technology Implementation Services office managed EEU project development. Whereas, the Enterprise Operations Infrastructure Services office oversaw EEU project operations and maintenance.

In our audit of the Linux migration project, we found that inadequate governance of the Oracle Solaris to IBM's Linux migration project contributed to poor planning, insufficient technical skills, significant delays, and funds prematurely spent on hardware and service support. During the migration, the Linux migration project operated without governance that was specific to its

[86] TIGTA, Ref. No. 2019-20-060, *E-Mail Records Management Is Generally in Compliance With the Managing Government Records Directive* (Sept. 2019).
[87] OMB, M-12-18, *Managing Government Records Directive* (August 24, 2012).

operations. Without sanctioned governance, the Linux migration project did not start with proper controls or authorization of its process and procedures. Inadequate governance led to several factors that contributed to project delays. For example, the business case relied upon to support the decision to go forward did not include key factors, such as the time required to train employees on how to set up and support a Linux environment. Specifically, the Enterprise Services function needed trained personnel with specific technical skills to perform proper capacity planning, performance analysis, and performance testing. In addition, the Applications Development function did not have the staff with the required technical skills needed to determine the scope of the project. Because the project's staff did not have the technical skills required to carry out the migration, the project purchased $814,272 worth of support services provided by the vendor. Project status briefings show that support services included technical labor for setting up the IBM mainframes with customized program coding. Due to insufficient planning, the Enterprise Operations function personnel did not schedule zLinux mainframe training until two years after the start of the Linux migration project. However, the IRS could not provide evidence that the training was completed.

The Linux migration project started with goals to migrate 33 percent of its 140 target applications to Linux by December 2015, and 66 percent, including the Modernized e-file system, by December 2016. However, the IRS did not develop an initial project plan, conduct upfront assessments, or perform a complete technical analysis on the applications and databases that were to be migrated. The migration team did not effectively assess the portability of applications and databases from Solaris to Linux. The migration team's insufficient planning and analysis led to an inadequate understanding of all requirements needed for an enterprise-wide Linux migration effort. As of February 2018, only eight of the 140 applications have been migrated to Linux.

While the migration team established the Linux environment, it initially did not follow standard software development practices. Prior to the Linux migration project's kickoff, the migration team began evaluating applications to migrate to Linux. The approximately four-month long evaluation identified the Totally Automated Personnel System/Single Entry Time Reporting application as a pilot project for its Linux migration efforts, which started in March 2014. The team had to restart the pilot project's migration process using standard software development practices in order to develop repeatable standards, processes, and procedures for future migrations. As a result, the entire pilot process of migrating the Totally Automated Personnel System/Single Entry Time Reporting application to the Linux environment took 22 months and was completed in September 2015.

Inadequate governance also allowed for an improper approval and prioritization process across the project. For example, internal risk-tracking documents reported the Linux migration project did not have proper control authorization to build Linux servers. Without these controls, projects from various departments would be able to submit unified work requests without approved engineering designs.

The Linux migration project spent nearly $15 million in Fiscal Year 2016 and $11.4 million in Fiscal Year 2017 for the acquisition of software, hardware, and contractor services, according to a briefing status report and investment documentation.[88] The project requested an additional $14.9 million for both Fiscal Years 2018 and 2019 for contracting support and the migration of applications. If approved, the funding requests bring the Linux migration project's total costs, excluding the IBM hardware purchase, to $56.2 million through Fiscal Year 2019.

According to the IRS, in Fiscal Year 2017, the hardware and software maintenance costs to continue running all IRS legacy systems on the Solaris platform that can be migrated to Linux was nearly $2.4 million annually, or more than $7 million through Fiscal Year 2019. This amount does not include other potential costs savings, such as software licensing, that might affect how quickly the IRS recovers the Linux migration expenses. The IRS estimates that the migration project will be completed in Fiscal Year 2020. The IRS will be unable to recover the full costs of migrating to Linux and begin realizing savings until several years after the project is completed.

In addition, we found that the Enterprise Demand Management process has improved the migration efforts. For the Solaris to Linux Migration project, the IRS designed and developed the Enterprise Demand Management process in Calendar Years 2015 and 2016. Once the IRS successfully deployed the Totally Automated Personnel System/Single Entry Time Reporting pilot to show that a migration to Linux was possible, the Enterprise Demand Management team began developing the goals, objectives, and requirements for any IRS system to be migrated to Linux. In January 2017, the Enterprise Demand Management process started requiring all projects to use the Linux Cross Functional Playbook and complete the required steps in order to migrate and deploy a system to Linux.

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.

In Fiscal Year 2019, TIGTA conducted four audits in the area of information technology project management. We initiated an audit[89] to review the systems development process to implement 2019 Filing Season changes. We found that the IRS completed extensive programming and systems changes in a compressed time frame and started the 2019 Filing Season on January 28, 2019, which is within the normal time frame. The Tax Cuts and Jobs Act of 2017

[88] These amounts exclude the purchase in September 2016 of two IBM mainframes running zLinux along with service and support for $6.8 million.

[89] TIGTA, Ref. No. 2019-24-035, *The Internal Revenue Service Completed Extensive Programming and Systems Changes in a Compressed Timeframe for the 2019 Filing Season* (June 2019).

(hereafter referred to as the Act) is the first major tax reform legislation in more than 30 years and made significant changes to the tax code affecting individuals, businesses, and tax-exempt organizations. The Act contains 119 tax provisions that affect both domestic and international taxes. Modifications were needed for tax return processing, for compliance activities, to accommodate the newly revised tax forms, and to ensure that IRS personnel were able to respond to an estimated four million additional telephone calls and taxpayer correspondence. This audit was a continuation of an initial review[90] we conducted of the IT organization's efforts to implement the Act.

One of the continuing challenges the IRS faces each year in processing tax returns is the implementation of new tax law changes. Before the filing season begins, the IRS must identify the tax law and administrative changes that affect the upcoming filing season. Once these changes are identified, the IRS must revise the various tax forms, instructions, and publications. The IRS provided documentation stating that for the 2019 Filing Season, the IRS reprogrammed 124 computer systems to ensure that tax returns were accurately processed.

In March 2018, the IT organization initiated an iterative requirements development process called the Rapid Requirements Elicitation. This process accelerates the gathering of programming requirements to allow the IT organization the maximum amount of time to implement the identified changes, identify gaps and risks earlier, and promote collaboration to ensure common understanding of the business need and feasibility. The Rapid Requirement Elicitation sessions use integrated project teams that consist of key members across business units and the IT organization.

During the Rapid Requirements Elicitation process, business unit officials discussed an Act-related requirement that they wanted the IT organization to implement for the 2019 Filing Season. However, due to the compressed delivery cycle, the IT organization asked business unit officials to defer submitting the requirement to create new tax forms in an automated format that would enable them to collect data efficiently for compliance purposes. The IT organization determined that it could not deliver the automated forms in time for the 2019 Filing Season. As a result, the business units planned to develop manual procedures to collect the data they need, which may cause compliance reviews to be less efficient. The business unit officials will request that all affected forms be converted to fully functioning automated forms for the 2020 Filing Season.

In addition, the Enterprise Systems Testing group within the IT organization implemented several mitigations to reduce the impact of a compressed delivery cycle for the 2019 Filing Season. Applications Development management reprioritized work so employees could be reallocated to the Act implementation. Applications Development function management also stated that overtime credit hours were granted so employees could help with the shortened

[90] 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).

delivery cycle. Although we requested a complete list of all mitigations along with supporting documentation, Applications Development function management did not provide any documentation.

IT organization management stated that at the start of the filing season, January 28, 2019, functional testing was complete and Final Integration Testing was 80 percent complete. As of January 30, 2019, IT organization management reported 77 open defects. Most of the open defects were style sheet/display errors. Style sheets format tax return data to display properly for the IRS tax examiners who need to access/view tax returns online. All critical defects were resolved prior to the start of the 2019 Filing Season.

Further, we found that existing IT organization personnel and contracted support implemented the Act with limited impact on ongoing programs. IRS management identified seven ongoing programs that might be delayed or slowed down due to the reallocation of employees and other resources to the Act implementation. These seven programs include: Taxpayer Digital Communications Outbound Notifications, Online Payment Agreement Behind Web Apps, Wage and Investment Submission Processing Campus Consolidation, Customer Account Data Engine 2 Integrated Tax Processing Engine, Cloud Implementation, DevOps, and zLinux migration. We analyzed the work hours of IT organization employees who charged time to one or more of these programs and to the Act. Our analysis determined that the reallocation of labor resources might contribute to a slowdown in Enterprise Services function work on zLinux migration and Applications Development function work on DevOps and the Customer Account Data Engine 2 Integrated Tax Processing Engine programs.

In our audit of the DLP solution, we found that continued delays with implementing the Data-at-Rest and Data-in-Use components are preventing realization of the full benefits of the DLP solution. The Safeguarding Personally Identifiable Information Data Extracts project, which is responsible for implementing the DLP solution, started in Calendar Year 2010 and is ongoing. While the project team implemented and expanded the Data-in-Motion component of the solution, project management issues were a contributing factor that affected the Safeguarding Personally Identifiable Information Data Extracts project's ability to deploy the Data-at-Rest and Data-in-Use components. For example:

- Efforts focused primarily on the Data-in-Motion component implementation. According to the IRS, this was the primary cause of the overall project delay. The significant work required to deploy the Data-in-Motion component and the post-implementation technical efforts encountered were key contributing factors delaying the timely deployment of the Data-at-Rest and Data-in-Use components. After the Data-in-Motion component was placed into production, the amount of work required to maintain and expand its capabilities was more than anticipated. When the amount of work to develop other capabilities such as sensitive image recognition[91] was also considered, the IRS chose to

[91] An add-on capability to the DLP software that enables detection of sensitive text embedded in images.

re-evaluate the overall focus of the project, which resulted in further delays to the Data-at-Rest and Data-in-Use components.

- Project management documentation was not always prepared or updated as required after deployment of the Data-in-Motion component, indicating inconsistent project management related to the Data-at-Rest and Data-in-Use components. The project began in Calendar Year 2010, and we identified some required documentation that was approved in Calendar Year 2011, *e.g.*, the Project Charter and the Project Management Plan. However, after the Data-in-Motion was placed into production in May 2015, some required documents were still in draft form or had not been updated as required. For example, the Project Management Plan was originally approved in August 2011; however, even though it is a key project planning document, the Plan had not been updated as required since the original approval. While the project team continued to develop the Data-in-Motion component over time, the documentation issues observed after it was deployed showed that working on the Data-at-Rest and Data-in-Use components was a not a priority until Calendar Year 2018, when the project focus was re-evaluated.

Because of the delays, two key components involving data in repositories and data in use are still not operational, more than eight years after the project started. Without these components, PII continues to be at risk of loss.

In our audit of the IRS's implementation of software tools, we reported that the initial scope of the IBM Rational tools migration is being implemented successfully. The IRS estimated that it has been using IBM Legacy Rational tools for at least 12 years. The IBM Rational Collaborative Lifecycle Management tools solution replaces several IBM Legacy Rational tools and delivers requirements management, quality management, change and configuration management, project planning, and tracking. These integrated capabilities foster greater communication, collaboration, and visibility to accelerate delivery, improve quality, and support better development decisions. Figure 10 compares the IBM Legacy Rational tools and the Rational Collaborative Lifecycle Management tools solution.

Figure 10: IBM Legacy Rational Tools Versus the Collaborative Lifecycle Management Tools Solution

Legacy Rational Tool	Rational Collaborative Lifecycle Management Tools Solution	IRS Usage
Rational RequisitePro	Rational DOORS Next Generation • Capture Requirements. • Complete Traceability. • Collaborate and Review. • Generate Reports.	Manage requirements and business rules.
Rational ClearCase, Rational ClearQuest	Rational Team Concert • Work Item Management. • Project Planning. • Source Code Management. • Build Management (Automation).	Track defects for testing, changes for requirements, source code management, project planning, and build management.
Rational Test Manager	Rational Quality Management • Comprehensive Test Plans. • Streamlined Manual Testing. • Reporting With Purpose. • Requirements-Driven Testing.	Manage test cases, defect reporting, and traceability.

Source: IRS Rational Tools Initiative management.

During our review, the IRS was in the process of migrating Rational RequisitePro to Rational DOORS Next Generation. In March 2018, the IRS met its deadline for completing the migration of 135 projects with 268 repositories from Rational RequisitePro to Rational DOORS Next Generation. The IRS has also defined the scope of work required for the migration of 170 Rational ClearCase projects to Rational Team Concert. The Rational Tools Initiative team is currently developing a migration strategy and a time frame. However, some project owners may not convert to Rational Team Concert if they are successfully using Rational ClearCase. This would result in the IRS paying for two different tools that perform the same function. Issuing a policy directive to employees requiring the migration and use of Rational Team Concert would prevent the IRS from paying for and servicing two Rational tools with similar functionality.

In our audit of the IRS's management of e-mail records, we found that the IT organization has substantially completed its migration of mailboxes from Exchange 2010 to Exchange 2016. This involved the migration of active and deprovisioned user mailboxes, as well as shared mailboxes. The existing e-mail infrastructure had three e-mail domains, which consisted of the IRS Main, Chief Counsel, and CI domains. The migration of mailboxes to the IRS Main domain was complete as of May 31, 2019, except for the migration of 20 percent of the Chief Counsel active users and 7 percent of the Chief Counsel shared mailboxes. There are 179 Chief Counsel users remaining to be migrated, of which 100 are general Chief Counsel users and 79 are Criminal Tax unit users. These remaining users will be migrated pending the renewal of software licenses for a migration tool that expired during the Government shutdown and the receipt of the Department of Justice approval to migrate Criminal Tax unit users.

During our review, we tested the completeness of the move of mailbox contents from Exchange 2010 to Exchange 2016 for the IRS Main, Chief Counsel, and CI users. The IRS provided us with a list of users who had been migrated to Exchange 2016; the list included a total of 194,609 users. We matched the Exchange 2016 users to IRS employees in the Treasury Integrated Management Information System. The management information system is an official automated personnel and payroll system for storing and tracking all employee personnel and payroll data. The match determined that there were a minimal number of employees, 50 in total, comprised of 21 IRS Main/Chief Counsel users and 29 CI users who were not in the Exchange 2016 list of migrated users. Subsequently, the IRS provided documentation to validate that 47 of the 50 employees were actually migrated to Exchange 2016, and that the three remaining employees did not have a business need for an e-mail account.

We also found that the EEU project was not compliant with the enterprise life cycle methodology's commercial-off-the-shelf development path. In June 2016, the Enterprise Life Cycle office issued a memorandum stating that infrastructure projects did not need to follow the enterprise life cycle methodology. The Enterprise Operations function decided that the EEU project was solely an infrastructure project and did not need to follow the enterprise life cycle methodology's commercial-off-the-shelf development path. However, the EEU project involved implementing new hardware, programming scripts to customize the installation of the commercial-off-the-shelf product, as well as configuring a new release of systems software that encompassed significant functionality changes configuring systems software parameters affecting the environment, security, audit logs, and site resiliency.

In August 2016, the EEU project team recommended to the Enterprise Operations Executive Steering Committee that the EEU project should follow both the enterprise life cycle methodology and the *Project Management Framework*.[92] In October 2016, the EEU project team met with the Enterprise Life Cycle office to create an EEU Project Tailoring Plan to identify the artifacts that they agreed to follow to comply with the enterprise life cycle methodology's commercial-off-the-shelf development path. The plan included creating a

[92] The Enterprise Operations function created the *Project Management Framework* to help ensure that Enterprise Operations function projects achieve operational readiness, which considers factors such as: Does the proposed hardware conform to the Enterprise Standards Profile? Have procurement requirements been approved? Has new hardware been received? Have system environments been installed and are they ready for use? Are hardware and software licenses current and will not expire within six months of deployment? However, the *Project Management Framework* does not address software development.

Business System Report, a *Simplified Design Specification Report*, as well as conducting software development milestone exit reviews.

In October 2017, the EEU project team contacted the Requirements Engineering Program office to request a waiver of the *Business System Report*. The Requirements Engineering Programming office decided that it could not grant a waiver for any of the enterprise life cycle methodology artifacts after the fact because the EEU project had already been deployed for use. In addition, we found that the EEU project obtained a waiver from the Enterprise Services function's Solution Engineering Directorate, for completing the *Simplified Design Specification Report*, and did not hold software development milestone exit reviews. Accordingly, the programming of custom scripts and the configuration of systems software parameters were being managed without sufficient controls and oversight that are inherent to the enterprise life cycle methodology, *i.e.*, *Business System Report*, *Simplified Design Specification Report*, and milestone exit reviews.

Data retention

Data retention is the storage of an organization's data for compliance or business reasons. Reasons for data retention can include: complying with Federal regulations; supporting decisions made by management; and the ability to recover business critical data in the event of data loss, such as a fire or flood. In our audit of the IRS's management of e-mail records, we found executive e-mail records are retained permanently using the National Archives and Records Administration approved Capstone approach. The Capstone approach manages e-mail retention categories and scheduling based on the positions the e-mail account owners hold within the organization. The IRS decided to implement the Capstone approach to retain permanent e-mails for senior officials, including the Head of the agency, principal assistants, deputies, as well as principal management positions such as the CIO and Chief Financial Officer, directors of significant program offices, and advisory positions.

In total, the IRS has 85 Capstone positions that it maintains. The IRS is using a high watermark approach, meaning that once an employee holds a Capstone position, even if they leave that position, their retention setting will always be set to never expire. For the IRS Main and Chief Counsel domains, we reviewed the September 2018 *Capstone Reconciliation Report* and the process used to create it and found that the PGLD office is effectively reconciling Capstone employees in Exchange 2016 to the Treasury Human Resources Connect System, thereby ensuring that Capstone employees' retention settings are properly set. For the CI domain, CI has only six Capstone positions to track and manually reconciles its Capstone roles using the *CI Capstone User Spreadsheet*.

Moreover, we found that appropriate retention settings have been applied to user e-mails. E-mails for Capstone users will be retained at the IRS and then after 20 years, transferred to the National Archives and Records Administration. The IRS decided to set its retention for non-Capstone employees to 20 years, unless the employee's account has been placed on litigation hold. For employees whose accounts have been placed on litigation hold, the IRS retention policy is set to never expire, as long as the litigation hold indicator is applied to the user's e-mail account. Once the Chief Counsel's office determines that the hold is no longer needed, the attorney will mark the hold as inactive and a script will run to remove it from the user's mailbox. Once the 20-year retention period has passed, the IRS will transfer on an annual basis all permanent Capstone e-mail records to the National Archives and Records Administration and will delete all e-mails for non-Capstone employees.

We selected purposive samples[93] to test the retention setting controls the IRS applied to user e-mail accounts. We reviewed the e-mail accounts of 26 current and two departed Capstone employees from the IRS Main and Chief Counsel September 2018 *Capstone Users Report*. We also reviewed the e-mail accounts of four current and one departed Capstone employees from the *CI Capstone User Spreadsheet*. We found that the 33 e-mail accounts were properly set to the executive retention schedule of unlimited retention. We also reviewed the e-mail accounts of 30 non-Capstone employees selected from the Outlook Global Address List. We found that the appropriate retention setting had been enabled for all 30 non-Capstone employees' e-mail accounts. In addition, we reviewed the e-mail accounts of 10 employees from the litigation hold database maintained by Chief Counsel to determine if the litigation hold was enabled and if it was enabled in a timely manner. We examined the e-mail accounts of six IRS Main employees, two Chief Counsel employees, and two CI employees. We found that the litigation hold feature had been properly enabled for all 10 e-mail accounts.

Information technology service and helpdesk requests

The IT organization provides and maintains the information technology products and services needed by the IRS to deliver tax administration. This includes providing information technology services to maintain IRS operations, implement legislation, maintain security over taxpayer data, and ensure the timely delivery of the individual tax return filing season. The use of some IT organization resources is mandated by statute through the budget allocation process. For example, IT organization funds needed to implement the Health Coverage Tax Credit legislative mandate were included in the Fiscal Year 2017 IT organization budget. The remaining IT organization resources are used to support IRS business unit requests for services as well as to support ongoing operation and maintenance of IRS systems.

For Fiscal Year 2019, TIGTA conducted two audits in the area of information technology service and helpdesk requests. We initiated an audit[94] to evaluate the effectiveness of IRS efforts to prioritize computer programming requests to support effective tax administration. We found that the allocation of information technology resources is primarily set by the IT organization, with minimal involvement from the business units. For example, each year the IT organization identifies the IRS's annual information technology service priorities. For Fiscal Year 2018, the

[93] A purposive sample is a nonprobability sample, the results of which cannot be used to project to the population.
[94] TIGTA, Ref. No. 2019-40-043, *Unmet Needs for Information Technology Support Result in Inefficiencies and Higher Tax Administration Costs* (July 2019).

IT organization established two primary priorities for use in allocating information technology resources: maintain current operations and deliver the individual tax return filing season. IT organization management indicated that these priorities reflect the areas in which the need for information technology services has historically been the greatest.

IT organization management also stated that while the IRS Senior Executive team[95] establishes the overall direction and priority of the operations support required for the agency, the IT organization has sole discretion as to which information technology services it will provide to the business units. It does not consult or include the business units in establishing the discretionary IT organization resource priorities. As a result, there is a concern on the part of the business units that their lack of participation limits their input when establishing agency priorities for determining how to allocate IT organization resources.

We also found that information technology service requests denied during the precoordination step to identify information technology service needs are not tracked and maintained in the Work Request Management System. As a result, the extent of organizational demand for information technology services is unknown. The management system does not accurately reflect resources needed based on business unit identification and requests. For example, Small Business/ Self-Employed Division management stated that in Calendar Year 2016, 50 requests for identified needs were not formally submitted into the Work Request Management System. Wage and Investment Division management was unable to determine the number of requests that were denied during precoordination.

In addition, we found that the process for requesting information technology services may discourage business units from submitting requests that would result in more efficient and effective tax administration. Small Business/Self-Employed Division and Wage and Investment Division management stated that, before submitting a request for information technology services, they explore whether a nonsystemic alternative can be implemented to address their need, even if a systemic solution would result in more efficient and effective tax administration.

When we asked Wage and Investment Division management why they would not submit the request for information technology service, they stated that the IT organization is more likely to deny the request during precoordination if there is a nonsystemic alternative. For example, the Wage and Investment Division explored the option of creating an electronic inventory system for the Accounts Management Return Integrity and Compliance Services' Integrity and Verification Operation organization to replace the existing labor-intensive manual inventory process. The manual inventory system requires creating a spreadsheet, monitoring the referrals to ensure receipt of requested information from the taxpayer, and returning the taxpayer's response to the

[95] The Senior Executive team consists of the IRS Commissioner; Deputy Commissioner for Services and Enforcement; Deputy Commissioner for Operations Support; Chief of Staff; Chief Risk Officer; Chief, Appeals; Chief, Communications and Liaison; National Taxpayer Advocate; Chief Counsel; Chief, CI; Chief, Facilities Management and Security (formerly Agency-Wide Shared Services); Chief Financial Officer; the CIO; Human Capital Officer; Chief, Procurement Officer; and business unit executives.

requestor. Wage and Investment Division management indicated that the electronic inventory system would result in a cost savings that includes the reduction of 15 full-time employees and would provide increased accuracy, efficiency, and timeliness when resolving Integrity and Verification Operation cases. The IT organization denied the request due to insufficient resources.

Additionally, we found that due to insufficient resources, projects are not completed that would reduce taxpayer burden, protect revenue, and save significant IRS resources. Our review of information in the Work Request Management System for 82 requests submitted in Calendar Year 2016 and denied after precoordination found that the two most common reasons for denial were: 1) the work was discretionary rather than mandatory and 2) there were insufficient funds or resources to complete the request.[96] Small Business/Self-Employed and Wage and Investment Division executives indicated the requests that were denied had an impact on tax administration with the potential for billions of dollars in lost revenue due to large corporations underpaying their tax liabilities, taxpayers not receiving proper credits, and the IRS having to pay a large amount of interest due to more than $5 million in withholding not being credited to taxpayer accounts.

Finally, we found that the Work Request Management System used to track information technology requests does not always accurately reflect information technology service request status and actions taken. For example:

- Information technology service requests denied in precoordination are not captured. Processes do not require all requests to be submitted via the Work Request Management System, nor is consolidated information maintained to support the reason that a request was denied during precoordination. Because denied requests are not captured, the IT organization cannot identify requests denied due to insufficient resources that could be fulfilled if additional resources become available later.

- The status of work requests is not always accurate. Our review of 943 completed work requests as of May 31, 2018, identified 64 requests (7 percent) for which information in the notes section of the Work Request Management System contradicted the status. While the notes section included language such as stopped/halted, no longer impacted, or recommended for denial, IRS management confirmed that 38 requests (59 percent) were completed and implemented, 23 requests (36 percent) had not been completed, and three requests (5 percent) were partially completed and implemented.

- Required information was not consistently captured to describe why information technology requests were denied. Our review of the 82 denied work requests submitted in Calendar Year 2016 identified 18 requests (22 percent) for which information was not

[96] The IRS uses the word "discretionary" for work requests submitted to update an information technology application's functionality, enhance existing systems, create a new capability to support the IRS's mission, make changes to current applications, or make programming updates to enhance functionality.

included in the Work Request Management System to describe why the IT organization denied the request.

- IT organization resources and contractor costs were not always captured as required. Our review of 1,164 work requests submitted in Calendar Year 2016 identified 80 requests (7 percent) for which the estimated staff hours, actual staff hours, and contracting costs were not included in the Work Request Management System as required.

We also initiated an audit[97] to assess the effectiveness and efficiency of the processes and practices for resolving information technology incidents and reported problems for the IRS's tax administration systems. We found that the IRS has taken steps to improve its controls over incident ticket management, such as identifying and implementing initiatives to enhance the overall customer experience and to foster more effective and efficient incident management operations. However, we also found that the IRS can take additional steps to improve incident management performance levels and metrics reporting as well as incident ticket resolution efficiency.

Specifically, we reviewed Priority (P) 1 through P4 incident tickets and found that the IRS has not generally improved the percentage of tickets resolved and closed within their target resolution times over the last three fiscal years. Using the *Open Time* and *Close Time* fields from the Knowledge Incident/Problem Service Asset Management-Service Manager module, the percentages of incident tickets resolved within their target resolution times for Fiscal Year 2018 have decreased when compared to Fiscal Year 2017 for all four priority levels. In addition, when compared to Fiscal Year 2016, the Fiscal Year 2018 percentages decreased for three of the four priority levels.

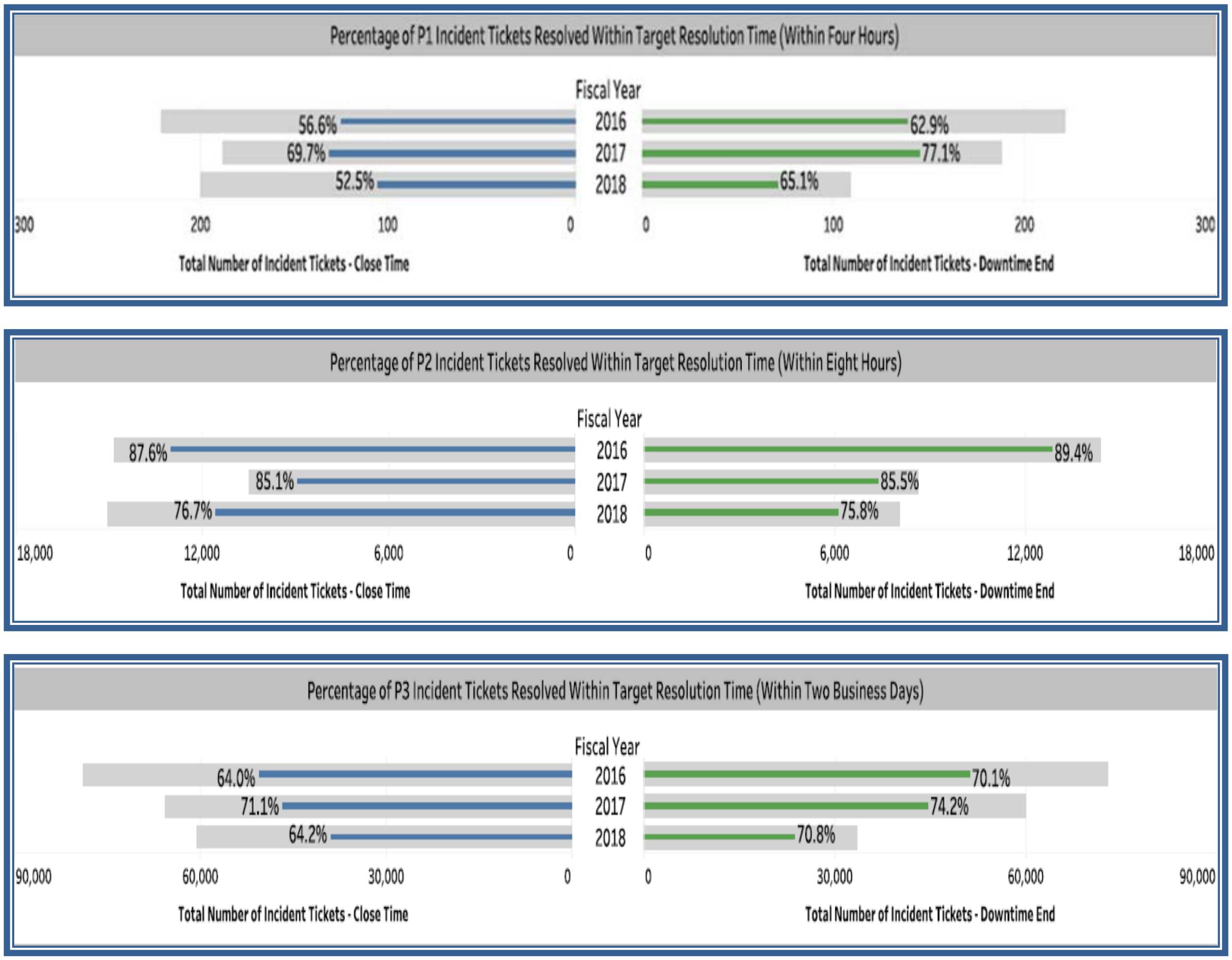
In discussions with Enterprise Operations function management, they stated that assessing the effectiveness of the resolution of incident tickets is a much more complicated calculation than just using the *Open Time* and *Close Time* fields from the Knowledge Incident/Problem Service Asset Management-Service Manager module. For example, some incident tickets are left open and monitored to ensure that their issues have been fully resolved or to identify and associate other incident tickets with similar issues, resulting in the incident tickets remaining open and not immediately closed. In these situations, a more accurate indicator to calculate the incident ticket resolution time is to use the *Downtime End* field, which provides the actual time it took for an incident to be resolved.

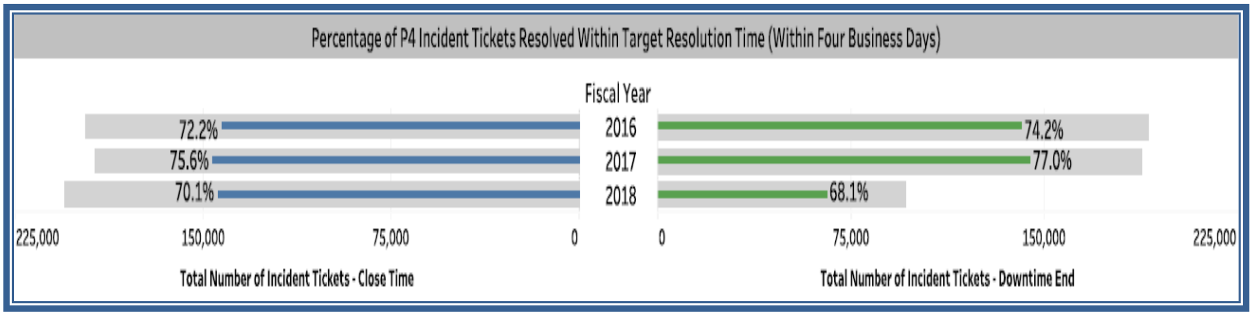
Based upon this information, we recalculated the percentage of incident tickets resolved within the target resolution times by priority level and fiscal year, using the *Open Time* and *Downtime End* fields. However, the *Downtime End* field was not always populated in the Knowledge Incident/Problem Service Asset Management-Service Manager module as this field is only used for incident tickets that are left open to ensure that their issues have been fully resolved or to

[97] TIGTA, Ref. No. 2019-20-055, *Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets* (Sept. 2019).

associate other tickets with similar issues. For example, 143,132 (50.9 percent) of 281,102 incident tickets closed in Fiscal Year 2018 did not have any information in the *Downtime End* field, leaving only 137,970 incident tickets with the field populated. From incident tickets with that field populated, the percentage of incident tickets resolved within their target resolution times between Fiscal Years 2017 and 2018 have decreased for all four priority levels as in our initial assessment. However, when compared to Fiscal Year 2016, the percentages for only two of the four priority levels decreased in Fiscal Year 2018. Figure 11 provides a side-by-side comparison of the percentages of incident tickets resolved within their target resolution times by priority level and fiscal year, using the *Close Time* and *Downtime End* fields.

Figure 11: Percentage of Incident Tickets Resolved Within Target Resolution Times by Priority Level and Fiscal Year (Comparison Between Close Time and Downtime End Fields)





Source: TIGTA review of incident tickets closed between October 1, 2015, and September 30, 2018, from IRS-provided data extracts of the Knowledge Incident/Problem Service Asset Management-Service Manager module.

In addition, we found that in Fiscal Year 2018, the IRS met its monthly performance goals more than 50 percent of the time for only 12 of its 25 incident management metrics, *e.g.*, *Overage Tickets – Level 1*, *Resolution Timeliness*, *User and Network Services Percent on Time – Level 1: P2*. Only seven of the 25 incident management goals, *e.g.*, *Call Handle Time*, *Customer per Deskside Technician*, *First Level Resolution*, were consistently met for 10 months or more during the fiscal year. It is important to resolve incident tickets within target resolution times to minimize the level of disruption to the IRS and its ability to consistently process taxpayer returns and further tax administration.

We also found that incident management metrics are not consistently used or not used at all. Based on the results of our analysis of incident management data, we sent a survey to employees who management identified as receiving one or more of the metric reports. We sent the survey to 69 employees (12 Enterprise Operations function and 57 User and Network Services function employees) and asked each employee to identify the report(s) received, the incident management metric(s) reviewed, and how the metric(s), if any, are used to manage their respective program or function. Of the 57 employees (seven Enterprise Operations function and 50 User and Network Services function employees) who responded, we made the following observations:

<u>Enterprise Operations function employees</u>

- Three employees responded that they do not use the Enterprise Operations function incident management report because they no longer work in the program or functional area.[98]
- Three employees responded that they just do not use the report.
- One employee responded that the metrics in the incident management report are "descriptive," *e.g.*, identify surges in work on a particular day and time, but does not

[98] This is the *EOps [Enterprise Operations] ITOCC [Information Technology Operations Command Center] Metrics Dashboard* report.

believe the metrics provide the necessary information to make timely decisions to be effective.

User and Network Services function employees

- 6 employees responded that they do not use User and Network Services function incident management reports because they no longer work in the program or functional area.[99]
- 8 employees responded that they just do not use the reports.
- 36 employees responded that they use one or both of the reports.

Moreover, we found that incident ticket resolution efficiency would improve with better documentation of incident assessments and actions taken to potentially help reduce the number of ticket reassignments. Specifically, we believe that incident tickets with multiple reassignments provide indications of potential workflow inefficiencies, resulting from improper routing of the tickets.

To obtain a perspective of the extent of reassignments and sufficiency of documentation, we obtained and reviewed a judgmental sample of 16 closed incident tickets with four or more reassignments during Fiscal Year 2018. Based on our analysis of the documented actions performed in the *Activities* section of the incident tickets, we determined that seven of the 16 tickets may have had inefficiencies in working the incident between first-level support specialists and service providers. For example, one incident ticket was reassigned to various service providers 16 times, while another incident ticket was mostly reassigned back and forth between two service providers 12 times, including one reassignment back to a first-level support specialist. In both cases, documentation of the actions performed or reasons provided for the reassignment were minimal, if documented at all. Without proper documentation of actions performed, the next first-level support specialist or service provider working on the incident ticket may not know what work was performed or what still may be needed to resolve the issue. This can lead to multiple reassignments and inefficiency in working incident tickets.

Risk management

Risk management is the process of identifying, monitoring, and mitigating project and program risks. Effective risk management emphasizes the need to integrate risk management into existing business activities of an agency. It can help the IRS, including its IT organization, more securely and effectively administer the Federal tax system by identifying and mitigating emerging risks before they affect performance.

[99] These are the *UNS [User and Network Services] Balanced Scorecard* and the *UNS Operational Dashboard* reports.

During Fiscal Year 2019, TIGTA initiated an audit[100] to assess the effectiveness of the IT organization's risk management process. Overall, we found that information technology risks are identified, assessed, and reported, but mitigation documentation and oversight need improvement.

The IRS has appointed a Chief Risk Officer and established a risk management structure. The Chief Risk Officer oversees the Enterprise Risk Management program to identify and assess risks, which provides an enterprise-wide approach to risk management. It also helps the IRS incorporate risk management principles into its strategies and provides senior management the information necessary to make sound decisions. The IRS has defined roles and responsibilities for the Chief Risk Officer, senior risk advisors, and Enterprise Risk Management liaisons. The IRS also established an Executive Risk Committee, comprised of senior management, to facilitate collaboration on enterprise risk decisions and a risk working group, which includes representatives from the various IRS business units and functional offices.

On an annual basis, the Office of the Chief Risk Officer facilitates an enterprise-wide risk assessment. The Office of the Chief Risk Officer guidance specifies that business unit leadership should manage and monitor its risks on an ongoing basis. Accordingly, business units, including the IT organization, provide a business unit risk register to the Office of the Chief Risk Officer annually. The business unit risk register is a mechanism to document and monitor identified risks. The Office of the Chief Risk Officer aggregates the results and provides initial reports to the risk working group. In turn, the risk working group analyzes the results from an enterprise perspective and works with the Office of the Chief Risk Officer to develop a proposed enterprise risk list.

We obtained and reviewed the IT organization's 2017 and 2018 business unit risk registers. The register is prepared once a year by the Information Technology Risk Liaison. Once the business unit risk register is generated, it is discussed among the Associate CIOs and the CIO before it is shared with the Chief Risk Officer. However, the IT organization's business unit risk register is not updated throughout the year as recommended.

In addition, we reviewed a judgmental sample of 18 function risks and 15 program risks and found that the IT organization's functions and programs are identifying, assessing, and reporting risks, but information on risk mitigation plans, mitigation activities, and closure rationale, as well as closure documentation, is not being captured in sufficient detail to enable us to conclude if risks were being appropriately mitigated. We found that not all 18 function risks included detailed descriptions of or had descriptions for risk mitigation plans and mitigation activities. For example, the mitigation plan for an Applications Development function risk stated, "Coordinate with delivery partners to align on regression testing timeline for FS 19," without providing any further details. In addition, the listed mitigation activities were not detailed for

[100] TIGTA, Ref. No. 2019-20-052, *Information Technology Risks Are Identified, Assessed, and Reported, but Mitigation Documentation and Oversight Need Improvement* (Aug. 2019).

this risk and there was no closure rationale. Overall, for the 18 function risks, nine function risks did not include closure rationale, four did not include detailed descriptions of closure rationale, and the five remaining risks did not require a closure rationale because they remained candidate risks. Closure documentation was unavailable for seven function risks and not expected for the remaining 11 risks that either were withdrawn or were not closed, *i.e.*, open risks and candidate risks.

Although all 15 program risks generally had some basic information, we found that 13 risks did not include detailed descriptions of the risk mitigation plans, 12 risks did not include detailed descriptions of the mitigation activities, 14 risks did not include detailed descriptions of the closure rationale, and 12 risks did not have detailed closure documentation. For example, the mitigation plan for a Foreign Account Tax Compliance Act risk stated, "Prepare Solaris contract extension, create environment, create barrier, remove tiger team," and the closure rationale provided was, "Environments delivered," without providing any further details. In addition, mitigation activities were not detailed for this risk and there were no closure documents available. Overall, mitigation plans were unavailable for two program risks, mitigation activities were unavailable for three risks, and closure documentation was unavailable for three risks. One risk did not require a closure rationale because it was reopened. Without a complete description of the risk mitigation plans, mitigation activities, and closure rationale, as well as closure documentation, it will be more difficult for the IT organization to effectively monitor and manage its outstanding information technology risks.

The lack of detail is attributed, in part, to some of the IT organization functions using a risk management tool that does not capture essential information. For example, four functions use the Item Tracking Reporting and Control system to track risks, while two functions use ProSight®. There are two important fields captured in the Item Tracking Reporting and Control system that are not captured in ProSight: closure rationale and risk mitigation activity.

The Item Tracking Reporting and Control system user guide also requires detailed descriptions of the mitigation activities and closure rationale. However, none of the function or program risks maintained in the Item Tracking Reporting and Control system that we reviewed contained enough information for us to evaluate their dispositions properly.

In addition, the Associate CIO, Strategy and Planning, also mandated via a *Risk, Issue, and Action Item Management Directive,*[101] that all information technology programs and projects should record and maintain risks in the Item Tracking Reporting and Control system. However, no mention of this requirement was extended to IT organization functions. By not mandating that the functions use the Item Tracking Reporting and Control system uniformly, some important risk mitigation information is not being captured.

[101] Dated June 18, 2018.

Further, we found that accepted unmitigated risks are not being reassessed. We judgmentally selected five IT organization risk acceptance form and tools (RAFT) for detailed testing.[102] We reviewed the RAFTs for proper approvals and for evidence that management was reviewing and reassessing the accepted risks covered in the RAFTs quarterly. We determined that there were proper management approvals for our sample of the RAFTs. However, management had not reviewed and reassessed all five RAFTs quarterly as required. Accordingly, we expanded our review to include the total population of 20 IT organization RAFTs and observed that 19 had not been reassessed quarterly. For 16 of the RAFTs, the reassessment date was either scheduled or occurred at least one year or more after the RAFT was prepared and IT organization management accepted the risk. Without evidence of regular reviews of the RAFTs, there is limited assurance that the status of the RAFTs is accurate, appropriately reconsidered for mitigation, and properly communicated to the Chief Risk Officer.

[102] The RAFT inventory included 22 total enterprise RAFTs, of which 20 were specifically related to the IT organization.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the adequacy and security of the IRS's information technology[1] program. This review is required by the IRS Restructuring and Reform Act of 1998.[2] To accomplish our objective, we:

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

II. Obtained and reviewed the *IRS Integrated Modernization Business Plan* to provide an overview of it.

III. 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 2019. During the review, we analyzed and prepared an assessment of the systems security and privacy issues.

   B. Identified and summarized other relevant TIGTA and/or external oversight assessments dealing with systems security and privacy.

IV. 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 2019. During the review, we analyzed and prepared an assessment of the systems development issues.

   B. Identified and summarized other relevant TIGTA and/or external oversight assessments dealing with systems development.

V. 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 2019. During the review, we analyzed and prepared an assessment of the systems operations issues.

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

B. Identified and summarized other relevant TIGTA and/or external oversight assessments dealing with systems operations.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. 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 2019. 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
Jason Rosenberg, Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Deputy Chief Information Officer for Filing Season and Tax Reform
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, Enterprise Audit Management

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	GAO-19-150	*FINANCIAL AUDIT: IRS's Fiscal Years 2018 and 2017 Financial Statements*	November 9, 2018
2	GAO-19-49	*INFORMATION TECHNOLOGY: Departments Need to Improve Chief Information Officers' Review and Approval of IT [Information Technology] Budgets*	November 13, 2018
3	2019-20-008	*The Solaris to Linux Migration Project Was Delayed and Needs Improved Governance*	December 6, 2018
4	2019-40-012	*Partnership With State and Industry Leaders Is a Key Focus in Further Reducing Tax-Related Identity Theft*	December 27, 2018
5	2019-20-005	*Management and Implementation of Information Technology Software Tools Needs Improvement*	February 21, 2019
6	2019-20-017	*Electronic Authentication Security Controls Have Improved, but Continued Progress Is Needed to Ensure the Protection of Public-Facing Applications*	April 19, 2019
7	GAO-19-340	*TAXPAYER INFORMATION: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices*	May 9, 2019
8	GAO-19-288	*DATA PROTECTION: Federal Agencies Need to Strengthen Online Identity Verification Processes*	May 17, 2019
9	2019-20-031	*Software Version Control Management Needs Improvement*	June 13, 2019
10	2019-24-035	*The Internal Revenue Service Completed Extensive Programming and Systems Changes in a Compressed Timeframe for the 2019 Filing Season*	June 17, 2019
11	2019-20-038	*Controls Over Information Technology Procurements Need Improvement*	June 19, 2019

No.	Report Reference Number	Audit Title	Report Issuance Date
12	2019-40-043	*Unmet Needs for Information Technology Support Result in Inefficiencies and Higher Tax Administration Costs*	July 3, 2019
13	GAO-19-474R	*MANAGEMENT REPORT: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls*	July 18, 2019
14	2019-20-052	*Information Technology Risks Are Identified, Assessed, and Reported, but Mitigation Documentation and Oversight Need Improvement*	August 14, 2019
15	2019-20-049	*The First Phase of the Data Loss Prevention Solution Is Working As Intended, but the Remaining Phases Continue to Experience Delays*	August 22, 2019
16	2019-20-046	*The Bring Your Own Device Program's Security Controls Need Improvement*	September 12, 2019
17	2019-20-060	*E-Mail Records Management Is Generally in Compliance With the Managing Government Records Directive*	September 12, 2019
18	2019-20-055	*Controls Should Be Strengthened to Ensure Timely Resolution of Information Technology Incident Tickets*	September 13, 2019
19	2019-20-062	*Some Components of the Privacy Program Are Effective; However, Improvements Are Needed*	September 20, 2019
20	2019-20-061	*Firewall Administration Needs Improvement*	September 24, 2019
21	2019-20-082	*Fiscal Year 2019 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act*	September 24, 2019

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.
Adobe® Systems Flash Player	Software used to stream and view video, audio, and multimedia on a computer or supported mobile device.
American Customer Satisfaction Index Score	The only national cross-industry measure of customer satisfaction in the United States. Each year, roughly 300,000 customers are surveyed about the products and services that they use most. The survey data serve as inputs to an econometric model that benchmarks customer satisfaction with more than 400 companies in 46 industries and 10 economic sectors as well as various services of Federal and local government agencies.
Antivirus Software	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 the profiles of 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.
Artifact	The output of an activity performed in a process/procedure, which is created throughout the life cycle of a project.
Asset Manager	Tracks information technology and non-information technology equipment used throughout the IRS.

Term	Definition
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
Audit Trail	A record showing who has accessed an information technology system and what operations the user has performed during a given period.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
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.
BigFix®	A set of IBM products that leverage a single infrastructure, single agent, and console, enabling continuous monitoring, threat protection, and incident response across servers, laptops, and desktops regardless of their location. A content-driven messaging and management system. This technology distributes the work of managing information technology infrastructures out to the managed devices themselves, providing for scalability and flexibility. The single, multipurpose agent controls multiple services regardless of where the endpoint is, optimizing configuration control and minimizing security risks.
*******2******* *******2******* *******2*******	***************************2**************************** ******2******.
Bona Fide Needs Rule	Requires appropriated funds be used only for goods and services for which a need arises during the period of that appropriation's availability for obligation.
Bug	An error or defect in software or hardware that causes a program to malfunction.
Business Case	Structured proposal for business improvement that functions as a decision package for organizational decision makers. 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.

Term	Definition
Business Unit	A title for major IRS organizations such as Appeals, Wage and Investment Division, the Office of Professional Responsibility, and Information Technology organization.
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. In September 2016, the IRS announced that it will streamline submission processing at its campuses. The Ogden Campus will process most business tax returns after September 2019, while the Kansas City Campus will process most individual paper returns after September 2024.
Capstone	An approach that manages e-mail retention categories and scheduling based on the positions the e-mail account owners hold within the organization. The IRS decided to implement the Capstone approach to retain permanent e-mails for senior officials, including the Head of the agency, principal assistants, deputies, as well as principal management positions such as the CIO and the Chief Financial Officer, directors of significant program offices, and advisory positions.
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.
Change Log	Audit trail records that capture activities before and after changes are made to the baseline configurations for information technology products, including those made to remediate vulnerabilities. It registers any changes made to the configuration of the system as well as who made them and when they were made.
Change Request	The method for requesting approval to change a baselined product or other controlled item.
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.
COBIT® 5	Best practice that provides a comprehensive framework that assists enterprises in achieving their objectives for governance and management of enterprise information technology assets.

Term	Definition
Common Vulnerability Scoring System	Provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.
Computer Security Incident Response Center	Positioned to be proactive in preventing, detecting, and responding to computer security incidents targeting the IRS's enterprise information technology assets. It provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS enterprise.
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 systems 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 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 or individual 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.
Credential Service Provider	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers.

Term	Definition
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.
Critical Pay Authority	An agency may request critical pay authority only after determining that the position in question cannot be filled with an exceptionally well-qualified individual through the use of other available human resources flexibilities and pay authorities.
Customer Account Data Engine 2	Establishes a single database that houses all individual taxpayer accounts, including Individual Master File data, which provides IRS employees the ability to view updated account information online.
Cyberattack	An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network.
Data	Information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data. Computer data may be processed by the computer's central processing unit and is stored in files and folders on the computer's hard disk.
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.
Data-at-Rest	Provides the capability to scan data residing in data repositories to identify data vulnerable to exfiltration. These data repositories can include data on workstations, server drives, or network shares. Once data at risk are identified, appropriate actions can be taken, including encrypting the data or deleting the data if they are not needed.
Data-in-Motion	Refers to data being transmitted outside of the organization through Internet routers, e-mail gateways, and web proxies.
Data-in-Use	Refers to data accessed or used by a system at a point in time. This includes copying data to a thumb drive, sending information to a printer, or even cutting and pasting between applications.

Term	Definition
Database	A computer system with a means of storing information in such a way that information can be retrieved.
Death Master File	A Social Security Administration database that contains death information about individuals. The IRS obtains and uses this file to identify tax accounts associated with deceased individuals.
Department of Justice	The department of the U.S. Federal Government charged with the responsibility for the enforcement of Federal laws.
Direct Pay	A system that can be accessed through IRS.gov in which individual taxpayers can make payments to the IRS from their bank account.
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.
DOORS Next Generation	Part of the Collaborative Lifecycle Management tools solution, which replaced several IBM Legacy Rational® tools and delivers requirements management, quality management, change and configuration management, project planning, and tracking.
Earned Income Tax Credit	A tax credit for certain people who work and have income under established limits.
e-File	A method to securely file and pay taxes online through an IRS-approved electronic channel.
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.
Electronic Return Originator	The authorized IRS e-filing provider that originates the electronic submission of a return to the IRS.
Encryption	Conversion of plain text to cipher text through the use of a cryptographic algorithm.
Enterprise Demand Management Process	A step-by-step process followed by the IRS to migrate from Oracle Solaris to IBM's zLinux operating system.
Enterprise Learning Management System	A learning management system is used for the administration, documentation, tracking, and reporting training, as well as the delivery of e-Learning. The Enterprise Learning Management System is the IRS Learning Management System, which is the system of record for all IRS training.

Term	Definition
Enterprise Life Cycle	A structured business systems development method that requires the preparation of specific work products during different phases of the development process. The enterprise life cycle establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduce the risks of systems development and ensure alignment with the overall business strategy.
Enterprise Self-Assistance Participation Rate	Measures the percentage of instances in which a taxpayer uses one of the IRS's self-assistance service channels, *i.e.*, automated calls, web services, versus needing support from an IRS employee, *i.e.*, face-to-face, over the telephone, via paper correspondence.
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.
Enterprise Standards Profile Product Catalog	A list of IRS approved products, *e.g.*, updated software versions, and standards. The products listed in the catalog have been evaluated and approved for use within the IRS environment.
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.
e-Services	Provides a set of web-based business products as incentives to third parties to increase e-filing; also provides electronic customer account management capabilities to all businesses, individuals, and other customers.
Exchange	An e-mail and calendar server that runs exclusively on Microsoft® Windows server operating systems.
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.
Extended Validation Secure Sockets Layer Certificate	The highest form of a secure sockets layer certificate, which is issued from a trusted certificate authority. It uses a cryptographic key to provide validation for a web server, detailing its domain name, server name, host name, company name, and location.
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.

Term	Definition
Federal Information Security Modernization Act Evaluation Period	A period of time from July 1 through June 30 of the following calendar year.
Federal Trade Commission	A Federal agency with a dual mission to protect consumers and promote competition. It protects consumers by stopping unfair, deceptive, or fraudulent practices in the marketplace. It promotes competition by keeping prices low and the quality and choice of goods and services high.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
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.
First-Level Support Specialist	The initial customer contact and is responsible for recording, classifying and prioritizing, investigating and diagnosing, resolving or forwarding, and closing incidents as well as monitoring their progress.
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.
Flexera® Technopedia® Catalog	A trusted and comprehensive asset information repository of enterprise software and hardware.
Franchise Fund Shared Services Program	The Shared Services Program with the Treasury Franchise Fund provides common administrative services that benefit customers both within the Treasury Department and outside agencies.
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	Public-facing application that provides the ability to view, print, or download an individual's tax records using e-authentication.
Global Address List	A list of recipients in a Microsoft Exchange organization.

Term	Definition
Good for Enterprise Application	Combines enterprise e-mail, calendar, contacts, presence, document access, document editing, and more for Blackberry mobile devices. Users can complete any business workflow on-the-go without returning to their desktops.
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.
IDVerify	An IRS online identity verification service.
Incident Ticket	Used to document and track any unplanned interruption or reduction in the quality of an information technology service.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Information System	A set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
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.
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 business unit 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.
Interagency Agreement	A document generally between Government agencies and departments that defines cooperative work between them. The agreement defines the parties involved, the work performed, and the transfer of technologies and funds.

Term	Definition
Internal Revenue Manual	The IRS's primary source of instructions to its employees related to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
International Business Machines®	A global technology company that provides hardware, software, and cloud-based services and cognitive computing.
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.
IRS2Go	An IRS smartphone application that lets taxpayers check on the status of their tax refund, obtain tax tips, make payments, follow IRS social media, and more.
Item Tracking Reporting and Control System	A customized tool that allows users to submit and update risks, action items, and issues.
Iterative Requirements Development	A process that accelerates the gathering of programming requirements to allow the IT organization the maximum amount of time to implement the identified changes, identify gaps and risks earlier, and promote collaboration to ensure common understanding of the business need and feasibility.
Jailbroken	An attempt to bypass certain security features built into Apple® devices. Jailbreaking allows root access to the operating system and may allow a user to use applications (referred to as apps) besides those in the Apple apps store.
Knowledge Incident/Problem Service Asset Management System	A system that maintains the complete inventory of information technology and non-IT 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.
Legacy Programming Code	An application system source code type that is no longer supported and continually patched.
Legacy System	A mainframe or minicomputer information system that has been in existence for a long period of time.
Linux®	Enterprise-wide operating system designed to meet various performance, reliability, and scalability demands on a broad range of hardware, including mainframes, servers, workstations, and personal computers.
Mainframe	A powerful, multiuser computer capable of supporting many hundreds of thousands of users simultaneously.

Term	Definition
Major Investment	Treasury Department 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.
Malware	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Management Plan	Defines the project's scope of work and its approach to managing all project activities. Its purpose is to provide a framework for managing project activities and for completing the project successfully.
Migration Period	The period of time moving the use of one operating environment to another. Migration can involve upgrading to new hardware, software, or both.
Mobile Device	A portable computing and communications device with information storing capability.
Modernization	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 e-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.
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	A part of the Department of Commerce that is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
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.

Term	Definition
Office of Management and Budget	The largest component of the Executive Office of the President. The management side oversees and coordinates Federal procurement policy, performance and personnel management, information technology, and financial management. In this capacity, it oversees agency management of programs and resources to achieve legislative goals and administration policy.
Office of Personnel Management	Serves as the chief human resources agency and personnel policy manager for the Federal Government.
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.
Oracle®	A relational database management system produced by the Oracle Corporation, which is the largest software company whose primary business is database products.
Patches	Updates to an operating system, application, or other software issued specifically to correct particular problems with the software.
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, and biometric records, 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, and mother's maiden name.
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
Portal	A point of entry to a network system that includes a search engine or a collection of links to other sites, usually arranged by topic. It provides the infrastructure that allows users (including IRS employees and taxpayers) to have web-based access to IRS information.
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.
Privacy and Civil Liberties Impact Assessment	A process analyzing and documenting how PII and Sensitive But Unclassified information are used, collected, received, displayed, stored, maintained, protected, shared, and managed.

Term	Definition
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 an 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.
Privacy Impact Assessment Management System	A series of web pages that allows customers to input responses to questions about PII. It also allows privacy subject matter experts the ability to analyze the data requirements for the particular system in an electronic format.
Privileged Account	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.
Processing Year	Calendar year in which the IRS processes the tax return or document.
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.
Programming Language	A high-level language used to write computer programs.
Project Charter	A written instrument that creates and defines the rights, privileges, and membership of a project.
Project Management Framework	Comprised of best practices required to deliver and implement a project successfully and supports the IRS's project management practices, allowing for consistency and repeatability, best practices for governance and management, and knowledge sharing as well as transition amongst program/project management staff.
ProSight®	A database tool designed with specific tracking, reporting, and decisionmaking features used to monitor projects.
Protocol	A detailed plan of procedures.
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.

Term	Definition
Requirement Engineering Program Office	Provides standards and guidance to requirements engineering activities, process modeling, and requirements-related solutions. Oversees requirements development and requirements management efforts on all business change, software development, systems integration, and legacy system upgrades.
Return Integrity and Compliance Services Incident Management Database	A database in which the IRS has primarily tracked information on security incidents since December 2016.
Return Review Program	An IRS system used to identify potentially fraudulent e-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.
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 Acceptance Form and Tool	Used in an organization's approval processes to clearly document business decisions in the context of risk and acceptance.
Risk Assessment	Determining the extent to which an entity is threatened by potential adverse circumstances or events. Risk assessment for information system-related security risks includes assessment of the susceptibility to adverse impacts through information, *e.g.*, consideration of the dependence on information, the vulnerabilities in mission and business processes, the effectiveness of risk mitigations, and the assessment of the threat environment with regard to causing such impacts.
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 NIST guidelines, whether related to a technical, operational, or management control.
Rooted	A mobile device that has been modified to bypass the built-in restrictions on security, operating system use, *etc*.
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.
Ruleset	A rule that defines and compares the parameters against each connection. Specifies what services to let through a firewall.

Term	Definition
Secure Enterprise Messaging System	Outlook Secure Messaging allows you to digitally encrypt e-mail messages and attachments for transmission between IRS e-mail users. Secure Messaging is available to everyone with an Enterprise e-mail account and approved workstation. Secure Messaging is used to encrypt e-mail messages and attachments holding Sensitive But Unclassified information.
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.
Server	A computer that carries out specific functions, *e.g.*, a file server stores files, a print server manages printers, and a network server stores and manages network traffic.
Service	The supplying of helpful activities or the supplier of commodities.
Service Provider	Provides information technology services to internal and external customers.
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.
Short Messaging Service	A technology for sending short text messages between mobile phones.
Small Business/ Self-Employed Division	The IRS business unit that helps small business and self-employed taxpayers understand and meet their tax obligations.
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.
Solaris®	The UNIX®-based operating system of Sun Microsystem®.
Solution	An aggregation of products and services, as opposed to a single discreet system or piece of software, that helps solve a particular problem.

Term	Definition
Sunset Date	Intentional phasing out of a product or product version due to a predetermined retirement date or vendor published end of life (support) date. The period from identification to retirement date is the sunset period. Products in this phase will no longer be supported and are no longer approved for deployment.
System	A set of interdependent components that perform a specific function and are operational. It may also include software, hardware, and processes.
System Configuration	Provides the settings or hardware and software arrangement, and how each device and software or process interact with each other based on a system settings file created automatically by the system or defined by the user.
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 Identification Number	A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the Taxpayer Identification Number is either an Employer Identification Number, a Social Security Number, or an Individual Taxpayer Identification Number.
Threat Vector	The path or route used by an adversary to gain access to the target. The following threat vectors are used to classify incidents by the method of attack: Attrition, E-mail/Phishing, External/Removable Media, Improper Usage, Loss or Theft of Equipment, Web, Physical Cause, Other, and Multiple Attack Vectors.
Tier I	A computing infrastructure consisting of mainframe computers that handle a high volume of critical operational data.
Tier II	A computing infrastructure consisting of non-mainframe 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.
Tier III	Systems that include all workstation devices and any hardware operating under a Windows operating system, including all hardware used in a desktop environment: workstations functioning with a single-user (stand-alone) operating system including UNIX workstations that run single-user versions of UNIX and workstations that run any Windows operating system.

Term	Definition
Totally Automated Personnel System/Single Entry Time Reporting Application	An automated personnel system used by IRS management for processing requests for personnel actions, as well as employee information report generation. In addition, it is designed to accumulate time and attendance information for employees.
Treasury Human Resources Connect System	A Treasury Department personnel system that aligns employees to the manager of record and organizational code that provides employee data to other internal systems.
*********2*******®**	*****************************2****************************** *****************************2****************************** *****************************2****************************** *****************************2****************************** *****************************2****************************** *****2****.
UNIX	An operating system known for its relative hardware independence and portable application interfaces. Some of the popular UNIX derivatives are Linux and Solaris.
Virus	A segment of self-replicating code planted illegally in a computer program, often to damage or shut down a system or network.
Volunteer Income Tax Assistance Program	Specially trained 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	The IRS business unit that serves taxpayers whose only income is derived from wages and investments.
Work Request Management System	Used for managing requests for information technology products and services.

Term	Definition
Worm	A type of malicious software program whose primary function is to infect other computers while remaining active on infected systems. Self-replicating malware duplicates itself to spread to uninfected computers. It often uses parts of an operating system that are automatic and invisible to the user.