TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the Internal Revenue Service's Information Technology Program for Fiscal Year 2020

October 30, 2020

Reference Number: 2021-20-001

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

HIGHLIGHTS: Annual Assessment of the Internal Revenue Service's Information Technology Program for Fiscal Year 2020

Final Audit Report issued on October 30, 2020
Reference Number 2021-20-001

Why TIGTA Did This 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 information technology of the IRS.

Impact on Taxpayers

In Fiscal Year 2019, the IRS collected approximately $3.6 trillion in Federal tax payments, processed approximately 253 million tax returns and supplemental documents, and paid approximately $452 billion in refunds to taxpayers. In addition, the IRS employs approximately 78,000 people in its Washington, D.C., headquarters and 519 offices in all 50 States and U.S. territories. The IRS relies extensively on computerized systems to support its financial and mission-related operations. Weaknesses within the IRS's computer operations could begin to adversely affect its ability to meet its mission of helping taxpayers comply with their tax responsibilities and enforcing the tax laws with integrity and fairness to all.

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* function areas as "effective." However, taxpayer data could be 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, access controls, system environment security, and separation of duties as well as security policies, procedures, and documentation.

In our reviews of systems development and information technology operations, TIGTA found that, generally, the IRS is effectively monitoring the progress of the Individual Tax Processing Engine project and incorporated Government Accountability Office best practices to estimate the duration of the project and velocity rate.

However, TIGTA found that the IRS lacks an enterprise-wide definition of a legacy system or specific individual plans to identify, manage, or modernize all of its legacy systems. Problems were also reported with the IRS's information technology acquisitions, asset management, governance and project management, cost management, data management, risk management, implementation of corrective actions, and modernizing operations.

What TIGTA Recommended

Because this report was an assessment of the adequacy and security of the IRS's information technology based on TIGTA and Government Accountability Office reports issued during Fiscal Year 2020, TIGTA did not make any further recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

October 30, 2020

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 2020 (Audit # 202020023)

This report presents the results of our assessment of the adequacy and security of the information technology of the Internal Revenue Service (IRS). This review is required by the IRS Restructuring and Reform Act of 1998.[1] This audit was included in our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenges of *Security Over Taxpayer Data and Protection of IRS Resources*, *Modernizing IRS Operations*, *Improving Tax Reporting and Payment Compliance*, and *Achieving Operational Efficiencies*.

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

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

Table of Contents

Background ..... Page 1

Results of Review ..... Page 5

System Security and Privacy of Taxpayer Data ..... Page 5

Systems Development and Information Technology Operations ..... Page 33

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 67

Appendix II – List of Treasury Inspector General for Tax Administration and Government Accountability Office Reports Reviewed ..... Page 68

Appendix III – Glossary of Terms ..... Page 70

Appendix IV – Abbreviations ..... Page 80

Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998[1] requires the Treasury Inspector General for Tax Administration (TIGTA) to annually assess and report on an evaluation of the adequacy and security of the IRS's information technology. TIGTA's Security and Information Technology Services business unit assesses the information technology of the IRS by evaluating cybersecurity, systems development, and information technology operations. This report provides our assessment for Fiscal Year 2020.[2]

The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In Fiscal Year 2019, the IRS collected approximately $3.6 trillion in Federal tax payments, processed approximately 253 million tax returns and supplemental documents, and paid approximately $452 billion in refunds to taxpayers.

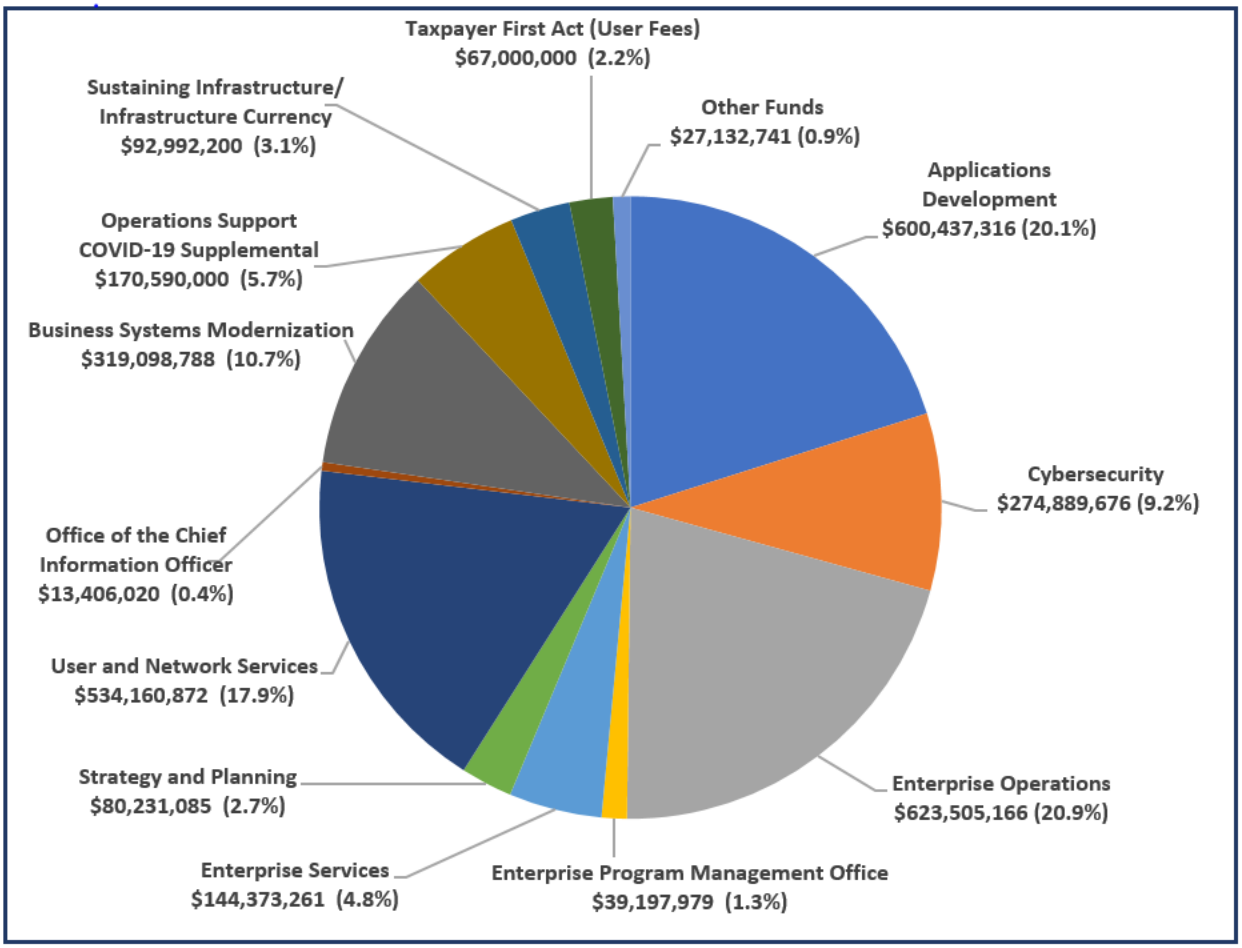
The IRS collected approximately $3.6 trillion in Federal tax payments and paid approximately $452 billion in refunds to taxpayers.

Further, the size and complexity of the IRS add unique operational challenges. The IRS employs approximately 78,000 people in its Washington, D.C., headquarters and 519 offices in all 50 States and U.S. territories. 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 as well as 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 2020, the IRS's appropriations increased by $200 million to $11.5 billion, designated for taxpayer services, enforcement, operations support, and modernization. The Information Technology (IT) organization comprises a significant portion of the IRS's budget and plays a critical role to enable the IRS to carry out its mission and responsibilities. The IRS's Fiscal Year 2020 projected available funds included approximately $3 billion for information technology investments, representing 26.1 percent of the total IRS budget, down from approximately $3.1 billion in Fiscal Year 2019. Figure 1 illustrates the IRS's Fiscal Year 2020 information technology funding by IT organization function and major program.

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

Figure 1: Fiscal Year 2020 Information Technology Funding by IT Organization Function and Major Program[3]

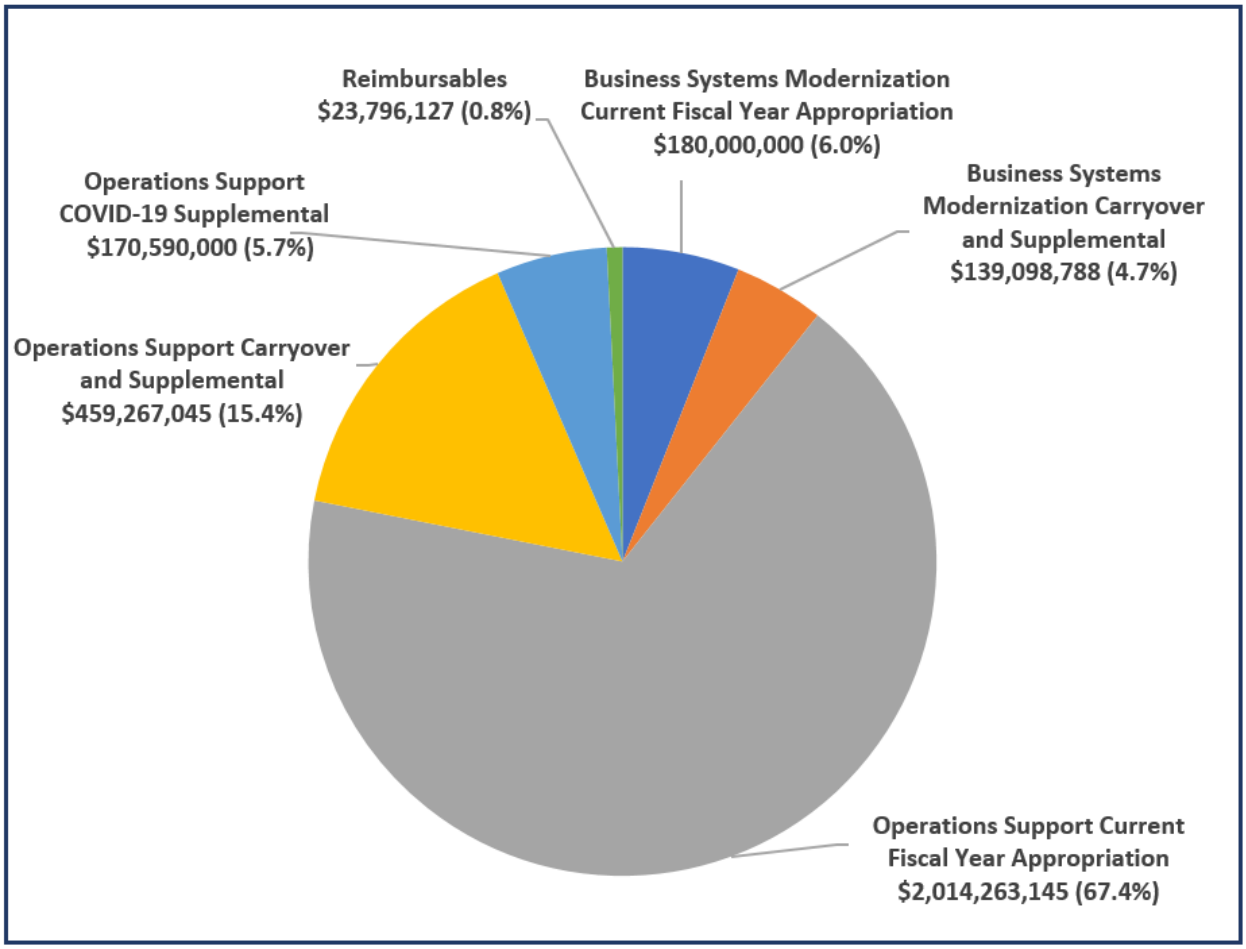


Source: IT organization budget data as of May 2020, based on information provided by the Strategy and Planning function's Office of Financial Management Services. The Other Funds category includes Shared Support and multiyear funds.

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

Figure 2 shows the IT organization funding for Fiscal Year 2020 by funding source.

Figure 2: Fiscal Year 2020 Total Available Funding by Funding Source[4]



Source: IT organization budget data as of May 2020, based on information provided by the Strategy and Planning function's Office of Financial Management Services.

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

Figure 3 illustrates that, as of May 2020, the IRS had a total of 7,237 employees and 6,113 contractors working across eight different IT organization functions—141 more employees and 245 more contractors than in Fiscal Year 2019.

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

IT Organization Function/Office	Employees	Contractors
Applications Development	1,972	1,941
Enterprise Operations	1,956	528
User and Network Services	1,447	881
Enterprise Services	749	983
Cybersecurity	542	671
Strategy and Planning	323	186
Enterprise Program Management Office	232	891
Office of the Chief Information Officer	16	32
Total	**7,237**	**6,113**

Source: IRS Human Resources Reporting Center as of May 2020.

- The **Applications Development function** is responsible for building, testing, delivering, and maintaining integrated information applications systems, or software solutions, to support modernized systems and the production environment.
- The **Enterprise Operations function** provides computing (server and mainframe) services for all IRS business entities and taxpayers.
- The **User and Network Services function** supplies and maintains all deskside (including telephone) technology, provides workstation software standardization and security management, inventories data processing equipment, performs 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.
- The **Enterprise Services function** architects, designs, introduces, and tests enterprise solutions in alignment with strategic direction and the needs of internal and external customers in the tax ecosystem.
- The **Cybersecurity function** 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.
- The **Strategy and Planning function** 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.

- The **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 Chief Information Officer** includes the Chief Information Officer (CIO), three Deputy CIOs, and their employees. Deputy CIOs serve as principal advisors to the CIO and provide executive direction and focus to help the IT organization increase its effectiveness in delivering information technology services and solutions that align to the IRS's business priorities.

Results of Review

During this annual review, we summarize information from program efforts in information technology security, systems development, and operations as required by the IRS Restructuring and Reform Act of 1998. During Fiscal Year 2020, TIGTA audits of the information technology program addressed the IRS major management and performance challenges of *Security Over Taxpayer Data and Protection of IRS Resources*, *Modernizing IRS Operations*, *Improving Tax Reporting and Payment Compliance*, and *Achieving Operational Efficiencies*. This report presents a summary of TIGTA and Government Accountability Office (GAO) audit results previously reported for Fiscal Year 2020. It does not reflect any additional audit work or corrective actions that may have been taken by the IRS since the initial reporting of the audit results.

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. While the IRS has made progress in many information technology areas, additional improvements are needed. Otherwise, weaknesses within the IRS's computer operations could begin to adversely affect its ability to meet its mission of helping taxpayers comply with their tax responsibilities and enforcing the tax laws with integrity and fairness to all.

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 activities 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. Therefore, 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 effect on a broad array of Government operations and assets.

Without effective security controls, computer systems are vulnerable to human errors or actions committed 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 2020, TIGTA designated *Security Over Taxpayer Data and Protection of IRS Resources* as the number one major management and performance challenge area for the tenth 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 (FISMA)[5] report that provides an overall assessment of the information security program, we performed several audits to assess the IRS's efforts to protect its information and taxpayer data. Our audits covered privacy of taxpayer data, access controls, system environment security, and separation of duties as well as security policies, procedures, and documentation.

Overall assessment of the information security program

The FISMA requires Federal agencies to develop, document, and implement an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by contractors. It assigns specific responsibilities to agency heads and Inspectors General in complying with FISMA requirements. It also directs Federal agencies to report annually to the Director of the Office of Management and Budget, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with the FISMA. In addition, the FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to the Office of Management and Budget. The FISMA states that the independent evaluation is to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.

The *Fiscal Year 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*[6] were developed as a collaborative effort among the Office of Management and Budget, 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 2020 metrics represent a continuation of the work that began in Fiscal Year 2016 to align the Inspector General metrics with the five Cybersecurity Framework 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*).[7] Figure 4 shows the five *Cybersecurity Framework* function areas and alignment with each of the associated security program components (or metric domains).

[5] Pub. L. No. 113-283, 128 Stat. 3703. This Act amends chapter 35 of title 44 of the U.S.C. to provide for reform to Federal information security.
[6] Version 4.0, dated April 17, 2020.
[7] Version 1.1, dated April 16, 2018.

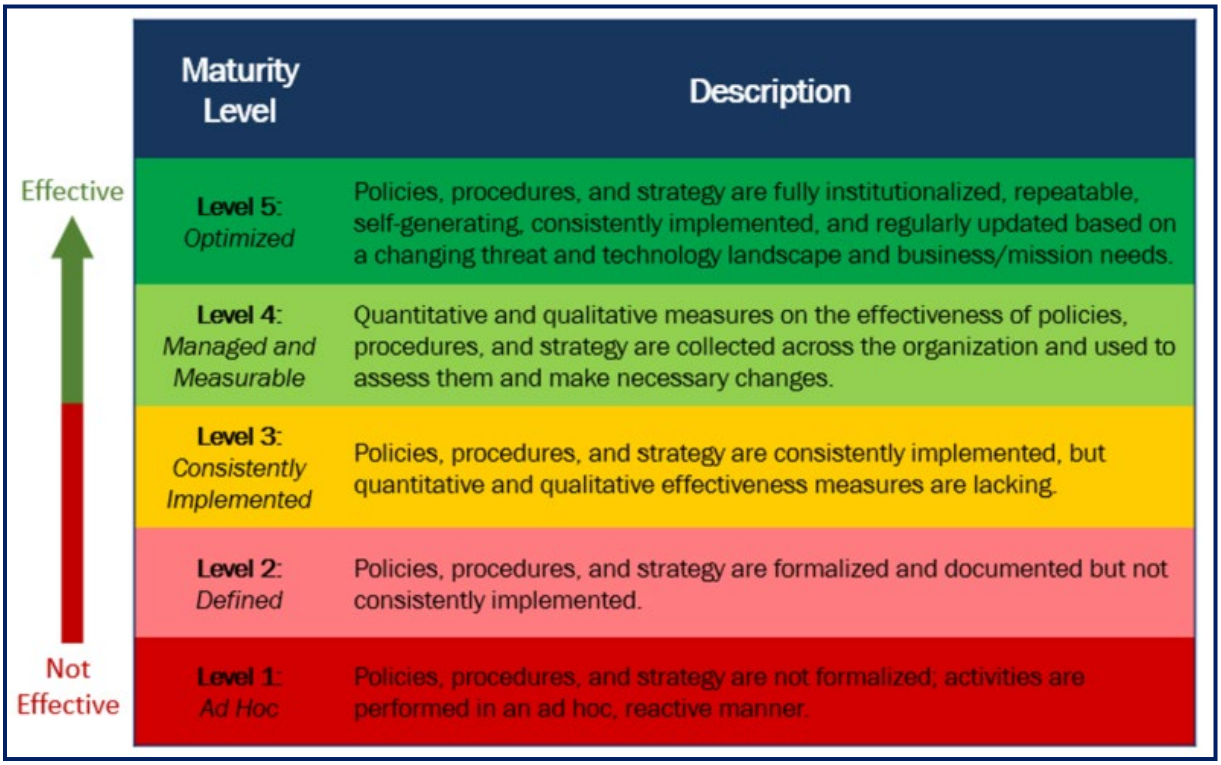
Figure 4: Alignment of NIST Cybersecurity Framework Function Areas to the Fiscal Year 2020 Inspector General FISMA Metric Domains

Cybersecurity Framework Function Area	Cybersecurity Function Objective	Fiscal Year 2020 Inspector General FISMA Metric Domains
IDENTIFY	Develop the organizational understanding to manage cybersecurity risk to systems, assets, and capabilities.	Risk Management
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical services.	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Information Security Continuous Monitoring
RESPOND	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Incident Response
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.	Contingency Planning

Source: Fiscal Year 2020 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 in which the metric domains ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institute those policies and procedures. Figure 5 details the five maturity model levels: *Ad Hoc*, *Defined*, *Consistently Implemented*, *Managed and Measurable*, and *Optimized*. The scoring methodology defines "effective" as being at a Maturity Level 4, *Managed and Measurable*, or above.

Figure 5: Inspectors General Assessment Maturity Model Spectrum



Source: Fiscal Year 2020 Inspector General FISMA Reporting Metrics.

To determine the effectiveness of the cybersecurity program, we evaluated[8] the maturity level of the program metrics specified in the *Fiscal Year 2020 Inspector General FISMA Reporting Metrics*. Along with our review of pertinent documents and discussions with IRS subject matter experts, we based our evaluation on a representative subset of seven information systems and the implementation status of key security controls as well as considered the results of other TIGTA and GAO audits. These audits, for which results were applicable to the FISMA metrics, were performed, completed, or contained recommendations that were still open during the FISMA evaluation period of July 1, 2019, to June 30, 2020. As shown in Figure 6, TIGTA rated three *Cybersecurity Framework* function areas as "effective" and two as "not effective."

[8] TIGTA, Ref. No. 2020-20-073, *Fiscal Year 2020 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act* (Sept. 2020).

Figure 6: Maturity Levels by Function Area

Function Areas and Metric Domains	Assessed Maturity Level	Effectiveness
1. IDENTIFY – Risk Management	Consistently Implemented (Level 3)	✗
2. PROTECT – Overall	Managed and Measurable (Level 4)	✓
2a. Configuration Management	Defined (Level 2)	
2b. Identity and Access Management	Consistently Implemented (Level 3)	
2c. Data Protection and Privacy	Managed and Measurable (Level 4)	
2d. Security Training	Managed and Measurable (Level 4)	
3. DETECT – ISCM	Consistently Implemented (Level 3)	✗
4. RESPOND – Incident Response	Managed and Measurable (Level 4)	✓
5. RECOVER – Contingency Planning	Managed and Measurable (Level 4)	✓

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

We found that three *Cybersecurity Framework* function areas, *i.e.*, PROTECT, RESPOND, and RECOVER, and their four security program components, *i.e.*, Data Protection and Privacy, Security Training, Incident Response, and Contingency Planning, respectively, were at *Managed and Measurable* (Maturity Level 4) and therefore were deemed as "effective." We also found that two of the security program components, *i.e.*, Configuration Management and Identity and Access Management for the function area PROTECT, and the remaining two function areas, *i.e.*, IDENTIFY and DETECT, were deemed as "not effective." Based on the *Fiscal Year 2020 Inspector General FISMA Reporting Metrics*, we found the following.

The security program components of Configuration Management and Identity and Access Management

The security program components for the *Cybersecurity Framework* function area of PROTECT were all deemed as "effective," except Configuration Management and Identity and Access Management, which were at *Defined* (Maturity Level 2) and *Consistently Implemented* (Maturity Level 3), respectively. While the overall function area PROTECT is at an effective level, the following are examples of Configuration Management and Identity and Access Management metrics that did not meet the *Managed and Measurable* maturity level.

Configuration Management

- While the IRS has defined policies and procedures for managing the configurations of its information systems, it has not consistently implemented its policies and procedures.

- While the IRS has defined common secure configurations, it has not ensured that its information systems consistently maintain secure configuration settings in compliance with IRS policy.
- While the IRS has defined flaw remediation policies, including patching, it has not consistently implemented flaw remediation and patching on a timely basis.

Identity and Access Management

- While the IRS reported that 100 percent of its privileged users are required to use personal identity verification cards to access the network, it reported that only 79 (59 percent) of the 134 internal systems are configured to require personal identity verification cards. In addition, TIGTA and the GAO reported authentication weaknesses.
- While the IRS has defined its processes for provisioning, managing, and reviewing privileged accounts, the IRS has not consistently implemented controls related to privileged account management. Both TIGTA and the GAO reported control deficiencies that included unnecessary access rights granted to accounts, lack of segregation of duties, and inconsistent monitoring of systems and accounts.

The *Cybersecurity Framework* function areas of IDENTIFY and DETECT

We found that the *Cybersecurity Framework* function areas of IDENTIFY and DETECT and their respective security program components, Risk Management and Information Security Continuous Monitoring, met a *Consistently Implemented* (Maturity Level 3), which was deemed as "not effective." The following are examples of metrics that did not meet the *Managed and Measurable* maturity level.

- To address deficiencies on accurately accounting for its hardware inventory, the IRS completed an Information Technology Asset Management program proof of concept that produced a dashboard to identify and resolve differences on the inventory of hardware assets. This tool will also play a key role in maintaining information on software assets. However, this solution will not be fully implemented until Fiscal Year 2021. In addition, TIGTA found that the IRS has a Plan of Action and Milestones (POA&M) that documents open hardware and software inventory weaknesses.
- The IRS has developed the Information Security Continuous Monitoring strategy, but the strategy did not include vulnerability scanning [redacted].

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

Privacy of taxpayer data

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. The proliferation of stolen Personally Identifiable Information poses a significant threat to tax administration by making it difficult for the IRS to distinguish legitimate taxpayers from fraudsters. Tax-related scams, and the methods used to perpetrate them, are continually changing and require constant

monitoring by the IRS. The IRS's ability to continuously monitor and improve its approach to taxpayer authentication is a critical step in defending the agency against evolving cyberthreats and fraud schemes and in protecting billions of taxpayer dollars.

During Fiscal Year 2020, TIGTA performed two audits involving privacy of taxpayer data. We initiated an audit[9] to assess the adequacy of and adherence to the IRS's volunteer site requirements to safeguard and protect sensitive taxpayer information. The Volunteer program provides no-cost Federal tax return preparation and electronic filing to underserved segments of individual taxpayers, including low-income to moderate-income, elderly, disabled, and limited English-proficient taxpayers. The Volunteer program includes the Volunteer Income Tax Assistance and the Tax Counseling for the Elderly programs and sites operated in partnership with the U.S. military and community-based organizations.[10] We found that the IRS's Stakeholder Partnerships, Education, and Communication function, responsible for the Volunteer program, worked with its partners to heighten data security awareness at 10,921 volunteer sites with 82,214 volunteers preparing 3,458,737 tax returns[11] during Fiscal Year 2019. Heightened data security awareness guidance related to information technology included the following.

- Publication 4299, *Privacy, Confidentiality, and Civil Rights*,[12] outlines volunteer site requirements to protect taxpayer information: Publication 4299 provides requirements, *e.g.*, specifications on use of wireless devices, not sharing tax information without a need to know, and reporting lost or stolen computers, that volunteers must follow to protect taxpayer information. Volunteer sites are required to maintain a copy of the publication for reference.
- Procedures for identifying lost or stolen computers: Volunteers are required to notify the IRS within 48 hours for lost or stolen IRS-owned computers and are requested to notify the IRS within 48 hours for lost or stolen partner-owned computers. For stolen IRS-owned computers, volunteers must also notify local law enforcement immediately. In addition, volunteer sites are required to evaluate the risk associated with any loss of taxpayer information and, if warranted, notify the taxpayers.

However, improvements are needed to strengthen data security processes. During February and March 2019, we performed unannounced visits to 20 judgmentally[13] selected volunteer sites and identified multiple security weaknesses at each site. These sites were also visited by Stakeholder Partnerships, Education, and Communication function reviewers in Calendar Year 2018, who concluded that these sites were fully compliant with the security requirements. Examples of the security weaknesses we identified include:

- IRS policies and procedures do not restrict volunteer access to tax information after returns are prepared. Our review identified that all volunteers who prepare returns at a site have the capability to [redacted]. The tax preparation software used by volunteer sites has a

[9] TIGTA, Ref. No. 2020-40-004, *Actions Are Needed to Improve the Safeguarding of Taxpayer Information at Volunteer Program Sites* (Nov. 2019).
[10] Community-based organizations may include colleges, senior citizen centers, faith-based organizations, and libraries.
[11] As of April 28, 2019.
[12] Revision September 2018.
[13] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

security feature that would restrict volunteer access to prepared returns, [redacted].

- Site coordinators are unaware of security requirements in Publication 4299. Site coordinators at 16 locations indicated that they were unaware of Publication 4299. The Stakeholder Partnerships, Education, and Communication function's site reviews do not determine whether site coordinators are familiar with the security requirements and whether a copy of Publication 4299 is available to review.
- Sites using wireless connections to transmit taxpayer information did not complete the required risk assessment. Wireless connections to the Internet to prepare and transmit tax returns were used at 11 of the 20 sites visited. However, for the 11 sites, the partners did not complete the risk assessment as required. [redacted].

In addition, improvements are needed to better protect taxpayers from potential identity theft. Specifically, volunteer sites are not complying with procedures when computers are lost or stolen. Our review identified that the required Form 13747, *Checklist for Lost/Stolen Equipment*, was not prepared for five of 36 IRS-owned computers reported lost or stolen in Calendar Years 2016 through 2018. In addition, our review of the 19 Forms 13747 that were prepared for the remaining 31 lost or stolen computers identified that the forms lacked information the Stakeholder Partnerships, Education, and Communication function needed to evaluate these incidents. For example, all 19 forms had missing checklist items or a vague explanation of the incident. Information missing included details on whether a police report was filed and whether sensitive data were stored on the computer. Despite this missing information, the Stakeholder Partnerships, Education, and Communication function concluded that none of the computers stored taxpayer information and no taxpayers needed to be notified. When security weaknesses exist at the volunteer sites, taxpayers' personal information is more susceptible to theft and misuse.

We also initiated an audit[14] to evaluate the effectiveness of security controls and procedures over wireless networks in use at IRS facilities and the preventative measures against unauthorized wireless access points. We found that wireless broadcast signals could be better controlled. We tested the wireless access point broadcast signal strength and determined that the wireless signals extended well beyond the IRS-controlled space in 21 (75 percent) of the 28 locations visited. For example, in one location, we detected the wireless signal from one wireless access point in a loading dock several floors away from the IRS space. In other locations, we detected the wireless signal in public parking lots, outside the front door of the building that housed an IRS office, and outside of a building with an IRS office facing the street. However, we did not identify any signal boosting or enhanced wireless signal devices at any of the locations we visited.

When we asked the IRS what evaluations were performed regarding the ranges of the access points, User and Network Services function management stated that when the IRS initially deployed the wireless networks, it did not reduce the access point signal strength. In addition, User and Network Services function management stated that the IRS is in the process of reducing the signal strength to limit the range and is preparing to replace a significant number of its access points. As a part of this equipment refresh, the User and Network Services function

[14] TIGTA, Ref. No. 2020-20-063, *Improvements Are Needed to Ensure That Wireless Networks Are Secure* (Sept. 2020).

plans to upload existing floor plans in a location and mapping feature to help determine the best access point locations. User and Network Services function management also provided, as an example, planning and design documents for two locations that included a heat coverage map to illustrate the intended coverage area and strength of the signal but still allow the user to access the wireless networks and perform work. By having the wireless network signal broadcasting beyond its controlled space, the IRS increases the risk that hackers might be able to intercept the wireless broadcast signal and hack into the IRS network.

In addition, while testing wireless access point broadcast signal strength at the 28 locations, we detected 90 multifunction printers broadcasting a wireless signal, violating IRS policies. These printers are not directly managed and secured by the wireless network team nor do the wireless networks control the wireless signals broadcasting from the printers. However, we believe they pose a security risk and should be addressed. Because the IRS was not the only occupant in many of the buildings and our scans captured limited information, *i.e.*, the name of the printer and the wireless network address for each device, we were unable to determine if all of the printers identified belonged to the IRS.

When discussing this issue with the IRS, User and Network Services function management acknowledged that there are IRS printers that broadcast a wireless signal. Other management thought that the multifunction printers in question might be primarily desktop types and do not have IRS network connections but are connected to the laptops through a cable. We agree that a printer broadcasting a wireless signal not connected to the network is a lower risk. However, we believe printers with wireless signals that are connected to an employee's computer are still an unnecessary risk, which creates potential for hackers to attempt to find their way into the IRS network through the printer. To be compliant with IRS requirements and to mitigate the potential risk, the IRS should disable and lock the wireless capability to prevent wireless broadcasting on all IRS printers.

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 access controls, *i.e.*, authorization, authentication and identity proofing, access management, and cryptography.

Physical security access controls

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. They include, among other things, policies and practices for the use of access cards and locks authorizing individuals' physical access to facilities and resources.

In Fiscal Year 2020, TIGTA initiated an audit[15] to evaluate the effectiveness and efficiency of the Integrated Submission and Remittance Processing (ISRP) Active Directory implementation. As part of this review, we performed site visits at six IRS locations to evaluate the physical security controls protecting the computer rooms housing ISRP domain controllers.[16] We evaluated the

[15] TIGTA, Ref. No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020).
[16] The ISRP supports seven IRS locations; however, only six locations housed ISRP Active Directory domain controllers.

physical security controls, including environmental protections, fire safety and suppression, temperature and humidity controls, emergency power sources, and shutoff switches as well as multifactor authentication. We found 15 physical security violations related to these controls.

- Fire safety and suppression (2 violations) – The fire extinguisher in the computer room at one location was not inspected on a monthly basis. In addition, while all six locations annually tested the automatic fire suppression systems, another location failed its most recent annual test because multiple devices from a previous system needed to be either removed or connected to the new system. The fire suppression system test report did not specify which of the two possible actions the IRS needs to complete to resolve the failure.
- Emergency power sources and shutoff (1 violation) – The emergency power shutoff switch in the computer room for one location was disabled by a large paper clip purposefully lodged behind it, not allowing the switch to be engaged, and was covered with a piece of paper.
- Limited Area access (6 violations) – We found six violations of the Limited Area access policies in three of the six locations visited. For example, personnel with access to the computer room at one location did not have personal identity verification cards with the required "R" indicator, which signifies an individual assigned to a Limited Area.[17] In addition, the computer rooms in two locations did not have Forms 5421, *Limited Area Register*, for visitors to sign. Further, when we reviewed the May 2019 *Authorized Access List* for the computer room at one of these two locations, there was no evidence that the list is reviewed monthly and updated. In another location, we also found that, while an ISRP domain controller is housed in a locked cabinet, it was located in an unlocked computer room that is part of a greater Limited Area for submission processing operations. Visitors and employees with access to the larger processing area also have uncontrolled access to the computer room.
- Multifactor authentication (6 violations) – Multifactor authentication has not been implemented, as required, for any of the Limited Area computer rooms in the six locations. Five of the six computer rooms containing ISRP domain controllers were accessed via card reader, which serves as a single authentication factor. The computer room at one location was not secured from employees who have access to the larger submission processing area.

Without adequate access controls, such as multifactor authentication, the IRS increases the risk of unauthorized individuals gaining access to information technology assets.

System security access controls

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

[17] The personal identity verification card is encoded with permission to access a Limited Area. The "R" on the card is a visual indicator showing an individual's assignment to a Limited Area.

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 2020, TIGTA and the GAO provided coverage on system authorization in three audits. TIGTA initiated an audit[18] to evaluate the effectiveness and efficiency of the IRS mainframe systems security and operations. We found that privileged, *i.e.*, system or network administrator, and service account access controls over the International Business Machines® (IBM) mainframe platform were working as intended.[19] Our review of the account access authorizations in the Online 5081 system determined that all system administrator and service accounts had the required approvals, including associated documentation, to access the IBM mainframe platform environment. We also reviewed the *Online 5081 Manager Guide*[20] and found that the updated guidance includes a field to ensure that expiration dates for non-IRS employees, *e.g.*, contractors, are used in the Online 5081 system. By providing adequate administrative oversight of system access controls, the IRS protects the security posture of the mainframe platform and helps prevent unauthorized system access.

In our active directory audit, we reviewed the Domain Admin group membership of the IRS's Microsoft® Active Directory. Domain Admin group membership should be required only in situations in which an account needs high levels of privilege. Our review for five production forests found, for example:

- Multiple instances in the Domain Admin groups in which more than one account appeared to belong to a single employee.
- Accounts that lack the administrative suffix to differentiate between a business role and a system or network administrative account.
- Business role accounts inappropriately assigned in the Domain Admin group.

By having multiple accounts belonging to a single user in the Domain Admin group, the IRS allows business role accounts to execute privileged functions. When elevated access is persistent or elevated privilege accounts use the same credentials to access multiple resources, a compromised account can result in a major breach. In addition, if an application that has too many privileges is compromised, the attacker might be able to expand the attack more so than if the application had been under the least amount of privileges possible.

[18] TIGTA, Ref. No. 2020-20-045, *Mainframe Computing Environment Security Needs Improvement* (Sept. 2020).
[19] The IRS employs two mainframe platforms – IBM and Unisys mainframe systems. We did not include the Unisys mainframe platform in the scope of this audit.
[20] Dated April 2019.

The GAO initiated an audit[21] 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. The GAO reported that the IRS did not update documentation supporting authorization and access for managing servers.

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.*, something an individual possesses and controls, such as a password, that is used to authenticate his or her identity.

In Fiscal Year 2020, TIGTA and the GAO performed four audits covering authentication and identity proofing. We initiated an audit[22] to evaluate the effectiveness of the IRS's efforts to deploy unified access controls to identify and authenticate valid user and device accesses to its internal network. As part of its Unified Access project, the IRS uses the Cisco Identity Services Engine (ISE) software product to authenticate users, *i.e.*, employees, contractors, and partners,[23] and devices accessing its internal network, regardless of the connection type, *i.e.*, through wired, wireless, or Virtual Private Network (VPN). The ISE is integrated with and queries Microsoft Active Directory to authenticate users and devices. The IRS Main Active Directory domain in the ISE for the most part refers to all IRS functions,[24] except Criminal Investigation.[25] As of December 31, 2019, the IRS has enforced the authentication of users and devices for all 507 sites used by the IRS Main Active Directory domain. Users authenticate using either their personal identity verification cards or passwords generated from grid cards.[26] Devices are authenticated using either the 802.1X protocol using certificates or passwords or the Media Access Control Authentication Bypass protocol before being granted network access.

[21] GAO, GAO-20-411R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (May 2020).
[22] TIGTA, Ref. No. 2020-20-036, *Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action Is Needed to Verify the Identity of Devices* (Aug. 2020).
[23] According to the IRS, its partners include the Department of Homeland Security, the GAO, TIGTA, and the Federal Emergency Management Agency.
[24] According to the IRS, 99.9 percent of the Chief Counsel domain users and devices have been migrated to the IRS Main Active Directory domain as of February 12, 2020.
[25] The IRS plans to enforce authentication of the Criminal Investigation domain users and devices by December 2020.
[26] Grid cards identify users by asking the user to input a series of characters based on a preregistered pattern that the user knows on a grid and a grid of pseudo-random characters generated by the authenticator.

We selected and reviewed a judgmental sample of one day, February 6, 2020, of activity from the ISE audit log. Figure 7 provides the summary results of our analysis of the successful user and device network accesses.

Figure 7: Summary of Successful User and Device Network Accesses Captured in the One Day Sample of ISE Audit Log Activities[27]

	Network Connection Method		
	Wired	**Wireless**	**VPN** [28]
Successful Network Accesses	104,910	4,999	26,237
Users accessing the network			
Authentication by Certificate	95%	100%	N/A[29]
Authentication by Password	5%	0%	N/A
Total	**100%**	**100%**	**N/A**
Devices accessing the network			
Authentication by Certificate	97%	5%	0%
Authentication by Password	3%	3%	0%
Not Authenticated	0%	92%	100%
Total	**100%**	**100%**	**100%**

Source: TIGTA's analysis of ISE audit log activities on February 6, 2020.

Our review also found that all devices connecting through a VPN and approximately 92 percent of the devices connecting wirelessly to the internal network daily were not authenticated. The User and Network Services function's Enterprise Remote Access program is responsible for managing VPN access to the internal network. In the ISE architecture, policy service nodes[30] do not make authentication decisions for VPN users, as this occurs independent of the ISE software by the AT&T managed service. Accordingly, Cisco adaptive security appliances managed by AT&T make the authentication decisions for VPN users, *i.e.*, allowing or denying VPN users internal network access. Devices connecting to the internal network through VPNs are not authenticated using either passwords or device certificates before being granted access.

According to the IRS, approximately 78,000 users are able to access its internal network. Of the total population of users, approximately 5,000 typically connect daily to the internal network using a wireless connection. Based on our review of one day of activity on the ISE audit log, certificate-based and password-based authentication was occurring on 5 percent and 3 percent,

[27] Authentication requests can include multiple requests from a single user or device.
[28] We did not review VPN transactions captured on the ISE audit log because AT&T authenticates VPN users. VPN transactions in the ISE audit log are actually authorization requests, not authentication requests. Authorization requests involve requesting privileges for a user, program, or process.
[29] The adaptive security appliances make authentication decisions for VPN users and pass the decisions to the ISE, where the ISE blocks user accesses as needed.
[30] A Cisco ISE node with the policy service persona that evaluates authentication policies and makes all authentication decisions.

respectively, of the devices connecting wirelessly. The remaining 92 percent of the devices connecting wirelessly to the internal network were not authenticated. By not properly authenticating all devices, the IRS does not have adequate controls to ensure that only authorized devices are allowed access to its internal network, and taxpayer data may be at risk.

In addition, our review of 30,131 rejected authentications[31] by error type concluded that the reasons for the failed authentications were reasonable. The vast majority of failed authentication requests require remediation by Enterprise Field Operations personnel at the remote IRS sites in the form of installing or updating software, correcting device certificates, or re-enabling disabled accounts in Active Directory. While our review did not identify any suspicious devices in the ISE audit log activities, the IRS provided evidence that, when the ISE engineers identify suspicious devices, they report them to the Cybersecurity function for resolution.

Further, our review found that there are approximately 91,000 Windows®-compatible desktops and laptops that connect to the IRS's internal network using wired, wireless, or VPN connections via the 802.1X protocol. However, there are additional devices, such as wireless controllers, physical security devices, and select servers that are whitelisted in the ISE to allow the devices to authenticate using the Media Access Control Authentication Bypass protocol.

Unlike the 802.1X protocol, the Media Access Control Authentication Bypass protocol is not a strong authentication protocol because its authentication is vulnerable to spoofing attacks. A spoofing attack occurs when an intruder captures network traffic, intercepts the media access control addresses, and attempts to impersonate or act as one of the valid media access control addresses. Through spoofing attacks, invalid devices could access the internal network.

We also initiated an audit[32] to evaluate the IRS's identity proofing capabilities for secure electronic authentication to online applications. We found that the Digital Identity Risk Assessment (DIRA) process[33] is generally in compliance with NIST Special Publication 800-63-3, *Digital Identity Guidelines*,[34] but more work is needed to fully and timely meet current standards for remote and physical identity proofing for the IRS's 63 public-facing applications.[35]

Our review of the DIRA process identified concerns with the IRS's ability to provide compensating controls when the complete set of applicable requirements are not implemented. The IRS's compensating controls include the NIST level of assurance 2 and 3 workflow process for identity proofing and authentication based on superseded NIST Special Publication 800-63-2, *Electronic Authentication Guideline*,[36] guidelines. For the level of assurance 3 workflow process, the IRS uses four separate steps that collect and confirm distinct sets of information. Users must confirm their identity at each step before the IRS grants access

[31] There were an additional 248,713 Media Access Control Authentication Bypass protocol authentication failures captured in the ISE audit log that we did not review. According to the IRS, network adapters initializing on Windows-compatible devices before the Windows operating system was ready to login caused these authentication failures. Because the device certificates were not initially available while the Windows-compatible devices were powering up, this forced them to attempt authentication through the Media Access Control Authentication Bypass protocol. The ISE authentication failed due to the Windows-compatible devices not being in the whitelisted group.
[32] TIGTA, Ref. No. 2020-20-012, *While Progress Is Being Made on Digital Identity Requirements, Completion Dates to Achieve Compliance With Identity Proofing Standards Have Not Been Established* (Mar. 2020).
[33] The DIRA process consist of six steps: Step 1, Data Collection; Step 2, Analysis; Step 3, Review; Step 4, Implementation Determination; Step 5, Oversight; and Step 6, Ongoing Assessment.
[34] Dated June 2017.
[35] The IRS identified 64 public-facing applications; however, only 63 were scheduled for the DIRA process to date.
[36] Dated August 2013.

to its online services. This multistep approach provides the IRS with assurance of the taxpayer's identity.

- [redacted].
- [redacted].
- [redacted].
- [redacted].

[redacted]. However, neither the level of assurance 2 nor 3 workflow process are comparable to NIST Special Publication 800-63-3 requirements, which introduced the need for either remote or physical presence for identity proofing. NIST Special Publication 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*,[37] identity assurance level 2 requires that evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. It also requires remote or physically present identity proofing. Identity assurance level 3 requires the physical presence for identity proofing and that identifying attributes be verified by an authorized and trained Credential Service Provider (CSP) representative.[38] The IRS acknowledged that the workflow processes did not fully meet standards but stated that they are the most secure methods currently available to remotely identity proof and authenticate taxpayers. The IRS is developing a digital identity solution, which it planned to pilot in June 2020.

In addition, much of the information the IRS uses to provide assurance of the taxpayers' identities may have been stolen in the last four calendar years. For example, in Calendar Year 2015, the Office of Personnel Management and its interagency response team concluded that sensitive information, *e.g.*, full name, birth date, home address, and Social Security Number, for approximately 22 million individuals was stolen from its systems. In September 2017, the credit reporting bureau Equifax® announced that personal data including individuals' names, birth dates, Social Security Numbers, and in some cases, driver's license numbers had been stolen. A subsequent investigation determined the breach affected approximately 148 million individuals.

We also initiated an audit[39] to evaluate the IRS's controls to authenticate third-party authorization requests to access taxpayer data. We found that the IRS has not made sufficient progress developing an online third-party authorization tool to verify and accept taxpayers'

[37] Dated June 2017.

[38] For identity assurance level 1, there is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted, which are neither validated nor verified.

[39] TIGTA, Ref. No. 2020-40-067, *Improvements Are Needed to Address Continued Deficiencies in Ensuring the Accuracy of the Centralized Authorization File* (Sept. 2020).

electronic signatures on Forms 2848, *Power of Attorney and Declaration of Representative*, and Forms 8821, *Tax Information Authorization*. In addition, the IRS did not meet the Taxpayer First Act[40] deadline of January 1, 2020, to publish guidance on standards for verifying taxpayers' electronic signatures. On December 3, 2019, the IRS published internal guidelines on its public website to provide form owners with procedures to implement electronic signature methods for their respective forms. However, the guidelines do not provide standards for electronic signatures on Forms 2848 and 8821.

Wage and Investment Division's Customer Account Services function management stated that the IRS is planning to develop a system called "Tax Pro Account." The goal of this system is to strengthen security over the process for representatives to access taxpayers' account information. Specifically, the system will provide a secure online self-service portal for tax professionals with a complementary interface to the Online Account application, which provides taxpayer account information, such as balance due amount and payment history. The Tax Pro Account system will meet the requirements of the Taxpayer First Act and is consistent with the IRS's new electronic signature guidelines. However, IT organization management stated that analysis of business and security requirements for the Tax Pro Account system is not yet complete.

The IRS is several years away from deploying the Tax Pro Account system, and an alternate solution is needed to verify taxpayers' electronic signatures. Based on the *IRS Integrated Modernization Business Plan*,[41] the target delivery dates for Forms 2848 and 8821 in the Tax Pro Account system are the third quarter of Fiscal Year 2022 and the second quarter of Fiscal Year 2023, respectively. Web application development for the Tax Pro Account system was scheduled to begin in the third quarter of Fiscal Year 2020. However, funding was not allocated, which will lead to further delays. These delays and other concerns raised by officials in the National Association of Enrolled Agents, an organization that represents tax professionals who help taxpayers meet their tax obligations, warrant an alternate solution for verifying taxpayers' electronic signatures on Forms 2848 and 8821. This alternate solution can be used until the Tax Pro Account system is deployed. It can also be used to verify taxpayers' electronic signatures after the system is deployed because a significant number of taxpayers and their representatives will not use the Tax Pro Account system. Officials from the National Association of Enrolled Agents stated that many taxpayers and their representatives would be unable to pass the Tax Pro Account system's multifactor authentication process. However, the IRS has not made sufficient progress developing an alternate solution for accepting taxpayers' electronic signatures.

Identity Assurance function management stated that the IT organization is considering alternate solutions to verify taxpayers' electronic signatures on IRS forms. However, IT organization management stated that they have no estimated time frame for developing an alternate process because they are still attempting to understand the business requirements for verifying taxpayers' electronic signatures. Understanding the business requirements of a new system is a crucial first step in designing the system because business requirements describe the characteristics of the new proposed system from the viewpoint of the system's end users.

[40] Pub. L. No. 116-25.
[41] Dated April 2019.

In its audit of the IRS's information system security controls, the GAO reported that it found two deficiencies related to authentication. The IRS did not:

- Restrict employees from adding certificates that the Department of the Treasury (hereafter referred to as the Treasury Department) had not approved to the Adobe Acrobat Trusted Identities list.
- Use multifactor authentication for accessing a certain information system.

Access management

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

In Fiscal Year 2020, TIGTA performed two audits covering access management. In our active directory audit, we found that the ISRP Active Directory forest settings governing account password and lockout policies were generally compliant with current Internal Revenue Manual 10.8.1, *Information Technology (IT) Security – Policy and Guidance*,[42] requirements. However, we found one area of deviation from Internal Revenue Manual policies but determined that the effect is minimal. The manual also requires information systems to enforce password minimum and maximum lifetime restrictions. Business role accounts must be disabled, quarantined, or removed after a prescribed number of days of inactivity. Figure 8 shows the 16,192 service and business role account policy violations we found in the ISRP Active Directory forests.

Figure 8: Summary of Account Policy Violations

Policy Violations	Number of Violations
Enabled service account passwords set to not expire.	51
Enabled business role accounts that have passwords set to never expire.	2,016
Enabled business role accounts are not required to use personal identity verification card.	2,648
Enabled business role accounts have not reset passwords in 90 days.	2,194
Enabled business role accounts are not properly disabled.	1,729
Business role accounts are not properly placed in quarantine.	2,400
Business role accounts are not properly removed.	5,154
Total Policy Violations	**16,192**

Source: TIGTA's analysis of information collected from the Users and Computers feature within the active directory using PowerShell®.

[42] Dated May 9, 2019.

Attackers frequently discover and exploit legitimate but inactive business role accounts to impersonate legitimate users, making discovery of attacker behavior difficult for network monitoring tools to identify. Terminated contractor and employee accounts have often been misused in this way. This potentially places IRS data at risk for loss, manipulation, and other unauthorized access.

In our audit of controls to authenticate third-party authorization requests, we found that some employees have unneeded access privileges to the Centralized Authorization File. Our review of 672 employees,[43] who have Centralized Authorization File access privileges that allow them to change or add taxpayer authorizations, identified 364 (54 percent) employees who were not assigned to the Centralized Authorization File unit as of March 12, 2020. Further analysis of the 364 employees identified 115 who initiated actions to modify one or more Centralized Authorization File authorizations between January 2, 2020, and February 29, 2020. IRS records indicate that some of these employees have jobs such as mail clerk, file supervisor, facilities management and security assistant, or computer assistant, which do not require them to change or add taxpayer authorizations to the Centralized Authorization File.

Centralized Authorization File management stated that, of the 364 employees, 293 were granted access privileges in November 2019 because they were needed to help process aged Centralized Authorization File authorizations and 63 were granted access privileges because their jobs require them to perform research or programming relative to the Centralized Authorization File. For the remaining eight employees, Centralized Authorization File management stated that they are unable to confirm why access privileges were granted because the employees are not in the office due to the coronavirus pandemic.

Cryptography

Cryptography, *i.e.*, encryption, 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. The information cannot be read without a key to decrypt it.

In Fiscal Year 2020, the GAO performed an audit covering cryptography. In its audit of the IRS's information system security controls, the GAO reported that it found two deficiencies related to cryptography. The IRS did not:

- Implement cryptographic mechanisms to secure certain data in a system environment that processes taxpayer data.
- Enforce the use of encryption algorithms compliant with NIST, Federal Information Processing Standards 140-2, *Security Requirements for Cryptographic Modules*,[44] for certain operating systems.

System environment security

Management of the system security environment provides organizations the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the

[43] The list of employees resulted from an IRS match between monthly Integrated Data Retrieval System Security Profile Report data for employees with Centralized Authorization File access privileges and employee personnel data.
[44] Dated May 2001.

environments in which those systems operate. It also contributes to information systems that are more resilient to cyberattacks and other threats. Security controls include, but are not limited to, system configuration management; system scanning, vulnerability remediation, and patching; and audit logs.

System configuration 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.

During Fiscal Year 2020, TIGTA and the GAO each performed an audit of system configuration management controls. In our active directory audit, we found that the ISRP Active Directory lacks necessary logical security controls, specifically domain controller configuration compliance. Our review of Windows Policy Checker scans and reports found that all domain controllers had an average score of 83.25 percent but failed due to high-risk checks. According to the *Windows Policy Checker User Manual*, regardless of the calculated compliance percentage, any computer that fails for high-risk checks will be classified as noncompliant, presenting a serious risk. We also found that the Windows Policy Checker itself is out of date. The IRS's current version of Windows Policy Checker was released in December 2014. It uses Security Technical Implementation Guidelines set by the Defense Information Systems Agency that are more than five years old. The most current Security Technical Implementation Guidelines for active directory domain controllers were released in February 2019.

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

- Implement mandatory access control policies for Linux® servers supporting certain applications.
- Consistently install patches to a Windows server supporting a certain application.
- Consistently install patches to a hypervisor to support server virtualization across the IRS environment.

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 errors 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 2020, TIGTA performed three audits involving system scanning and vulnerability patching of IRS systems. TIGTA initiated an audit[45] to determine the effectiveness and efficiency of the Continuous Diagnostics and Mitigation (CDM) project implementation. We found that, while the IRS is using CDM project sensor tools to identify and report data on its information technology assets, the reported data are incomplete and require quality improvement. In a September 27, 2019, briefing to Cybersecurity function management, the project team reported[46] that six of nine metrics reported were categorized as below acceptable quality. These metrics identified missing device data from the endpoint management and the asset detection sensor tools. The other metrics stated that the total device counts were inaccurate and vulnerable devices were missing.

The IRS is in the process of implementing an upgrade to the endpoint management tool that communicates with the tool that transmits data to the Treasury Department dashboard. The tool upgrade will provide increased functionality and performance for the delivery of hardware, software, and configuration management settings information on devices with the sensor tool endpoints. According to the IRS, the endpoint management sensor tool has been implemented in five of the six segmented networks. The remaining network segment for the Research Applied Analytics and Statistics, Statistics of Income, is approximately 18.3 percent completed. The CDM project data for the segmented networks will be incomplete until full deployment of the tool, which was rescheduled for May 1, 2020, to avoid risk to the filing season operations. In addition, due to technical difficulties with segmented networks' firewalls and ports, the asset detection sensor tool is unable to capture all the detailed information of each endpoint in the segmented networks. CDM project management estimates that the asset detection sensor tool covers approximately 80 to 90 percent of information technology assets on the IRS network. Incomplete data and insufficient data quality can adversely affect decisions related to cybersecurity risks. Management needs accurate information to prioritize and minimize risks based on potential affects.

In our active directory audit, we found that the ISRP Active Directory lacks necessary logical security controls, specifically in vulnerability scanning and protection from malicious code. The IRS provided two vulnerability scan reports for all 11 ISRP domain controllers with a credential scan date of May 30, 2019. The scans were performed using an administrator-level credential, which provides significant advantages, *e.g.*, more information on what is running on the hosts leading to testing for more vulnerabilities, and more accurate scans with a lower false positive rate. Our review of the first vulnerability scan report found that the IRS was not performing monthly credentialed vulnerability scans. Specifically, we found that the IRS did not perform credentialed vulnerability scans on six domain controllers since January 2018, two domain controllers since November 2018, and the remaining three domain controllers since December 2017. When the IRS performed the credentialed vulnerability scan, it resulted in a 312 percent increase in the vulnerabilities identified from an uncredentialed scan.

The second vulnerability scan report provides limited historical information, such as first seen, last seen, and last scan dates and remediation status. The first and last seen dates allowed us to determine previous scan dates. Our review of the second vulnerability scan report found 377 critical and high vulnerabilities with a publication date as early as 2015. Specifically, we found that 245 of the 377 critical and high vulnerabilities were on one domain controller. Of the

[45] TIGTA, Ref. No. 2020-20-013, *The Continuous Diagnostics and Mitigation Project Effectiveness Would Be Improved by Better Performance Metrics and Tools Data* (Mar. 2020).
[46] IRS, *CDM Data Consistency and Quality Review – Draft* (Sept. 2019).

245 vulnerabilities, 167 vulnerabilities and 78 vulnerabilities were categorized as critical and high, respectively.

The IRS is also required to protect information systems from malicious code. We worked with system administrators, using an antivirus management console, to evaluate these requirements for the ISRP domain controllers. Our review determined that all domain controllers were up to date with antivirus malicious code protection and the virus definitions did not exceed 24 hours.

In our audit of mainframe systems, we found that the IRS implemented the necessary tools and processes to detect and remediate software vulnerabilities on its IBM mainframe platform. However, when we requested credentialed vulnerability scan reports, the Enterprise Technical Assessment Office stated that it could not perform [redacted] is not possible primarily due to a lack of known vulnerabilities to develop adequate tests and Common Vulnerability Scoring System scores. As a result, the IRS provided uncredentialed vulnerability scan reports for August, September, November, and December 2019. Our review of the uncredentialed reports determined the following.

- 4,146 unique vulnerabilities: 46 critical, 134 high, 66 medium, and 3,900 low vulnerabilities.
- 33 of the 46 critical vulnerabilities exceeded the IRS policy of 30 days for remediation. [redacted]. Management from both the Cybersecurity and Enterprise Operations functions provided evidence demonstrating that these vulnerabilities were false positives. The Cybersecurity function's Enterprise Vulnerability Scanning Office is working with the vendor to develop a fix that will prevent this false positive in future vulnerability scans.
- 10 of the 134 high vulnerabilities exceeded the IRS policy of 60 days for remediation. The 10 high vulnerabilities resulted [redacted]. These vulnerabilities also present operational challenges throughout the IRS enterprise, affecting a total of [redacted]. As a result, an enterprise-wide POA&M was created to track both findings across all operating systems.

Although the IRS is also required to protect information systems from malicious code, according to subject matter experts, the IBM mainframe platform does not have malicious code mechanisms due to a lack of known viruses that would allow for virus definition development.

[redacted][47]

[47] [redacted].

Figure 9: [redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted].[48]

[redacted][49]

[redacted].

[redacted].

[redacted]

[redacted]

[48] [redacted].

[49] [redacted].

[redacted]

confidentiality, integrity, and availability of the system.

[redacted]

[redacted]

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 2020, TIGTA performed two audits of audit logging. We initiated an audit[50] to determine whether the IRS has effectively implemented unauthorized access audit trail policies and procedures. We found that the IRS could not provide an accurate inventory of all applications that store or process taxpayer data and Personally Identifiable Information. We obtained different inventory lists from various offices at different points of the audit. For example, in March 2019, we received an inventory list of 155 applications from the Enterprise Security Audit Trails (ESAT) Project Management Office (hereafter referred to as the ESAT Office), and a month later, we received an inventory list of 167 applications from business units across the IRS. In November 2019, we received the inventory list of 48 applications from the Privacy, Governmental Liaison, and Disclosure Office. Throughout the audit, TIGTA's Office of Investigations also provided us with the inventory of applications with which it was working.

We collaborated and worked with the Office of Investigations as well as the IRS and determined there are 67 applications that store or process taxpayer data and Personally Identifiable Information that should be capturing and sending audit trails to the Security Audit and Analysis System (SAAS) for unauthorized access monitoring and investigations. The SAAS is a centralized data repository that collects audit logs of transactions from various applications and performs

[50] TIGTA, Ref. No. 2020-20-033, *Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information* (July 2020).

analyses for unauthorized access violation detection and investigations. Four (6 percent) of the 67 applications were not on the Office of Investigations' inventory list. In addition, 28 (42 percent) of the 67 applications were on the Office of Investigations' inventory list but not on the IRS's inventory lists. The importance of maintaining a current and accurate inventory is essential to ensure that applications with sensitive information are being monitored for unauthorized access.

We also found that the SAAS did not contain information for all applications and did not have sufficient audit trail information. Of the 67 applications, we found:

- 6 (9 percent) applications had accurate and complete audit trails in the SAAS.
- 30 (45 percent) applications were sending deficient audit trails to the SAAS. The missing data included success or failure of events, Internet Protocol address of the user initiating an event, Master File tax codes, Taxpayer Identification Numbers, and tax periods.
- 31 (46 percent) applications were not sending audit trail information to the SAAS.

We requested the *Audit Control Responses* for the 30 applications with deficient audit trails to determine whether the application owners and the ESAT Office are reporting and capturing the deficiencies as required. We found that the *Audit Control Responses* for 21 (70 percent) applications listed the missing data and nine (30 percent) applications did not.

In addition, our review of two Organizational Common Controls Security Plans[51] determined that the IRS timely reviewed and updated the list of auditable events at the organization level, at a minimum of every two years, as required. However, the ESAT Office procedures require application owners to perform an additional analysis to determine the criteria for which the audit events specific to their applications are implemented and to revalidate annually. Our review of 30 applications determined that the audit events for 17 (57 percent) applications were aligned with the updated Internal Revenue Manual 10.8.1. However, the audit events for the remaining 13 (43 percent) applications made reference to the obsolete Internal Revenue Manual 10.8.3, *Information Technology (IT) Security, Audit Logging Security Controls*.[52] The range of the dates on the *Audit Control Responses* were from April 28, 2011, to December 14, 2016. Because complete and accurate audit trails are not available for all applications that process taxpayer data or Personally Identifiable Information, the IRS cannot ensure that it or the Office of Investigations can sufficiently investigate security violations or unauthorized accesses.

In our audit of identity proofing, we found that generally the public-facing applications generate audit logs, but some logs did not include administrators' actions and other required data. The IRS decided the identity assurance levels for 25 of the 63 public-facing applications that completed Steps 4 and 5 of the DIRA process. The 25 public-facing applications were assessed as either identity assurance level 1, which will not require a user to validate or verify his or her identity, or identity assurance level 2, which will require a user to complete identity proofing remotely or by being physically present. We reviewed information from the systems security plans, the Office of Investigations' results from its analysis of the SAAS, and audit log data from the 25 public-facing applications (if data were available) and found the following:

[51] Dated June 26, 2017, and June 21, 2019.
[52] Dated July 7, 2015.

- The IRS generated audit trails for 20 applications, of which [redacted] and five were designated as identity assurance level 1. The IRS did not generate audit trails for the remaining five applications, of which [redacted] and one as identity assurance level 1. Of these five applications, two applications are currently offline and not in use, one application is hosted externally to the IRS as a managed service, one application is not in operation, and the remaining application does not generate audit trails because it is managed under another application.
- 19 of the 20 applications are sending audit trails to the SAAS. The IRS is working toward sending the audit trails for the remaining application to the SAAS.
- 7 of the 19 application audit trails sent to the SAAS were accurate or complete on content and 12 were not. For example, we found six applications were not providing records on accesses by database and systems administrators.

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.

In Fiscal Year 2020, the GAO performed an audit involving separation of duties. In its audit of the IRS's information system security controls, the GAO reported that the IRS allowed incompatible user roles to be assigned to certain employees for one of its financial reporting systems.

Security policies, procedures, and 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.

In Fiscal Year 2020, TIGTA performed six audits involving system policies, procedures, and documentation. We initiated an audit[53] to determine whether planned corrective actions (PCA) reported as closed by the IT organization have been fully implemented, adequately documented, and properly approved and whether those actions effectively corrected the identified deficiencies. We found that documentation supporting information technology PCA closures was not always uploaded to the Joint Audit Management Enterprise System (JAMES).

[53] TIGTA, Ref. No. 2020-20-022, *Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Fully and Effectively Implemented and Documented* (June 2020).

Prior to April 1, 2017, the Enterprise Audit Management organization did not require the IRS to upload supporting documentation to the JAMES if corrective action was taken to address the identified deficiency prior to signing the management's response to the TIGTA draft report. One of the 15 judgmentally sampled PCAs met this criterion; therefore, documentation for it was not required to be uploaded to the JAMES. Of the remaining 14 judgmentally sampled PCAs, our analysis determined that eight (57 percent) PCAs had insufficient documentation in the JAMES to fully support their closures.

For example, TIGTA originally found that reported vulnerabilities were not timely remediated on file transfer servers in the Demilitarized Zone. The IRS stated that it has a process in place to continuously and timely implement patches and would verify that patches were applied to the file transfer servers. The IRS uploaded an undated and unsigned half-page document that lists seven procedures that briefly describe patching responsibilities. This document is not official and does not provide sufficient support as an enterprise-wide process to continuously and timely implement patches to file transfer servers, including those located in the Demilitarized Zone. The IRS also did not upload documentation that supports verification of timely patching the file transfer servers. Enterprise Operations function management subsequently provided documents on the standards for server patch management and the standard operating procedure to continuously and timely implement patches to the information technology infrastructure. In addition, they provided customized patch reports to support that some patches were installed to file transfer servers, including those located in the Demilitarized Zone, within established time frames.

In addition, our review of 14 of the 15 judgmentally sampled PCAs found that Forms 13872, *Planned Corrective Action (PCA) Status Update for TIGTA/GAO/MW/SD/TAS/REM Reports,*[54] were adequately completed and uploaded to the JAMES. The Form 13872 for the remaining PCA was not uploaded to the JAMES, but the assigned JAMES audit coordinator for this PCA was able to provide a copy. Our subsequent review of the remaining Form 13872 determined that the JAMES audit coordinator did not sign the form, and the IRS approving official did not sign the form with either a handwritten or an electronic signature as required but rather typed his or her name on the form approximately 25 months after the PCA due date of October 2, 2016. Without sufficient supporting documentation in the JAMES, there is limited evidence readily available to support that all of the judgmentally sampled PCAs were fully implemented.

In TIGTA's audit of identity proofing, we found that the Cybersecurity function developed a draft standard operating procedure document that outlined the purpose, procedures, and output of each activity within the DIRA six-step process. For the DIRA process, NIST Special Publication 800-63-3 requires 10 elements that are to be strictly followed. We determined that three of the 10 elements did not apply, *e.g.*, an agency relying party shall select individual assurance levels based on risk, because the IRS is not and does not plan to be a CSP for other Federal agencies.[55] For the remaining seven elements, we confirmed that the IRS included them in the draft DIRA Standard Operating Procedure.

[54] All business units also use this form to record specific actions taken to implement and to update the status of their PCAs, *e.g.*, adding the PCA implementation date or extending the due date. MW is Material Weakness, SD is Significant Deficiency, TAS is Taxpayer Advocate Service, and REM is Remediation Plan.

[55] The IRS considers itself a CSP under the superseded NIST Special Publication 800-63-2 guidelines. As a CSP, the IRS uses the electronic authentication level of assurance 2 and 3 workflow process that involves the Integrated Customer Communications Environment verification, financial verification, and/or telephone verification to issue or register tokens and issue electronic credentials to taxpayers.

However, we identified two requirements in the draft DIRA Standard Operating Procedure that should be updated prior to it being finalized. First, we did not identify a requirement for capturing the concurrence of the preoversight and oversight voting decisions. The standard operating procedure required the approval of the assessed x assurance levels;[56] however, it did not specify that the approval be in writing or documented. Second, we had concerns with the vagueness of the "periodic" reassessment as part of Step 6 of the DIRA process that requires an ongoing assessment of the public-facing applications. The standard operating procedure stated that applications must be reassessed on an ongoing basis to ensure that appropriate x assurance levels are being applied and to validate that they are being consistently implemented. Reassessment will occur on a periodic basis or after event-based triggers, such as a DIRA process change or transaction data change within an application.

Management Action: After the completion of our audit work, the Director, Security Risk Management, provided the finalized version of the standard operating procedure dated August 2019. We reviewed the approved finalized standard operating procedure and verified that it included a requirement to capture the concurrences of the preoversight and oversight voting decisions as well as defined "periodic" as an annual reassessment of the public-facing applications for the appropriateness of the x assurance level designations.

In our audit of audit trails, we found that the IRS made some progress in implementing solutions to address audit trail processing with the issuance of policies, procedures, and guidance. On June 30, 2018, as a supplement to the overall Internal Revenue Manual audit trail requirements, the ESAT Office revised the Audit Trail Deficiency Memorandum to clarify the application owner's responsibility to correct audit deficiencies and made changes to the Enterprise FISMA Services function's responsibilities. Figure 10 shows the improvement that the IRS made in Calendar Year 2018 as compared to the previous three calendar years with timely creating the POA&Ms in the Treasury FISMA Inventory Management System to address the applications with deficient audit trails.

Figure 10: Timeliness of POA&M Preparation Based on Audit Trail Deficiency Memorandum Issuance for Calendar Years 2015 Through 2018

Calendar Year	Audit Trail Deficiency Memorandum Issued (POA&M expected unless otherwise noted)	POA&M Not Prepared	POA&M Prepared	
			Untimely	Timely
2015	10	3	6	1
2016	7	3	4	0
2017	4[57]	1	2	0
2018	11	4	1	6
Total	**32**	**11**	**13**	**7**

Source: TIGTA's review of IRS Audit Trail Deficiency Memorandums from Calendar Years 2015 through 2018, the corresponding POA&Ms, and security documentation.

[56] When described generically or bundled, NIST Special Publication 800-63-3 guidelines refer to the identity assurance level, authenticator assurance level, and federation assurance level as xAL (x assurance level).
[57] A POA&M was not required for one Audit Trail Deficiency Memorandum issued in Calendar Year 2017.

In addition, we found that weaknesses identified in Audit Trail Deficiency Memoranda are not always tracked in a POA&M. Specifically, our review of 30 applications with deficient audit trails and 28 applications with no audit trails being sent to the SAAS[58] determined that the IRS is not creating POA&Ms for all audit trail deficiencies and uploading the POA&Ms into the Treasury FISMA Inventory Management System as required. The Audit Trail Deficiency Memorandum provides the results of the ESAT Office's review of the documentation for the audit security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements.

We obtained 32 and 26 Audit Trail Deficiency Memoranda issued in Calendar Years 2015 through 2018 from the 30 applications[59] with deficient audit trails and 28 applications with no audit trails, respectively. For the 32 Audit Trail Deficiency Memoranda, we found:

- 20 (63 percent) Audit Trail Deficiency Memoranda were tracked in a POA&M. Seven (35 percent) POA&Ms were timely prepared within the 60-calendar-day requirement; however, 13 (65 percent) were untimely prepared with a range of 24 to 1,099 calendar days.
- 11 (34 percent) Audit Trail Deficiency Memoranda were not tracked in a POA&M.
- 1 (3 percent) Audit Trail Deficiency Memorandum was not required to be tracked in a POA&M.

For the 26 Audit Trail Deficiency Memoranda, we found:

- 20 (77 percent) Audit Trail Deficiency Memoranda were tracked in a POA&M. Three (15 percent) were timely and 17 (85 percent) were untimely prepared with a range of 29 to 1,319 calendar days.
- 6 (23 percent) Audit Trail Deficiency Memoranda were not tracked in a POA&M.

In our audit of the IRS's Volunteer program sites, we found that the IRS does not require its partners participating in the Volunteer program to develop a written information security plan for each site where taxpayers are provided free tax return preparation. An information security plan is a formal document that provides an overview of the security controls in place or planned to protect taxpayer information.

When we raised our concerns to Stakeholder Partnerships, Education, and Communication function management, they stated that they do not believe the requirement for financial institutions to develop a written information security plan applies to its partners in the Volunteer program. Management stated that IRS Publication 4557, *Safeguarding Taxpayer Data – A Guide for Your Business*,[60] defines a financial institution covered by the Safeguards Rule[61] as professional tax preparers, and because volunteers are not professional tax preparers, it does

[58] There were three applications on the December 2019 updated Office of Investigations' inventory that were not on the January 31, 2019, inventory list that we used to obtain the Audit Trail Deficiency Memoranda to perform our analyses.
[59] An application can have more than one Audit Trail Deficiency Memorandum.
[60] Revision June 2018.
[61] The Safeguards Rule requires financial institutions under the Federal Trade Commission's jurisdiction to have measures in place to keep customer information secure.

not apply. We disagree. IRS Publication 4600, *Tips for Safeguarding Taxpayer Data*,[62] contradicts management's position. According to Publication 4600, financial institutions covered by the Safeguards Rule include return preparers, data processors, transmitters, service providers, and others who are *significantly engaged in providing financial products or services that include preparing and filing tax returns*. Volunteers are significantly engaged in preparing and filing tax returns and, as such, we believe the Safeguards Rule applies and an information security plan should be developed for each site in an effort to protect taxpayer data.

In our network user and device authentication audit, we found that the Unified Access project needs to implement an approved security change to an existing system. Cybersecurity function policy provides that, if the ISE is considered a new system, the project team is required to obtain an Authorization to Operate prior to deployment into production. Otherwise, the ISE would be considered a security change to an existing system, and the project team would be required to follow the Change Management process. In October 2017, the Cybersecurity function completed a Control Impact Assessment for the ISE. Subsequently, the Cybersecurity Change Advisory Board reviewed the impact assessment and determined that the change deploying the ISE into production in enforcement mode would require adding the ISE to an existing system's security boundary, System Security Plan, and Information Systems Contingency Plan.

In January 2020, the Unified Access project manager explained that it is management's intention to add the ISE to the General Support System-34 Enterprise Network security boundary. To confirm the relationship between the ISE and the General Support System-34, we reviewed a March 2015 Security Change Request that identified the ISE which affected the General Support System-34. Subsequently, we verified that the General Support System-34's system boundary had not been revised, and the General Support System-34's System Security Plan and Information Systems Contingency Plan had not been updated to include the ISE. Therefore, the Unified Access project team and the Cybersecurity function did not complete the necessary tasks to accomplish an approved security change to add the ISE to the General Support System-34. By not following the Enterprise Life Cycle (ELC) methodology, the software development, security, and contingency planning of the Unified Access project, as a component of a critical infrastructure protection asset, are potentially at risk.

In our audit of wireless networks, we found that the IRS has sufficient security policies and procedures over the wireless networks, and its primary guidance document, the Internal Revenue Manual, was properly aligned with selected controls for wireless network security from the NIST, Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.[63] In many instances, Internal Revenue Manual policies and procedures included additional detailed guidance related to wireless networks.

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

[62] Revision August 2016.
[63] Revision 4, dated April 2013 (includes updates as of January 22, 2015).

taxpaying public and its expectations, technological disruptions, shifts in the workforce, and an increasingly globalized and interconnected world.

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, asset management, governance and project management, cost management, data management, risk management, implementation of corrective actions, and modernizing operations.

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 for planning, negotiating, executing, and managing the procurement of information technology products and services. It is also 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.

During Fiscal Year 2020, TIGTA conducted an audit[64] to review the IRS efforts to implement an Enterprise Case Management (ECM) solution. We found that the procurement process delayed deployment of ECM, Release 1.0. The IRS suspended the previous ECM project's development activities in April 2017 following notification to the IRS Commissioner that the tool was not a viable solution. The IRS spent $85.4 million and approximately two and one-half years to develop a case management system that was unsuccessful. ECM program management stated that the unsuccessful development pushed them to thoroughly identify the business requirements needed for the ECM solution award. In April 2017, the IRS decided to use an in-depth, commercial off-the-shelf product assessment to ensure a successful procurement.

Phase I of the procurement process started with performing market research on case management solutions from private industry and five Federal agencies. The ECM program then completed two Requests for Information and a draft Request for Quotation. After issuing a final Request for Quotation in May 2018, the IRS completed product demonstrations and received proposals from eight vendors. Phase II started in September 2018, when the IRS selected two vendors and issued two Blanket Purchase Agreements, costing approximately $500,000 each, to procure the vendors' software to perform technical evaluations. IRS management stated that this enabled them to validate vendor capabilities and obtain insight into the vendor solution. They also stated that this process was beneficial in finding a solution that met the ECM program's needs.

[redacted][65]

[64] TIGTA, Ref. No. 2020-20-061, *The Enterprise Case Management Solution Deployment Is Delayed, and Additional Actions Are Needed to Develop a Decommissioning Strategy* (Sept. 2020).
[65] Any interested party, but typically the losing vendor, may file a protest if they feel a Government contract has violated procurement laws or regulations.

[redacted].

During the lessons learned process, the ECM Physical Assessment and Analysis test team identified gaps in communication and received inconsistent information between the vendor and the Office of the Chief Procurement Officer. These issues resulted in the misunderstanding of requirements during the ECM Physical Assessment and Analysis process of evaluating vendor software and could have mitigated some of the risks raised in the protest. ECM program management stated that the requirement discrepancy that led to the protest occurred because key personnel were not privy to the required procurement information.

During the protest, ECM program management discussed the procurement sensitivity issues with the Office of the Chief Procurement Officer. After the discussion, ECM program management stated that key decision makers and approving officials were provided with proper procurement sensitive information and a more collaborative process occurred. As a result, the IRS completed its corrective action and successfully procured the solution on April 2, 2020. The initial lack of proper detail in the Request for Quotation and the corresponding IRS decision to undertake a corrective action contributed to an eight-month delay in receiving the ECM solution. By identifying development activities that the ECM program could still work on during this delay, the IRS only pushed back its scheduled deployment date by approximately three months.

Asset management

Asset management controls are key to: 1) timely detecting loss, theft, or misuse of Government property; 2) helping to mitigate unauthorized access to taxpayer or other sensitive information; 3) ensuring accurate financial statement reporting; and 4) helping management make sound operating decisions and manage operations. Asset management includes asset inventory management and information technology architecture.

Asset inventory management

Asset inventory is the way an organization lists and provides details of the assets it owns. Asset inventory management is the means by which an organization monitors its assets, such as physical location, maintenance requirements, depreciation, performance, and eventual disposition of the asset. Implementing robust procedures for managing asset inventory is a critical part of the organization's accounting processes. It also helps to ensure that the organization has a clear understanding of the assets it owns and that the assets are being utilized in the most efficient and cost-effective manner.

In Fiscal Year 2020, TIGTA performed three audits covering the management of hardware inventory. We initiated an audit[66] to evaluate the IRS's controls over purchased non–

[66] TIGTA, Ref. No. 2020-10-039, *The Annual Inventory Certification Process for Non–Information Technology Assets Needs Improvement* (July 2020).

information technology asset inventory. We found that information technology assets were misclassified as non–information technology assets. During our physical inventory, we noted a total of 10 mail inserters, six of which were classified as information technology assets. Facilities Management and Security Services and IT organization personnel discussed the inconsistency and determined that all 10 mail inserters should be considered information technology assets. We then reviewed the inventory system; it contained seven mail inserters misclassified as non–information technology assets, having a total acquisition cost of $4.3 million, or 12 percent of the value of the non–information technology assets.

The physical inventory procedures in the Property and Asset Management program desk guide do not provide guidance on how to determine if assets are properly classified. However, it states that the assets listed in the inventory system should be verified by a physical count and any differences reconciled. We believe Facilities Management and Security Services organization personnel should have noted that only four of the 10 mail inserters were listed as non–information technology assets in the inventory system and determined there was an inconsistency in how these assets were classified. Proactively identifying similar assets during physical inventory verification would help ensure that all assets are appropriately accounted for and consistently classified.

In our audit of mainframe systems, we found that IBM mainframe hardware asset inventories were inaccurate and incomplete. The inventory system relies heavily on manual data entry and currently does not sufficiently leverage available automated tools to assist in maintaining an up-to-date, complete, and accurate inventory. We determined that the November 2019 and January 2020 inventory reports were both inaccurate and incomplete and did not contain the level of granularity required for timely and up-to-date tracking and reporting. Specifically, we found 62 policy exceptions [redacted].

Figure 11: [redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

Some specific examples of inaccurate and incomplete reporting include:

- The November 2019 inventory report listed eight assets as *In Use;* however, we found that the eight assets should have been listed as *Retired*.
- The January 2020 inventory report documented [redacted]; however, we found that [redacted] are located at [redacted].

- During a site visit to [redacted], we identified [redacted] that were not included on either inventory report. Further analysis determined that the [redacted] were incorrectly assigned to the Enterprise Network function.

In addition, we reviewed the November 2019 IBM mainframe platform inventory after the IRS received, installed, and replaced [redacted] in the production environment between August 3 and October 6, 2019. We identified the following discrepancies:

- The [redacted] were not listed in the inventory.
- Of the [redacted] that were documented, [redacted] were listed as *In Use*, but they should have been listed as *In Stock*. [redacted] were listed as *In Stock*, but no updates were submitted to indicate that they needed to be *Retired*.

Throughout the course of the audit, the [redacted] Support Branch worked closely with the User and Network Services function's Hardware Asset Management Office to correct all of the discrepancies we identified. As a result, the March 2020 inventory report provided an accurate and up-to-date list of [redacted] associated with the IBM platform. Without accurate inventories, the IRS cannot ensure that it is properly monitoring and maintaining mainframe computer components in a secure manner.

In addition, we found that the Treasury Department *Cybersecurity Analysis and Reporting Dashboard* report was inaccurate and incomplete. The Cybersecurity function's Office of Strategy and Business Analytics is responsible for all facets of the IRS's monthly dashboard submission. [redacted][67] [redacted], resulting in 52 logical partitions unreported. [redacted] Without accurate logical partition reporting, senior IRS leadership and executive stakeholders as well as external stakeholders will not have accurate information for decision-making.

In our audit of wireless networks, we found that the wireless access point inventory is incomplete and inaccurate. The IRS installed 852 wireless access points nationwide. We visited 28 IRS locations in four metropolitan regions across the United States, [redacted], and selected a judgmental sample of 321 (38 percent) of the 852 wireless access points to perform a physical verification. In total, we found inventory errors on 205 (64 percent) of the 321 wireless access points reviewed. We were unable to locate 27 (13 percent) of the 205 wireless access points with inventory errors. When we shared our results, User and Network Services function management stated that 15 devices were stored elsewhere in the same location or moved to another off-site location, one device was sent to a site for testing, and four devices were returned to a deployment team for reallocation. Because this information was provided to us as we completed our audit work,

[67] To satisfy this reporting requirement, the IRS reports the total number of logical partitions operating within the mainframe systems.

we were unable to physically verify the updated status for the 20 devices. The remaining seven devices could not be accounted for.

For the remaining 178 wireless access points, the inventory information had not been updated to properly reflect the location, and the access points were not correctly labeled.[68] Specifically, we found the following issues:

- 166 devices were either missing the IRS-assigned access point name or the name was different from what was shown on the inventory list.
- 27 devices were found in a location, *i.e.*, a room, that was different from what was shown on the inventory list.
- 4 devices had an IRS inventory barcode that was different from what was shown on the inventory list.

In addition, we found 13 wireless access points that were installed but not included in the inventory list. In March 2020, User and Network Services function management provided an updated inventory list, and we were able to account for eight of the 13 devices. The remaining five devices were not on the inventory list even though they were installed as official wireless access points. Having an incomplete or inaccurate inventory can impede IRS management's ability to manage the assets within the wireless networks or locate and troubleshoot any technical issues that may occur. An inaccurate inventory also hinders the IRS's ability to timely detect the loss or potential theft of the devices.

Information technology architecture

Information technology architecture is the fundamental underlying design of computer hardware, software, or both. An effective information technology architecture plan improves efficiencies. When the architecture program includes consolidation and centralization of information technology resources, complexity can be reduced and resource use can improve.

In Fiscal Year 2020, TIGTA performed an audit covering information technology architecture. In our active directory audit, we reviewed architecture administrative costs. We found that the IRS did not assess the current ISRP Active Directory architecture to potentially reduce the administrative costs and digital footprint of operating multiple active directory forests. Applications Development function personnel stated that each ISRP system currently needs a separate active directory forest because the system can only communicate across a local area network. Further, they explained that restructuring the ISRP Active Directory architecture would require a full system redesign. The IRS did not estimate potential system redesign costs. Without a system redesign estimate, we could not determine whether there would be any cost savings when consolidating the architecture into a single forest once these system redesign expenses were considered.

Governance and project management

An information technology project is an effort undertaken over a fixed period of time that includes all aspects of project management, such as planning, design, implementation, and training. Guiding the information technology project effort is a governance body.

[68] The total number of exceptions will not equal 178 because some wireless access points had multiple inventory issues.

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 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.

In Fiscal Year 2020, TIGTA provided coverage of information technology governance in two audits. We initiated an audit[69] to evaluate the implementation of the IRS's enterprise-wide cloud strategy to ensure compliance with Federal guidance. Enterprise Services function personnel created the Enterprise Cloud program and the Cloud Governance Board charters. For projects considering a cloud computing solution, the Enterprise Cloud program charter provides personnel the authority to develop cloud guidance and standards for project owners. The charter also authorizes personnel to provide cloud consultative services to business units and project owners. However, as of September 2019, the IRS had not authorized or approved the Cloud Governance Board charter.

The Cloud Governance Board, once authorized and approved, will provide governance and oversight to projects within the Enterprise Cloud program that are undertaken to achieve the IRS Cloud Target State.[70] The primary objectives of the Cloud Governance Board include ensuring that the Enterprise Cloud program delivers its scope on schedule, program expenditures are fiscally sound, and program risks are managed appropriately. An authorized charter will empower the Enterprise Cloud program to officially communicate and approve formal agreements between different IRS internal organizations—specifically, the Office of the Chief Procurement Officer and the ELC Office. The charter also will provide direction from the board to prioritize and formally approve new workstreams,[71] such as the cloud services procurement workstream. Because the charter is not approved, there is increased risk for potential wasted resources because the IRS could deploy multiple, duplicative, and overlapping systems with no coordination. Effective controls that comply with Federal guidance and enforce standards help mitigate the risk of inefficient or unsanctioned efforts to deploy cloud systems.

We also initiated an audit[72] to assess the effectiveness and efficiencies achieved through the IRS's implementation of Robotic Process Automation (RPA) and Intelligent Automation technologies. We found that the RPA program did not establish an effective governance structure. In November 2018, program management presented an overview of the RPA program to the IRS Commissioner and explained their plans to establish a governance structure to lead, develop, and operate automation development projects as well as develop a program strategy and acquire automation tools. However, as of July 2020, the program still has not established key components that comprise a proper governance structure for automation

[69] TIGTA, Ref. No. 2020-20-010, *The Enterprise Cloud Program Developed a Strategy, but Work Remains to Achieve Cloud-Based Modernization Goals* (Mar. 2020).
[70] The future state of IRS cloud operations as outlined in the December 2017 IRS Cloud Strategy.
[71] A readiness activity intended to produce an output that will help the IRS achieve the target cloud state, focused around the people, process, and technology elements necessary to support and enable the successful adoption of cloud services across the enterprise.
[72] TIGTA, Ref. No. 2020-20-060, *Process Automation Benefits Are Not Being Maximized, and Development Processes Need Improvement* (Sept. 2020).

projects. For example, the RPA program does not have an approved charter to define the program's mission, vision, scope, and expected outcomes; a program management plan to provide information on how the RPA program will be planned, executed, monitored, and controlled; an operating model to establish the structural framework for deploying the RPA at the agency level; and a roadmap to define the timeline and steps necessary to build the program, platform, processes, and procedures for developing automation projects. It also does not have a common platform to establish an enterprise capability to develop, deploy, and operate automation projects.

While the IRS had planned to establish an RPA Program office in the first quarter of Fiscal Year 2020, program efforts were paused while priorities for the IT organization's funding were examined. As a result, many of the RPA program governance and strategy documents were delayed. Subsequently, in mid-January 2020, the IRS decided to allocate some funds to continue RPA program activities to the end of the fiscal year. Without a functioning governance structure, an organization is not in place to oversee and manage the life cycle of automation projects from origination, development, testing, and deployment through operations.

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 2020, TIGTA provided coverage of information technology project management in seven audits. We initiated an audit[73] to determine whether the IRS is effectively and efficiently managing the Customer Account Data Engine 2 program's Individual Tax Processing Engine project with a focus on velocity estimates and development. We found that, generally, the IRS is effectively monitoring the progress of the project. The project is broken down into 24 product increments, each comprised of five two-week sprints, totaling 10 weeks in duration. The IRS held various meetings to plan and monitor the project during each product increment. Planning meetings occurred at the beginning of each product increment as well as at the beginning of each of the five sprints. Monitoring meetings occurred at various times.

As a result of their ongoing monitoring efforts, IRS management identified challenges, *e.g.*, insufficient backlog of building blocks,[74] insufficient resources, and implemented actions, *e.g.*, streamlined processes to reduce overhead, received approval for additional resources, to address project velocity challenges. The project team documents risks and issues in the Integrated Project Team meeting documents and participates in the Customer Account Data Engine 2 program risk reviews, which also manages risks and issues. When warranted, risks and issues were also reported in the Item Tracking Reporting and Control system, a customized tool that allows users to submit and update risks, action items, and issues.

In addition, we found that the IRS used an updated process to measure project progress. The IRS has taken steps to improve the process for estimating the development time required to convert lines of code from Assembler Language Code to Java. At the outset of the Individual

[73] TIGTA, Ref. No. 2020-20-062, *The Individual Tax Processing Engine Project Is Making Progress* (Sept. 2020).
[74] A grouping of Assembler Language Code lines of code with common functionality.

Tax Processing Engine project, the IRS identified the complexity of the Individual Master File[75] Assembler Language Code containing several irregular coding conventions that do not exist in modern programming languages. Customer Account Data Engine 2 management stated that, when they established initial development estimates in Fiscal Year 2017, the level of effort required to develop the Individual Tax Processing Engine scope was unknown. The IRS chose lines of code as the method to estimate the size of the development effort. There are 146,000 lines of code to convert plus 68,000 lines of code equivalents for Technical Enablers for the entire project. To measure the progress throughout Fiscal Year 2019, the IRS identified four Confidence Milestones to measure overall project health. The IRS stated that velocity was the most significant of the Fiscal Year 2019 Confidence Milestones because it provided insight into the Assembler Language Code to Java lines of code conversion velocity, a major quantifiable metric. Due to the velocity challenges that the project faced, the project did not achieve the Velocity Confidence Milestones, and they were discontinued for Fiscal Year 2020. However, the IRS continued to monitor the Individual Tax Processing Engine velocity by comparing planned lines of code work to actual work completed.

In April 2019, the IRS stated that it established an initial Trajectory Model to track and monitor velocity metrics, but it did not account for all work to be completed. In August 2019, the Customer Account Data Engine 2 Program Management Office worked with a contractor to create the *Customer Account Data Engine 2 Program Management Office Trajectory Model*. In September 2019, the Customer Account Data Engine 2 Program Management Office used data from Product Increments-6, -7, and -8 to update the Trajectory Model to project the Assembler Language Code lines of code conversion for each product increment, starting with Product Increment-9. Because of the extensive analysis to account for the project's complexity and capturing all work required, the updated Trajectory Model determined that the development end date needed to be moved from August 2021 to September 2022.

In weekly reports to IRS executives, the *Customer Account Data Engine 2: Individual Tax Processing Engine Weekly Executive Update* compares the actual work completed to both the Enterprise Program Management Office and Applications Development function planned work estimates. IRS management explained that the Enterprise Program Management Office estimate is determined by the Trajectory Model and is the minimum work needed to meet the revised September 2022 development end date. The Applications Development function sprint teams set goals for themselves during the product increment and sprint planning based on multiple factors. They are encouraged to set challenging goals, and those numbers become the Applications Development function's targets for the product increment. When reporting these metrics to the CIO, actual numbers are compared against Enterprise Program Management Office estimates.

We also determined that the IRS's current estimation process incorporates GAO best practices[76] to estimate the duration of the project and velocity rate. For example, the GAO states that estimators should understand interdependencies that affect the schedule. Some examples of interdependencies are employee availability, effective work hours per shift, and downtime from meetings, travel, and sickness. The Trajectory Model accounts for these interdependencies and many more, such as employee skill level, *e.g.*, beginner, intermediate, advanced, and project role, *e.g.*, developer, design architect, test; percent reduction in productivity for coaching;

[75] Data from the Individual Master File is used by the Customer Account Data Engine 2.
[76] GAO, GAO-09-3SP, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs* (Mar. 2009).

percent reduction in productivity for correcting defects; and filing season lines of code equivalents.

In addition, we initiated an audit[77] to evaluate the effectiveness of IRS efforts to implement an insider threat capability to detect, monitor, prevent, and report on insider threats. We found that the IRS's insider threat capability implementation efforts have resulted in substantial progress and adhered to Federal guidance and that controls generally are in place and effective. Specifically, we found that the IRS used relevant, applicable guidance to design its insider threat capability and ensured that it is aligned with modernization goals.

Completed in Fiscal Year 2017, the initial implementation plan included a description of the planned phases of the project as well as the expected services and elements needed to meet Cybersecurity function goals to deliver a mature insider threat capability. The plan also included information about the reporting processes and analytical tools to be deployed incrementally and about how the plan would build advanced capability within the staff. The goal of the initial plan was to drive compliance with NIST Special Publication 800-53 controls governing or directly related to the mitigation of insider threats. In Fiscal Year 2019, the insider threat capability was incorporated into the *IRS Integrated Modernization Business Plan* and renamed the User Behavior Analytics Capability (UBAC) project. We determined that the UBAC project is properly aligned with the strategic goals expressed in the plan. Specifically, it addresses the modernization objective to proactively identify emerging threats and vulnerabilities through the use of real-time intelligence information and analytics.

In addition, we found that processes are implemented to identify and refer potential insider threats. The UBAC project is in an Initial Operating Capability state, and processes have been implemented that use specifically designed criteria, known as use cases, to identify potential insider threats. The IRS developed behavioral analytics processes based on various insider threat types defined by the Carnegie Mellon University's Computer Emergency Response Team and tailored them to the specific IRS threat landscape. Potential insider threats are identified from a predefined series of machine and application log events that were combined to constitute a "behavior" that is potentially threatening to IRS systems (including taxpayer content residing on these systems), people, and resources. The use cases have been incorporated into an analytics tool.

From October 1, 2016, through February 29, 2020, the IRS identified 112 potential insider threats from initial operating capability results. Of these, nine potential threats were referred to the relevant stakeholders for investigation or resolution. The nature of these threats included potential unapproved access, manipulation of data, and a disgruntled employee. For the remaining 103 potential insider threats, the IRS closed 78 because the initial review concluded that the activity was not an insider threat. The other 25 were open, and the UBAC project was in the process of determining whether they should be referred as potential insider threats.

To reach the Full Operating Capability state, the IRS is developing enhanced user behavioral analytics for cross-functional data sharing, communications, data correlation, and reporting to expedite the ability to detect and mitigate risks to data and systems arising from insider threats. In addition, the IRS is developing enhanced user behavioral analytics to proactively identify emerging insider threats through the use of real-time intelligence information and analytics to mitigate risks to data and systems arising from insider threats. According to its status reports,

[77] TIGTA, Ref. No. 2020-20-043, *Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed* (Aug. 2020).

the IRS is on schedule to deliver these capabilities during Fiscal Year 2021. As technologies evolve, the IRS plans to continue strengthening its threat intelligence capabilities even after achieving Full Operating Capability. However, we found that the following additional improvements can assist in achieving an effective Full Operating Capability:

- The processes for determining high-value assets and assessing the related risks have not been documented. The UBAC project was aware of the criteria but believed that the efforts were covered by other IRS functions. Without specifically addressing the identification and assessment of high-value assets, the IRS risks an incomplete capability implementation that may not consider these assets and cannot ensure that all high-value assets are included within the insider threat capability and protected from insider threats. During the audit, the UBAC project initiated corrective actions and obtained a list of high-value assets and performed an initial mapping to risk indicators within its use cases.
- Executive status reports did not include recommended elements. Although the UBAC project's status reports included data related to accomplishments, resources, and risks, the status reports did not include recommendations and goals for program improvement or addressing major impediments or challenges. The UBAC project believed that its status reports provided a vehicle for this information; however, UBAC project management agreed that these items were not explicitly included within the status reports. Without explicit reporting on recommendations and goals for program improvement and addressing major impediments or challenges, executives responsible for recommendation implementation may not be aware of critical information useful for managing their implementation efforts. During the audit, the UBAC project initiated a corrective action and updated its biweekly meeting agenda to include a discussion of recommendations for program improvement and addressing major impediments or challenges.
- The implementation plan did not specially address recommended personnel training curricula. In addition, the IRS was able to provide only limited evidence of any specific training of UBAC project personnel. The UBAC project was unaware of the specific training requirements and, therefore, did not ensure that training was included in the plan as well as scheduled and completed by UBAC project personnel. By not specifically addressing the recommended training in the UBAC project implementation plan, relevant training is not documented and could go unfulfilled, which may create skills and knowledge gaps. Without sufficient training on critical skillsets, the overall effectiveness of the IRS's insider threat capability may be compromised. During the audit, the UBAC project initiated a corrective action and identified three applicable training classes that were added to UBAC project team members' training plans for Fiscal Year 2021.

In our audit of the enterprise cloud program, we found that there are controls in place to ensure that all information technology projects are adhering to ELC requirements. The IT organization currently relies on the existing ELC process to manage information technology projects, including cloud projects. Personnel in the ELC Office stated that there is no Internal Revenue Manual guidance or formalized process regarding cloud services projects. While all information technology projects are required to go through the ELC, the ELC Office relies on the business

units to initiate contact. However, we recently reported[78] that not all information technology infrastructure projects follow the ELC process, indicating these controls are not always effective.

In addition, we found that the IRS enterprise-wide cloud strategy partially met Federal guidance. The IRS created an enterprise-wide cloud strategy that was approved and authorized in December 2017. Enterprise Services function personnel stated that they have since built upon the initial cloud strategy and developed additional documents to guide cloud implementation within the IRS. We assessed the enterprise-wide cloud strategy and related documents as well as its current implementation status against major elements of the *Federal Cloud Computing Strategy*,[79] referred to as the Cloud First policy.

The Cloud First policy identifies a framework for agencies considering and planning for cloud migration, which covers three primary phases: Select, Provision, and Manage. The Select phase consists of assessing potential information technology systems for cloud migration. The IRS's strategy identifies the need for 10 workstreams, such as the cloud migration assessment and services procurement workstreams. The cloud migration assessment workstream is under development with partial implementation, while work on the cloud services procurement workstream, which the IRS identified as a high priority, has not started. The strategy calls for an enterprise-wide cloud portfolio assessment, but Enterprise Services function personnel reported that this assessment has not been performed primarily due to a lack of resources. Instead, the IRS considers projects on a case-by-case basis as the need arises. According to Enterprise Services function personnel, system or project owners considering cloud services should register the project with the Enterprise Cloud program's IRS Cloud Front Door[80] and complete a *Cloud Suitability Assessment*.[81] If a project does not engage the Cloud Front Door, it should be engaged by other IT organization teams as a project goes through the ELC process. However, there is no specific mention of the Cloud Front Door in the existing ELC policy.

The Provision phase consists of aggregating demand at the departmental level to pool purchasing power; integrating services into a wider information technology portfolio; generating contracts for cloud services with explicit service level agreements; and ensuring that legacy systems are decommissioned to realize the full potential of the new cloud solution. The IRS's strategy provides general terminology that contracts need to be clear, but it does not specify terms that need to be stated within the contract, such as explicit service level agreements for security, continuity of operations, and service quality that meet the IRS's needs. In addition, while the strategy generally speaks about cost and asset savings, there is not a consistent and repeatable mechanism to track cost and asset savings from the migration to and deployment of cloud services. There are also no specific details on decommissioning legacy systems.

The Manage phase consists of managing services rather than assets. This process actively monitors the service level agreements in place as well as regularly evaluates the service provider to ensure that the vendor is meeting all expectations set by the contracts and agreements in place. The strategy identifies the need for a cloud workforce development workstream and for

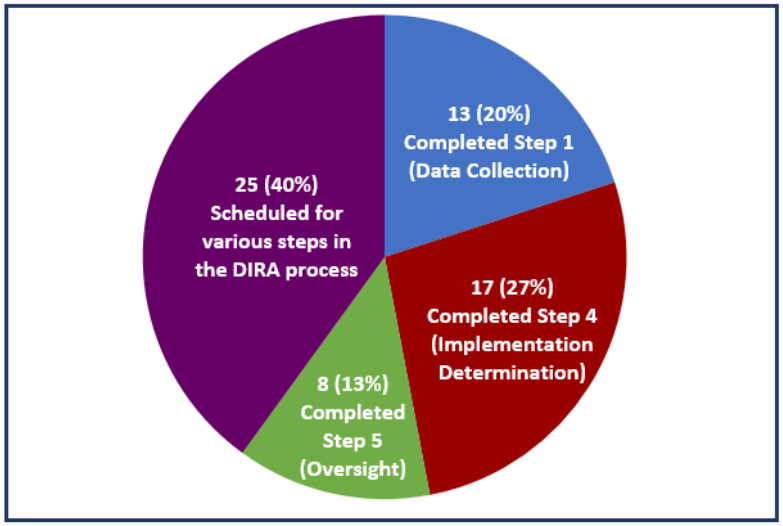
[78] TIGTA, Ref. No. 2019-20-060, *E-Mail Records Management Is Generally in Compliance With the Managing Government Records Directive* (Sept. 2019).
[79] The White House, U.S. CIO Vivek Kundra, *Federal Cloud Computing Strategy* (Feb. 2011).
[80] A central hub of the Enterprise Cloud program to connect directly to Enterprise Services function personnel and navigate cloud resources.
[81] A questionnaire with a three-step approach that enables Enterprise Services function personnel to assess, review, and recommend cloud candidates for migration or implementation.

developing guidance to standardize service level agreements with cloud service providers. Enterprise Services function personnel communicated a plan for the cloud workforce development workstream in October 2019. However, work on this workstream may be delayed due to budget constraints that will affect the ability to establish a consistent and repeatable mechanism to monitor and track service level agreements to ensure compliance and continuous improvement.

In June 2019, Cloud Smart[82] guidance was published, which updated the Cloud First policy. While the Enterprise Services function has incorporated elements of the guidance to inform its prioritization of workstreams, it also stated that it does not plan to incorporate the guidance into the December 2017 enterprise-wide cloud strategy. In September 2019, the Treasury Department released a special notice[83] for informational purposes regarding the development of a Treasury cloud acquisition roadmap. If the roadmap becomes a Treasury directive, it will affect all Treasury bureaus, including the IRS. Enterprise Services function personnel stated they were aware of the special notice and had some communication with the Treasury Department to discuss how the IRS fits into the Treasury cloud acquisition roadmap. Without an updated cloud strategy and defined workstreams, the IRS may miss the opportunity to deliver public value by increasing operational efficiency and responding faster to taxpayers' needs.

In our audit of identity proofing, we found that Cybersecurity function personnel used the draft standard operating procedure, outlining the purpose, procedures, and output of each activity, to perform the DIRA process. The process enables a data-driven approach to identity assurance risk determinations and related implementation for IRS public-facing applications. However, we have concerns about the timely completion of the DIRA process. The IRS has 63 public-facing applications that taxpayers or practitioners can access from the Internet. Figure 12 shows that, from October 2, 2018, through July 1, 2019, these applications either have been completed or were in varied steps in the DIRA process.

Figure 12: The 63 Public-Facing Applications in Varied Stages of the DIRA Process, as of July 1, 2019



Source: TIGTA's analysis of the IRS's 63 public-facing applications.

[82] The White House, U.S. CIO, Suzette Kent, *Federal Cloud Computing Strategy* (June 2019).
[83] Treasury Office of the CIO, *Cloud Acquisition Roadmap* (Sept. 2019).

The IRS decided the identity assurance level for the applications that completed Steps 4 and 5 of the DIRA process as either identity assurance level 1, which will not require a user to validate or verify his or her identity, or identity assurance level 2, which will require a user to complete identity proofing remotely or by being physically present. We attended meetings with the stakeholders and the DIRA team while they were discussing seven of the 25 applications and reviewed the supporting documentation for all 25 applications, *e.g.*, initial DIRA reports, that the IRS used to make its decisions. We concur that the designated identity assurance levels were appropriate, *i.e.*, six applications at level 1 and [redacted].

[redacted] include the Online Accounts application that permits 24 million taxpayers annually to view their balance due amounts, payment histories, and view or obtain transcript-related products. This includes the Get Transcript application that 16 million taxpayers access annually and the Identity Protection Personal Identification Number application that 500,000 taxpayers[84] access annually. For the remaining scheduled applications or those that have completed Step 1, the Cybersecurity function expects them to complete Step 4 by December 2019 and Step 5 by January 2020.

While the IRS is making progress, we are concerned as to whether the IRS can achieve these milestone dates. We analyzed the length of time the IRS took to complete each of the eight applications through Step 5 and determined that it took an average of 217 calendar days, ranging from 91 to 245 calendar days. Specifically, the IRS took an average of 42 calendar days, ranging from 20 to 62 calendar days, to complete the first four steps and an average of 175 calendar days, ranging from 32 to 218 calendar days, to complete through Step 5. The eight public-facing applications were approved on June 4, 2019.

The reason so much time elapsed in Step 5 was that IRS executives first convened in February 2019 but did not begin reviewing applications for approval until April 2019, which was six months after the first public-facing application completed Step 4. Other factors affecting the completion of the DIRA process, for example, included the preparation of IRS processes and systems due to the Tax Cuts and Jobs Act of 2017[85] for the 2019 Filing Season from October to December 2018 and the 2019 Filing Season from January to May 2019 that needed increased oversight by IRS leadership. We anticipate similar conditions, *i.e.*, the upcoming preparation for and implementation of the 2020 Filing Season, which could affect the IRS achieving its January 2020 goal.

In addition, we found that a digital identity proofing solution is being designed; however, some challenges are affecting its implementation. After NIST Special Publication 800-63-3 guidelines were issued in June 2017, the CIO tasked the Applications Development's Identity and Access Management function with developing a strategy to conform with these guidelines. The Secure Access Digital Identity platform was selected as the modernized solution. The Enterprise Services function developed the vision, scope, and architecture for the platform, with a goal to layout the conceptual architecture and then the logical architecture. While the IRS has developed the concept for the Secure Access Digital Identity platform to include a focus on security and empowering taxpayers, the IRS faces challenges to deliver the modernized solution.

[84] The number of taxpayers who annually access the Get Transcript and Identity Protection Personal Identification applications are not unique. In addition, for the Get Transcript application taxpayer count, it could include multiple transcripts that a single taxpayer requested.

[85] Pub. L. No. 115-97, 131 Stat. 2054 (2017). Officially known as "An act to provide for reconciliation pursuant to titles II and V of the concurrent resolution on the budget for Fiscal Year 2018."

1) Testing the modernized solution to prove assumptions and make further decisions – The Design and Innovation Branch plans to test its modernized solution in four phases, which will prove the assumptions made when performing analyses of alternatives to determine the optimal method to achieve the Secure Access Digital Identity vision. Phase I involves installing an enterprise infrastructure product, for testing only, that enables a centralized web access management system to allow user authentication and single sign-on, policy-based authorization, identity federation, and auditing of access to web applications.

   The IRS planned to perform Phase I from June 2019 to November 2019 and will make a decision on the outcome and any adjustments as needed. The next two phases were planned for October 2019 to January 2020 and December 2019 to May 2020. The final phase of the test, from June 2020 to November 2020, is a pilot with a CSP from end to end with one of the IRS's public-facing applications. Following the completion of the four tests, the IRS plans to complete a go/no-go evaluation of the platform based on the test results. In addition, the IRS will develop a plan to successfully migrate all of the online applications from the current system to the Secure Access Digital Identity platform by an undetermined implementation date.

2) Operating with levels of assurance that are based on superseded NIST guidelines – The IRS is operating with levels of assurance supported by the superseded NIST Special Publication 800-63-2 guidelines for [redacted] of the [redacted]. The levels of assurance are not comparable to the NIST Special Publication 800-63-3 requirements for the applications designated as x assurance level 2, which introduces the need for either remote or physically present identity proofing. We estimate that the [redacted] could have approximately 250 million user accesses annually, so better security is needed for the taxpayer data.

   The remaining 38 applications are in varied risk-based assessment steps in the DIRA process and could receive the identity assurance level 2 designation, further adding to the number of applications with taxpayer data that need better security. Given the previously stated timeline for the tests, the decisions that will follow, and the unknown implementation date for the modernized solution, we are concerned about the length of time the IRS will be operating with the existing levels of assurance for the applications that taxpayers will access to accomplish online business. In addition, the length of time could be further extended because of preparation for and operation during the upcoming filing season.

3) CSP limitations – The current CSPs have limited access to identity information that can be used to identity proof taxpayers or tax professionals because it is either owned by the States, which are protective of their residents' information, or owned by other Federal identity credential issuers, such as the Department of State for passports and the Department of Defense for the military. IRS personnel stated that they were not planning to work directly with the 50 States to obtain access to identity data but will leverage external CSPs and their access to State data.

   We examined NIST guidelines to determine what tasks a CSP must perform to successfully identity proof an applicant who wants access to Government digital services or benefits. There are three phases – resolution, validation, and verification – along with

tasks for each phase that are to be completed for successfully identity proofing an applicant. Figure 13 outlines the phases and tasks.

Figure 13: NIST Guidelines for a CSP to Successfully Identity Proof Applicants

Resolution	Validation	Verification
1.a. The CSP collects Personally Identifiable Information from the applicant, *i.e.*, name, address, date of birth, e-mail, and telephone number.	2.a. The CSP validates the information supplied in 1.a. by checking an authoritative source. The CSP determines that the information supplied by the applicant matches the authoritative source's records.	3.a. The CSP asks the applicant to take a photo of themselves, with liveness checks, to match the license and passport.
1.b. The CSP collects two forms of identity evidence, *i.e.*, a driver's license and a passport. For example, using the camera of a laptop, the CSP can capture a photo of both sides of both pieces of identity evidence.	2.b. The CSP checks the images of the license and the passport and determines that there are no alterations, that the encoded data matches the plain-text information, that the identification numbers follow standard formats, and that the physical and digital security features are valid.	3.b. The CSP matches the pictures on the license and the passport to the applicant's picture and determines that they match.
	2.c. The CSP queries the issuing sources for the license and passport and validates that the information matches.	3.c. The CSP sends an enrollment code to the validated telephone number of the applicant; the applicant provides the enrollment code to the CSP; and the CSP confirms they match, verifying that the applicant is in possession and control of the validated telephone number.
		3.d. The applicant has been successfully proofed.

Source: NIST Special Publication 800-63A.

Given the phases previously outlined for the CSPs, the number of users who annually access the identity assurance level 2 designated applications, and the extensive amount of Personally Identifiable Information that has been stolen because of breaches in the public and private sector, we are concerned with the IRS's ability to identity proof all taxpayers' identities when they use online services. The IRS stated that it is unable to cover everyone throughout the country and would have to perform demographic analyses to identify coverage gaps and how to expand its efforts to meet those gaps. Because of the expressed coverage limitations, we believe the IRS will need Federal and State Government assistance, through a CSP, for identity proofing its taxpayers and tax professionals.

The Federal Government and the States are coordinating their efforts to improve the reliability and accuracy of State-issued identification documents through the *REAL ID* effort; however, the thrust for that effort is law enforcement related. Identity proofing for access to IRS public-facing applications to accomplish online business is currently not considered to be law enforcement related. We reviewed the law that supports the

REAL ID effort and noted that, if the provision to provide electronic access to all other States' information contained in the motor vehicle database could be expanded to include Federal bureau electronic access, identity proofing for the IRS's identity assurance level 2 public-facing applications could be addressed.

4) Implementing requirements of the Office of Management and Budget memorandum – In May 2019, the Office of Management and Budget issued Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, updating guidance for efficient operations to identify, credential, monitor, and manage users that access Federal resources. It includes responsibilities for designated agencies, *i.e.*, the Department of Commerce and the General Services Administration, to improve the management and use of digital identity. Specifically, the responsibilities include publishing and maintaining roadmaps with timelines and milestones to develop criteria for and determine the feasibility of establishing or leveraging a public or private sector capability for accrediting products and services. The completion of these responsibilities was due in November 2019, and they will likely result in additional actions to be taken.

   When applying the memorandum to the Secure Access Digital Identity platform, the IRS believes the memorandum will not change its path forward but lessens the risk in selecting credentialed CSPs because of the designated agencies' involvement in properly accrediting the CSPs. We concluded that, because the designated agencies will need to first determine the feasibility of establishing or leveraging public or private sector capabilities and issue further guidance, identifying the CSPs for agency consideration may not occur until a future time.

The IRS is aware of the challenges and is carefully considering them as well as other security measures while developing Secure Access Digital Identity for identity proofing and authenticating taxpayers who want and need access to their data stored in IRS systems. However, it will not be a quick fix, and the IRS will continue to use compensating controls based on superseded NIST guidelines for the [redacted].

In our audit of the CDM project, the IRS reported that it successfully completed key milestones for the first of two CDM project implementation waves. While the Department of Homeland Security[86] did not establish due dates for the program phases, CDM project management organized the Phase I implementation into two waves. The first wave, completed in July 2018, entailed installing sensor tools to identify authorized hardware and software assets and ensure that they are properly configured with vulnerabilities mitigated. According to the IRS, the second wave of Phase I will involve continued efforts to improve data accuracy and deploy the remaining capabilities. Activities involved in the second wave include device boundary and assignment integration, upgrades to CDM project tools, and organizational readiness. IRS CDM project management initially estimated the second wave of Phase I would be complete by December 31, 2019, but was changed to May 1, 2020, to avoid risk to the filing season operations.

We determined that the IRS's CDM data quality has improved, but performance metrics have not been fully implemented. In June 2019, we requested the plan used to manage the CDM

[86] In Calendar Year 2013, the Department of Homeland Security established the CDM program as an implementation approach for continuously monitoring information systems.

project data consistency effort. CDM project management explained that they had not developed an IRS-specific plan and were relying on the Department of Homeland Security's *Continuous Diagnostics and Mitigation Data Consistency Management Guidance*.[87] It provides guidance to agencies and integrators[88] intended to resolve and prevent further data consistency concerns. The guidance also provides 11 data consistency problems reported by integrators and 18 data consistency concerns reported by agencies, of which the IRS had five[89] and 10[90] of the same concerns, respectively.

We requested evidence of the performance measures or metrics used by the CDM project to monitor implementation progress. However, the IRS was unable to provide adequate support. For example, we received a spreadsheet developed by a contractor that appears to provide relevant status information and data totals for each CDM project sensor tool. CDM project management explained that this spreadsheet was only used one time to determine if data were adequately flowing through the process from the sensor tools. The CDM project did not incorporate the spreadsheet as a tool to be used to manage or monitor implementation progress on an ongoing basis. The IRS did provide evidence for the testing of sensor tools.

After we presented our findings to management in November 2019, the IRS provided documentation as evidence of baselines and performance metrics. Documentation included a draft Data Consistency and Quality Plan,[91] which explains the methodology for data consistency and quality review; a data consistency briefing document,[92] which describes the methodology, tools, metrics, and target data quality goals; and a spreadsheet,[93] which describes the monitoring of the data quality results. CDM project management stated that these metrics were recently implemented and were considered to be still evolving in an effort to improve the data quality presented on the Treasury Department dashboard.

Further, the Treasury Department dashboard presents the Agencywide Adaptive Risk Enumeration risk indicator score. This score measures basic elements of an organization's cybersecurity posture, including unauthorized hardware, software vulnerabilities, and configuration management. The risk indicator score does not reflect risk acceptance or other technical mitigation. It provides a raw score for an asset. The IRS risk indicator score improved from 5.27 to 0.30 per device from March to June 2019. Contributing factors to the improvement of the risk indicator score were the removal of duplicate devices and device patching activities. While the IRS is working with the Agencywide Adaptive Risk Enumeration risk indicator score checklist to identify opportunities to continue score improvement, it has yet to develop an acceptable target score. CDM project management stated that the Department of Homeland Security has not established targets for CDM project data consistency. For example, we were unable to determine the effectiveness of the IRS CDM project implementation because no

[87] Dated March 28, 2019.
[88] The March 2019 Department of Homeland Security CDM Agency Dashboard Concept of Operations identifies Booz Allen Hamilton contractor employees as "integrators" to provide support for implementing a common set of CDM project capabilities.
[89] These concerns include increased network device count (because network switches register each device address on the switch as a separate uniquely identified device) and incomplete hardware and software asset management and vulnerability scanning tool deployments resulting in incomplete data integration and reporting visibility.
[90] These concerns include misidentified or inaccurately categorized assets, inaccurate or not current asset records, and undefined data consistency monitoring standards.
[91] Dated August 27, 2019.
[92] Dated October 6, 2019.
[93] Dated November 6, 2019.

performance measurement tools were developed or implemented that might be used to gauge the current progress of the data consistency effort. Without established performance metrics or measurement tools, management is unable to determine the project's status or improvement over time. Without this information, management risks errors in decision-making while implementing the project.

In our network user and device authentication audit, we determined that Unified Access project management did not comply with the ELC methodology. In February 2015, the project manager signed a Project Tailoring Plan[94] agreeing that the project would follow the ELC methodology's commercial off-the-shelf software development path. In November 2017, when the ISE software product was initially deployed into production to enforce user and device authentication, the Infrastructure Executive Steering Committee had performed and approved only the Project Initiation phase[95] Milestone Exit Review. A Milestone Exit Review is a mandatory review performed by the project team and IT organization management when a project reaches each milestone. The outcome of the review is a go/no-go decision that is documented with an unconditional approval, conditional approval, disapproval, or recommendation to suspend or to terminate the project. The remaining Milestone Exit Reviews were not completed for the Domain Architecture, Preliminary Design, Detailed Design, System Development, and System Deployment phases. The team also had not completed the required ELC methodology artifacts for requirements, design, security, contingency planning, and testing. The security artifacts that were not completed included the Systems Security Plan and the Information Systems Contingency Plan.

The project manager explained that a June 2016 memorandum issued by User and Network Services function management gave the authority to deploy the ISE into the production environment in monitor (read-only) mode. The memorandum explained that a production initial operation capability would be permitted prior to completion of the ELC process; however, the project team would need to complete all necessary ELC methodology requirements and milestones prior to full deployment of a Unified Access–Network Segmentation[96] solution. When User and Network Services function management allowed the Unified Access project to deploy in monitor mode in June 2016 prior to completion of all ELC requirements, they accepted the unknown security risks. According to the memorandum, this authorization was to end when the project transitioned to enforcement mode[97] or by December 31, 2017.

In our RPA audit, we found that a suitable development methodology has not been implemented for automation projects. When the IRS began exploring the use of RPA and Intelligent Automation solutions, program management decided that the software development of the Contractor Responsibility Determination Robot (CR BOT) would follow the ELC methodology. Although the software development ultimately did not follow this methodology, program management ensured that User Acceptance Testing was performed prior to deployment. The purpose of the User Acceptance Testing was to test functionality to ensure that contracting officers and contract specialists received accurate output from the CR BOT for each transaction. From the testing performed, we concluded that key requirements were

[94] Adapts the ELC methodology to the unique and specific needs of the individual project or release.
[95] The Project Initiation phase involves defining project scope, forming the project teams, and beginning many of the ELC artifacts.
[96] This refers to the closely related Network Segmentation project. For ELC methodology compliance purposes, the Unified Access project and the Network Segmentation project were initially managed together; however, as of August 2017, these efforts were separated into two separate projects.
[97] Enforcement mode was initiated in November 2017 and completed in December 2019.

incorporated and tested, and the results were documented showing the resolution of any exceptions.

In January 2020, RPA program management decided that, based on their experience with developing the CR BOT, the existing ELC methodology was not applicable or suitable for developing and deploying automation projects. However, the IRS outlined its plans for improving automation project deliverables to include documenting the project's process definition, development specification, and test plan and results as well as deployment, operations, and maintenance. According to the IRS, its ongoing automation projects are in the process of using these deliverables and updating them based on learning and feedback. Finalizing a well-defined automation project development methodology should help to ensure that business requirements are captured, privacy and security requirements are addressed, designs fully satisfy business requirements, solutions are properly tested and deployed in a controlled manner, and operations are closely monitored. However, as of July 2020, program management had not implemented a suitable development methodology.

Cost management

To use public funds effectively, the Government must employ effective management practices and processes, including the measurement of program performance. In addition, Government officials and the public want to know whether programs are achieving their goals and what their program costs are. A cost estimate is the summation of individual cost elements, using established methods and valid data, to estimate the future costs of a program. Developing reliable cost estimates is crucial for realistic program planning, budgeting, and management. Without this ability, agencies are at risk of experiencing cost overruns, missed deadlines, and performance shortfall. Further, cost overruns may cause the Government to reduce funding for other programs, which affects their results or timely execution.

In Fiscal Year 2020, TIGTA provided coverage of cost management in two audits. We initiated an audit[98] to assess the IRS's efforts to identify and replace its legacy systems. We determined that system-level cost data are insufficient to support legacy modernization decisions. According to the *IRS Integrated Modernization Business Plan,* the IRS reported that the costs of maintaining its current technology continues to grow every year at an unsustainable rate. In Fiscal Year 2019, the IRS spent over $2.86 billion to operate its current information technology infrastructure, nearly $2.04 billion (71 percent) of which was on operations and maintenance. If current trends continue, spending is expected to increase to over $3 billion annually by Fiscal Year 2026. The IRS also reported that the cost of operating these systems is overtaking other important components of effective tax administration and limiting its capacity to deliver quality service to taxpayers. Modernization is necessary to curtail these rising costs.

To determine the operations and maintenance costs associated with each legacy system, we obtained Fiscal Year 2019 cost data from the Integrated Financial System, the administrative accounting system used by the IRS, for 127 information technology investments. The operations and maintenance costs are further categorized by up to 18 different types of expenses, *e.g.*, contractor, labor, and operational travel.[99] For example, in Fiscal Year 2019, the IRS spent approximately $5.2 million on contractors and $9.1 million on labor for operations and maintenance of the Individual Master File legacy system. However, we found that, while some

[98] TIGTA, Ref. No. 2020-20-044, *Legacy Systems Management Needs Improvement* (Aug. 2020).

[99] The IRS also captures the same types of expenses, as applicable, for development, modernization, and enhancement costs for each information technology investment.

information technology investments can also be systems like in our example, the IRS generally does not capture operations and maintenance costs at the system level or at the subsystem level.[100] As a result, the IRS does not have enough detailed cost data that can be used in its decision-making processes to prioritize the modernization of its legacy systems and subsystems. Of the nearly $2.04 billion spent on operations and maintenance during Fiscal Year 2019, the IRS spent nearly half, $950 million, on three general information technology investments.

- End User Systems and Support ($176 million) – Provides desktops, laptops, mobile devices, asset (hardware and software) management program oversight, and incident management services to all IRS end users.
- Mainframes and Servers Service Support ($493 million) – Provides design, development, and deployment of server, middleware, and large systems and enterprise storage infrastructures, including databases, operating systems, and software for these platforms. This information technology investment category includes operations and maintenance funding for legacy systems.
- Telecommunication System Support ($281 million) – Provides data network infrastructure, engineering, voice, and video services throughout the IRS.

These costs are not allocated specifically to the information technology investment or system level. These costs are considered fixed costs spent on the operation of the IRS's information technology infrastructure. However, from these funds, we were able to determine that the IRS spent approximately $142 million on operations and maintenance costs for 52 of the 231 systems we identified as legacy. For the remaining 179 systems, we were unable to determine the amount spent on their operations and maintenance based upon the limited cost data available. We believe that this lack of sufficient and detailed cost information hinders the IRS's ability to make informed decisions and prioritize its legacy system modernization efforts.

In our RPA audit, we found that the true cost of RPA projects cannot be determined without detailed cost information. We requested the IRS's Fiscal Years 2019 and 2020 budget and expenditure data for the RPA program. The data included overall program start-up costs as well as the development costs of the CR BOT[101] and the Question and Answer Chatbot.[102] Based on our review of RPA program costs, we observed that the program generally does not fully allocate the direct and indirect costs for each automation project. For example:

- For the CR BOT, the IRS hired a contractor to help develop and deploy this technology solution into production. The direct costs of $376,450 charged by the contractor were paid out of the IT organization's overall Fiscal Year 2018 budget and were not reflected in the RPA program's expenditures. Further, no other direct or indirect costs incurred were allocated to the CR BOT.
- For the Question and Answer Chatbot, this project did not incur any direct costs, as the labor hours for its development were absorbed by the User and Network Services function and any indirect costs were not included in the RPA program's expenditures and allocated to the Question and Answer Chatbot.

[100] Component of an application or system.
[101] Because the CR BOT was the first automation project, the initial funding for this project was included in the IT organization's Fiscal Year 2018 overall budget.
[102] The Question and Answer Chatbot provides employees with an interface that answers their questions about Windows 10 functionality.

- The IRS also used Fiscal Years 2019 and 2020 funds to initiate the development of five additional automation projects, such as a robot to automate the Offers in Compromise payment process in the Small Business/Self-Employed Division and a robot to automate the e-mail referral processing in the Tax Exempt and Government Entities Division.

The IRS explained that the cost structure establishing the RPA program will look different from the cost structure when the program is more mature at full operations. According to RPA program management, as the program matures, they intend to allocate the costs associated with each project to the extent practical. Notwithstanding, the IRS believes that each automation project should be assessed on its cost, the risks mitigated, and the benefits realized. The allocation of all program and project costs will better allow for later comparison of outlaid costs to calculated benefits. If the IRS does not fully allocate both the direct and indirect costs of its RPA and Intelligent Automation projects, it cannot show the return on investment and effective stewardship of taxpayer funds.

Data management

Data management is the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively. The goal of data management is to help people and organizations optimize the use of data within the bounds of policy and regulation so that decisions can be made and actions taken that maximize the benefit to the organization.

In Fiscal Year 2020, TIGTA initiated an audit[103] to evaluate the accuracy of Currency Transaction Report (CTR)[104] data in IRS systems. We found that IRS systems display incorrect CTR amounts. The IRS was originally responsible for the collection of the CTR information, but in 2012, this responsibility was transferred to the Financial Crimes Enforcement Network, established by the Treasury Department to provide a Governmentwide, multisource financial intelligence and analysis network. The IRS now obtains the CTR data by accessing a Financial Crimes Enforcement Network server, where files are placed on a daily basis for downloading by outside agencies, including the IRS. After CTR data are downloaded, IRS programs transmit the data to other IRS systems, *e.g.*, the Information Returns Master File. Prior to 2013, CTR forms were filed on a transaction-by-transaction basis, with a dollar amount recorded for each transaction. In 2013, multiple CTR records could be batched into a single record that included an individual transaction amount and a form total amount.

The IRS has experienced technical difficulties with importing the Financial Crimes Enforcement Network data following the change to batched CTR records. Specifically, the IRS's data translation process transmits the CTR form total rather than the transaction total from the Web Currency and Banking Retrieval System to the Information Returns Master File when multiple transactions are reported on a single CTR form, resulting in millions of overstated transactions. For Calendar Years 2015 to 2017, IRS systems overstated CTR cash-in amounts totaling approximately $10 trillion and cash-out amounts totaling approximately $266 billion.[105] This inaccurate information was included in IRS systems, including the Integrated Data Retrieval

[103] TIGTA, Ref. No. 2020-30-055, *The Accuracy of Currency Transaction Report Data in IRS Systems Should Be Improved to Enhance Its Usefulness for Compliance Purposes* (Sept. 2020).
[104] A report used by financial institutions to report transactions of more than $10,000 conducted by, or on behalf of, one person as well as multiple currency transactions that aggregate to be more than $10,000 in a single day.
[105] Financial Crimes Enforcement Network defines cash-in and cash-out as a transaction or series of transactions in currency into and out of, respectively, a financial institution involving more than $10,000 conducted by or on behalf of the same person on the same business day.

System, preventing IRS examiners and workload planning functions from using the data to select and examine tax returns with cash transactions that may indicate underreported income.

In August 2019, the IRS issued an interim guidance memorandum to clarify actions examiners must take to analyze and document CTR data during an audit. The memorandum cautioned that CTR data on some IRS systems contain minimal information and the total reflected could be an aggregate of several unrelated transactions. Therefore, examiners must complete a form to request a full copy of CTR data. In May 2020, an IRS work request was approved requesting programming changes to ensure that multiple transactions recorded on a single CTR are correctly attributed to the respective transaction subject. The proposed implementation date for the changes is September 2021.

We also found that the IRS currently has limited processes in place to validate the quality and reliability of the data imported from the Financial Crimes Enforcement Network. Specifically, we found that some CTRs potentially from earlier calendar years are recorded as current year transactions in the IRS's databases. This resulted because the IRS performs limited validation on data (consisting of confirming that the CTR contains a Taxpayer Identification Number, name, and dollar amount) it receives. For example, the oldest currency transaction date for Calendar Year 2015 was August 25, 1950.

In addition, the IRS does not perform record count checks or other procedures to verify that all transactions are properly imported. During our review, we compared the total number and amounts of the CTRs contained in the Financial Crimes Enforcement Network and in IRS system databases for Calendar Years 2015 to 2017 and found 446,399 CTRs from the Financial Crimes Enforcement Network database that were not in the IRS's system databases. Further, the IRS does not include all useful data fields for use in its systems. The primary reason is that the IRS used data fields designed to import data for multiple tax forms, including the Form 1098, *Mortgage Interest Statement*, the Form 1099 series, as well as several other forms, and repurposed the data fields to import CTR data. However, not all CTR fields were viewable in IRS systems. Some examples of missing fields that could be useful include the type of CTR (initial/amended), alternate name/business name, and bank account numbers. As a result, the IRS may not have sufficient information to identify potential tax noncompliance and conduct quality examinations because incomplete currency transaction data from Financial Crimes Enforcement Network are imported into IRS systems.

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.

In Fiscal Year 2020, TIGTA and the GAO provided coverage of risk management in three audits. In our audit of wireless networks, we found that security weaknesses related to wireless networks are not always timely resolved. We reviewed the POA&M documents associated with weaknesses in the IRS's wireless networks and determined that 25 open POA&Ms were created between February 2017 and December 2019, with scheduled completion dates between February 2018 and October 2022. Eight (32 percent) of the 25 POA&Ms were beyond the scheduled completion dates, ranging from February 2018 to April 2020. Examples of the security weaknesses include [redacted]

[redacted]. In three of the eight POA&Ms, the Enterprise FISMA Services function personnel recorded updates were untimely. In the remaining five, the POA&Ms have been in progress since June 2018. When we discussed the eight POA&Ms with User and Network Services function management responsible for the technical support for the wireless networks, management was able to provide us with evidence to support that each POA&M was being addressed.

For the remaining 17 POA&Ms, User and Network Services function management stated that nine have been addressed, but the POA&Ms have not been closed. The evidence that supports the POA&Ms' closures has been provided to the appropriate User and Network Services function personnel for uploading to the Treasury FISMA Inventory Management System for subsequent testing and closure approval. Because this information was provided to us as we completed our audit work, we did not evaluate the evidence to determine whether the proposed closure actions would effectively address the security weaknesses. For the remaining eight POA&Ms, the IRS is still working to resolve the weaknesses by requesting evidence and clarification from other User and Network Services function offices.

A cornerstone to developing a sound information security program is the timely identification and resolution of information security weaknesses. Failure to resolve existing wireless network security weaknesses in accordance with IRS and NIST requirements compromises the security posture of the system. This could lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and exploitation, which compromise the integrity, confidentiality, and availability of the system.

In our audit of mainframe systems, we found that the IRS did not document two risk-based decisions when security controls or requirements could not be met. Specifically, the IRS was unable to perform [redacted]. When asked if a risk-based decision existed for this issue, the Enterprise Vulnerability Scanning Office stated that there was none. Following our discussion, the Cybersecurity function initiated a management action by developing the risk-based decision, which was approved on May 6, 2020. For the second issue, the IRS was unable to protect its IBM mainframe platform from malicious code. Cybersecurity and Enterprise Operations function management stated that there was no requirement for a risk-based decision regarding this deviation from policy because another internal security policy included an exception that this requirement is not applicable if the mainframe has no function or capability for providing malicious code scanning or protection. However, during a follow-on conversation, management from the Cybersecurity function's Architecture and Implementation Division agreed to update a previously approved 2015 risk-based decision related to this finding and route for approval.

By not adhering to the risk-based decision process, critical infrastructure and information technology assets may not be properly protected from external attacks or potential insider threats. Without explicit, well-informed, risk-based decisions, IRS leadership may be uninformed of security risks posed by these information systems.

In its audit of the IRS's information system security controls, the GAO reported two deficiencies related to risk management. The IRS did not:

- Have properly authorized Authorization to Operate memoranda or applicable documents signed by appropriate officials for accepting risks of external systems.
- Always follow its risk-based decision request procedures.

Implementation of corrective actions

Internal controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are being achieved. Internal controls protect assets, detect errors, and prevent fraud. Internal controls help Government program managers achieve desired results through effective stewardship of public resources. Systems of internal control provide reasonable assurance that the following objectives are being met: 1) effectiveness and efficiency of operations, 2) reliability of financial reporting, and 3) compliance with applicable laws and regulations.

In Fiscal Year 2020, TIGTA and the GAO performed six audits with coverage on whether the IRS's closed PCAs have been fully implemented and documented. In our audit of PCAs, our review focused on a judgmental sample of 24 PCAs from a population of 83 PCAs closed as implemented or canceled by the IT organization during Fiscal Years 2017 and 2018. Of the 24 PCAs, we selected 15 PCAs closed as implemented to assess the closure process and the effectiveness of the corrective actions taken, and we selected all nine PCAs closed as canceled to assess the closure process for canceling these PCAs. Our review of the nine PCAs closed as canceled determined that they were properly approved and adequately documented via the required Form 13872. Specifically, both an IRS and TIGTA executive approved the cancellation of these PCAs.[106]

Our analysis of the 15 judgmentally sampled PCAs reported as closed determined that the IRS fully implemented 11 of them.[107] Of these 11 PCAs, seven were effective in correcting the identified deficiencies. For the remaining four PCAs, we were unable to test for effectiveness due to the nature of the corrective actions, such as conducting a feasibility analysis,[108] updating the methodology section of a document, *etc*. However, our analysis also determined that the IRS did not fully implement four (27 percent) of the 15 closed PCAs reviewed. All four PCAs were partially implemented to address portions of the identified deficiencies.

For example, TIGTA originally found deficiencies on [redacted] related to [redacted] for [redacted]. The IRS agreed to implement mitigating controls for [redacted] that are [redacted] and stated that it has controls in place to include the annual recertification process. Enterprise Operations function management provided two standard operating procedures, [redacted] *Management Certification Process Standard Operating Procedures* and *Requesting* [redacted] *Standard Operating Procedures*,[109] documenting the annual [redacted] process and the creation of [redacted]. They also provided examples of two revalidation [redacted] reports detailing the status of the annual recertification of [redacted] for May and June 2019. Due to the large

[106] The JAMES audit coordinator and an IRS approving official did not sign two of the nine Forms 13872. TIGTA did not consider this material because of subsequent documentation provided showing that an IRS and TIGTA executive approved the cancellation of both PCAs.

[107] Two of the 11 PCAs were fully implemented after their PCA closure dates. For one PCA, Enterprise Services function management stated that, while one of a three-part corrective action was completed and the other two components were started, they did not realize that all three components must be completed fully prior to the closure of the PCA. All components of the PCA were subsequently completed after the closure date. For the second PCA, Applications Development function management stated that, while they updated documents with the validation of service account information, they did not realize until after closing the PCA that the updated documents were not the appropriate place to add that information. The appropriate documents were subsequently updated after the PCA closure date.

[108] An analysis that establishes whether conditions are right to implement a particular project.

[109] Dated March and June 2019, respectively.

number of [redacted], the Enterprise Operations function allocates a proportionate number of [redacted] each month to be revalidated for the annual recertification process. Our analysis of the June 2019 report determined that there were gaps in the revalidation. Of the 144 [redacted] listed, only [redacted] was revalidated. In addition, of the 16 [redacted] after the December 21, 2016, PCA closure date, 10 were never revalidated during the annual recertification process.[110] As a result, we determined that this PCA was partially implemented; however, the corrective actions taken were not fully effective.

In another example, TIGTA originally found that reported vulnerabilities were not timely remediated on file transfer servers. The IRS stated it has an enterprise-wide process in place to continuously and timely implement patches to the information technology infrastructure and will follow this process to ensure that patches are applied to file transfer servers, including those located in the Demilitarized Zone, within established time frames. The IRS stated it would also verify that patching for file transfer servers has been applied. Enterprise Operations function management provided two documents, *Server Patch Management Standard* and *Patch Implementation Standard Operating Procedures*,[111] that provide the procedures to continuously and timely implement patches to the information technology infrastructure. In addition, they provided customized patch reports, as of October 2019, to support that patches were installed to file transfer servers, including those located in the Demilitarized Zone, within established time frames. However, the patch reports also showed that some patches were not timely installed to some file transfer servers in the Demilitarized Zone. To illustrate, the IRS did not install all seven critical vulnerability patches within 30 calendar days as required (averaging 216 calendar days). The IRS also did not install 20 (10 percent) of the 199 important/high vulnerability patches within 90 calendar days as required (averaging 157 calendar days). As a result, we determined that this PCA was partially implemented; however, the corrective actions taken were not fully effective.

In our active directory audit, we found that the Active Directory Technical Advisory Board generally implemented TIGTA's recommendations.[112] In June 2018, the IRS agreed to review the scope of the advisory board's defined oversight responsibilities and modify it as necessary to ensure that the advisory board is providing enterprise-wide oversight of the active directory architecture, including the active directory forests that operate outside of the Enterprise Operations function. Further, the IRS agreed to update its Active Directory Technical Advisory Board charter and ensure that all individual forest owners are appropriately represented on the advisory board. In March 2019, the advisory board updated the charter to align its responsibilities with its activities as well as added voting and non-voting members, ensuring that all active directory forest owners are represented on the board.

In our audit of audit trails, we determined that the IRS fully implemented the PCAs for five of six TIGTA recommendations[113] to address audit trail deficiencies.[114] For example, we recommended that the CIO should ensure that the Associate CIO, Cybersecurity, revise the program-level

[110] The remaining six [redacted] were not applicable because they were recently [redacted] in June 2019 and a revalidation was not yet required.
[111] Both documents are dated May 2019.
[112] TIGTA, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018).
[113] TIGTA, Ref. No. 2015-20-088, *Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected* (Sept. 2015).
[114] The IRS did not fully implement its PCA for our recommendation that systems owners create a POA&M for all identified information technology security weaknesses, including audit trail deficiencies.

memorandum to clearly state that responsibility for audit trail controls revert to the system owner once the ESAT Office has approved the audit plan. We reviewed the *FISMA Security Controls Assessment Standard Operating Procedures*[115] and verified that the recommendation was fully implemented. In another example, we recommended that the CIO should ensure that the Cybersecurity function's Security Risk Management Office, which performs annual testing of security controls, ensures that testers are instructed to appropriately test audit trail controls and report the identified deficiencies. We reviewed the ESAT Office procedures, and they require that application *Audit Control Response* deficiencies are provided to the Cybersecurity function's Security Risk Management, Enterprise FISMA Compliance Office. The Cybersecurity function team will schedule the deficiencies for assessment in the next FISMA cycle, at which time either the deficiency will be discarded or a security assessment report will be provided. If an assessment report is provided, the deficiency is updated to a finding and a POA&M is required. To confirm implementation of these procedures, we verified that the IRS selected and reviewed controls, including audit controls, as part of our FISMA Fiscal Years 2018 and 2019 reviews.

In our audit of the ECM, we found that one of two PCAs from our July 2018 ECM audit[116] was not fully implemented and supported. We recommended that the CIO ensure that the ECM solution will enable the IRS to consolidate the majority of the legacy case management systems. The IRS stated that the PCA was implemented and closed as of August 8, 2019. However, our analysis determined that the completion of the PCA was not fully supported in the JAMES. We found that the IRS documentation included only minimal details, and it was not supported by detailed technical documentation to adequately support the solution's ability to consolidate the majority of case management systems. In addition, the ECM program is still in progress, and not all phases of the migration program are complete. Missing or incomplete details regarding solution capabilities and performance create risks to achieving the IRS's case management consolidation vision.

We also recommended that the CIO ensure that base and mission-critical ECM program requirements are determined and program-level activities are completed prior to the technical solution procurement. We reviewed the information uploaded in the JAMES and determined that the IRS supporting activities, *e.g.*, draft product assessment detailing IRS partner engagement to identify base and mission requirements and draft Request for Quotation to identify requirements for the ECM solution, relate to aspects of the identification of base and mission-critical requirements and meet the intent of our recommendation.

The GAO initiated an audit[117] to determine whether IRS financial statements are fairly presented and IRS management maintained effective internal control over financial reporting. The GAO reported that the IRS did not correct its reported control deficiencies as of September 30, 2018, concerning unnecessary access rights granted to accounts, inconsistent monitoring of systems and accounts, out-of-date and unsupported hardware and software, change controls over tax and financial management processing on the mainframe, and developing and implementing effective policies and procedures as part of the IRS's security management program.

In its audit of the IRS's information system security controls, the GAO followed up on the status of the IRS's corrective actions to address deficiencies in information system security controls

[115] Dated April 3, 2018.
[116] TIGTA, Ref. No. 2018-20-043, *Initial Efforts to Develop an Enterprise Case Management Solution Were Unsuccessful; Other Options Are Now Being Evaluated* (July 2018).
[117] GAO, GAO-20-159, *Financial Audit: IRS's Fiscal Year 2019 and Fiscal Year 2018 Financial Statements* (Nov. 2019).

and associated recommendations that remained open as of September 30, 2018. The IRS informed the GAO that it had implemented corrective actions to address deficiencies associated with 14 of the 127 recommendations resulting from prior GAO audits as of September 30, 2019. However, during a Fiscal Year 2019 audit,[118] the GAO determined that the IRS's actions had effectively addressed deficiencies associated with only 10 of the 14 recommendations. The GAO also found that the IRS had adequately addressed three of the 113 recommendations that the IRS had not submitted for validation. As a result, the GAO determined that 13 of 127 previously reported recommendations were closed. Combined with the GAO's 18 new recommendations, a total of 132 recommendations to the IRS for addressing deficiencies in information system security controls remain open as of September 30, 2019.

Modernizing operations

Successful modernization of 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 and aged hardware and software, and its use of outdated programming languages, pose significant risks to the IRS's ability to deliver its mission. Modernizing the IRS's computer systems has been a persistent challenge for many years and will likely remain a challenge for the foreseeable future.

In Fiscal Year 2020, TIGTA performed four audits covering the modernization of the IRS's operations. In our audit of legacy systems, we found that specific or long-term plans have not been developed to address updating, replacing, or retiring most legacy systems. When we asked for specific plans to identify, manage, or modernize IRS's legacy systems, IT organization and other business unit and function management stated that, generally, there were no individual plans for all systems at the IRS. IT organization management also stated that, for systems managed by the Applications Development function, modernizing systems is based on business needs and the system capabilities or processes to deliver them, which may or may not include updating, replacing, or retiring legacy systems. However, IT organization management referenced seven various direction and strategy documents that generally guide the IRS's information technology enterprise. Our review of five of the documents, *i.e.*, *Enterprise Technology Blueprint*,[119] *Legacy Code Reduction Strategy*,[120] *Target Enterprise Architecture*,[121] *Portfolio Rationalization*,[122] and *IRS Integrated Modernization Business Plan*, determined that the IRS has initiatives identifying 21 systems for modernization or potential candidates for modernization and 25 systems for retirement.[123]

Our review of the remaining two documents (*IRS Strategic Plan, Fiscal Years 2018-2022*[124] and *IT Vision 2.0*[125]) determined that the IRS did not identify any additional systems for modernization or retirement. According to IT organization management, these two documents,

[118] GAO, GAO-19-473RSU, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (July 2019).
[119] Release 1.1, dated March 31, 2020.
[120] Dated December 13, 2019.
[121] Release 2020, dated September 18, 2019.
[122] Dated March 17, 2020.
[123] Some investments, programs, and systems identified for modernization or retirement may affect associated subsystems. Subsystems were included in our total only if they were specifically identified in the information technology enterprise direction and strategy documents. Duplicate systems identified are counted only once.
[124] Revised April 2018.
[125] Dated January 2018.

which provide the strategy and direction of information technology in support of tax administration, were not meant to identify specific systems for modernization or retirement. In addition, IT organization management stated that, moving forward, *Portfolio Rationalization* will be their primary modernization program for the systems they manage.[126] They further stated that the collective initiatives focus on incrementally modernizing IRS capabilities and systems in batches; together with the *Portfolio Rationalization* program, these initiatives are expected to eventually provide and develop specific plans.

Aside from the systems specifically identified in the *Portfolio Rationalization* document, the *Portfolio Rationalization* team also maintains a "backlog" of initiatives, identifying an additional 24 systems for potential modernization and nine systems for retirement if resources and funding become available. However, other than the systems we identified in the five information technology enterprise direction and strategy documents and as part of the *Portfolio Rationalization* program "backlog" of initiatives, the IRS does not currently have any specific or long-term plans to either update, replace, or retire its remaining legacy systems in operation.

Management Action: After the completion of our audit work, IT organization management provided five examples[127] of long-term plans for modernizing legacy systems that were developed as a result of the *Portfolio Rationalization* program's efforts.

In addition, we found that the IRS lacks an enterprise-wide definition that can be uniformly applied to identify its inventory of legacy systems. After much discussion and a request for how TIGTA defines a legacy system, IT organization personnel provided the Treasury Department's definition:

> *…an information system that may be based on outdated technologies but is critical to day-to-day operations. A legacy system, in the context of computing, refers to outdated computer systems, programming languages, or application software that are used instead of more modern alternatives. A legacy system may be problematic, due to compatibility issues, obsolescence, or the lack of support. What is key [sic] is that a legacy system has been identified as strategic, but in need of replacement.*

IT organization personnel subsequently clarified and further defined a legacy system to include application age equal to or older than 25 years, programming languages that are considered obsolete, *e.g.*, Assembler Language Code and Common Business-Oriented Language, and systems meeting other factors such as a lack of vendor support, training, or resources. Applying this definition, IT organization personnel provided a list of legacy systems that they managed as of September 5, 2019.

IT organization personnel also stated that their definition of a legacy system only applied to their organization and that other business units and functions may have different definitions. Consequently, we contacted 20 business units and functions on November 26, 2019, and requested that they provide their definition of a legacy system as well as a current list of systems under their control that met their definition. Ten business units and functions responded that they do not manage any systems. The remaining 10 business units and functions did not have a definition or had varying definitions of a legacy system. For example,

[126] The *Portfolio Rationalization* program does not include systems managed by other IT organization functions or other business units and functions.
[127] These included the Audit Information Management System Related Reports, Combined FedState, Miscellaneous Computations, Reimbursable Accounts Systems, and Remittance Processing System.

business units and functions defined a legacy system as either a system that is in operations and maintenance, development of a system that is older than five calendar years, or partially used the IT organization's definition, *i.e.*, older than 25 years.

Given the number and different IRS definitions of a legacy system, we met with the CIO and other senior IT organization executives. They agreed that the IT organization's definition should be considered the IRS's enterprise-wide definition and used for the purpose of our review. Based upon this information, we applied the IT organization's definition of a legacy system to the IRS's As-Built Architecture[128] to identify all current systems that should be considered legacy. On April 29, 2020, we obtained a list from the As-Built Architecture that showed that there are 669 systems in the production environment. Our review found that 288 (43 percent) systems were missing basic and essential information,[129] *i.e.*, application age and programming language,[130] which prevented us from determining whether the system should be considered legacy. Of the remaining 381 systems, we determined that 231 systems were legacy and 150 were not legacy. Figure 14 provides a summary of the legacy and non-legacy systems by managing organization.

Figure 14: Number of Legacy and Non-Legacy Systems by Managing Organization[131]

Organization Responsible for Managing Systems	Systems Identified As Legacy	Systems Identified As Non-Legacy	Systems Missing Information	Total
IT Organization	204	116	97	417
Business Units	6	2	73	81
Business Unit Not Identified by the IRS	21	32	118	171
Total	**231**	**150**	**288**	**669**

Source: TIGTA's analysis of the April 29, 2020, As-Built Architecture list.

When we compared our list to the IT organization and other business units' and functions' lists of legacy systems, we identified 46 systems as legacy, *e.g.*, Automated Underreporter and the ISRP, that the IRS had not. Conversely, the IRS incorrectly identified the Telephone Routing Interactive System–Integrated Data Retrieval System as legacy that we did not consider legacy based on the IT organization's definition of a legacy system.

To provide additional perspective and the scope of legacy systems in future operations, we further analyzed the data from the As-Built Architecture to determine the number of systems that will become legacy over the next 10 calendar years. Our analysis determined that an

[128] According to IT organization management, the As-Built Architecture is the authoritative source of information for the IRS's systems architecture.
[129] Three hundred and thirty-six systems that were missing information on the application age, the programming language, or both include 236 systems that did not have information on both the application age and programming language as well as 37 systems that did not have the application age and 63 systems that did not have the programming language.
[130] We did not apply other factors, such as lack of vendor support, training, and resources, when defining a legacy system due to variables in subjectivity.
[131] Due to a conflicting understanding of which organization has managing responsibilities for some systems, our analysis was limited to information provided from the As-Built Architecture.

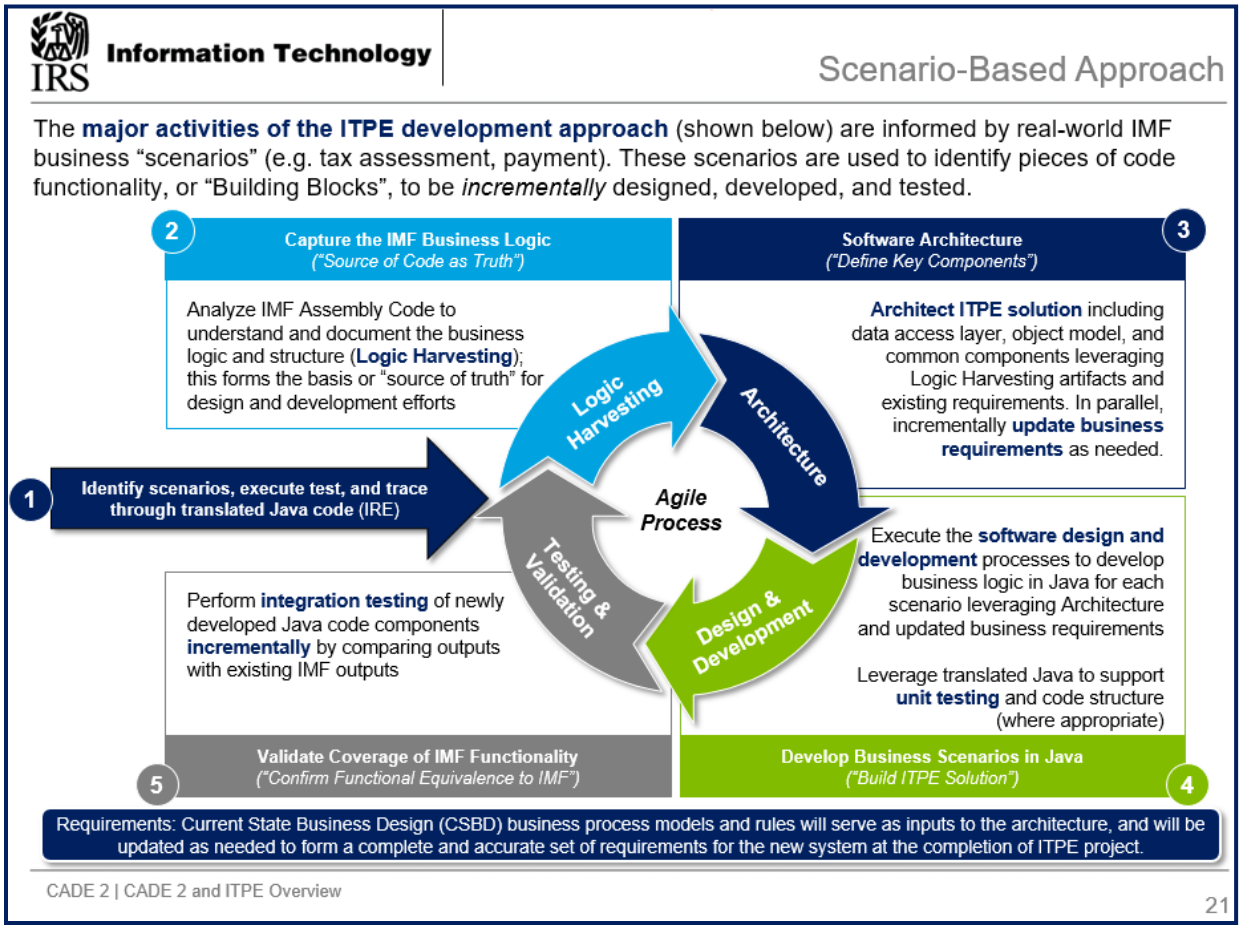
additional 49 systems[132] will become legacy due to meeting or exceeding each system's application age.[133] This will potentially increase the total number of legacy systems to 280 systems if current modernization plans are not fully implemented. If further action is not taken to address the growing number of and reliance on legacy systems, the IRS faces the risk of increasing cybersecurity threats and maintenance costs as more of its systems become legacy.

In our audit of the ECM, we found that the legacy case management decomissioning strategy is not fully developed. However, the ECM program developed a sequencing tool that will help identify and analyze the existing case management processes in legacy systems in order to consolidate and implement these processes into the new ECM solution. The ECM program plans to include legacy systems as a factor in the sequencing decision-making process. The General Services Administration established guidance[134] that directs agencies to develop a decommission plan, which should involve key stakeholders to ensure a coherent strategy for retiring legacy systems. The failure to establish an effective ECM decommissioning strategy could lead to a lack of coordinated technology investments to replace existing legacy case management systems in a cost-effective and efficient manner and could disrupt business processes and taxpayer service as legacy case management systems are migrated to the ECM solution.

In our audit of the Individual Tax Processing Engine project, we found that a scenario-based approach was adopted to convert legacy Assembler Language Code to Java. This approach uses business scenarios based on Individual Master File business transactions to incrementally implement functionality into an end-to-end solution. Figure 15 outlines the IRS's scenario-based approach for the Individual Tax Processing Engine project.

[132] The IT organization manages 46 of these systems, the Wage and Investment Division manages one of these systems, and the IRS did not identify the business unit(s) managing the remaining two systems.
[133] The As-Built Architecture does not always provide a specific application age but rather provides an age range, *e.g.*, 20 – 25 years old.
[134] General Services Administration, *Modernization and Migration Management (M3) Playbook* (Sept. 2018).

Figure 15: Overview of the Scenario-Based Approach



Source: Customer Account Data Engine 2 and Individual Tax Processing Engine Overview, dated July 17, 2019. IMF = Individual Master File. IRE = Individual Master File Reverse Engineering. ITPE = Individual Tax Processing Engine.

In July 2019, we met with the Individual Tax Processing Engine project team for an overview of the project. IRS management stated that they were moving forward with a scenario-based approach for Individual Master File Runs 12 and 15, which are the bulk of tax processing logic. The purpose of using this approach is to facilitate the iterative delivery of the project and improve workflow. We also performed research to determine if other approaches for converting Assembler Language Code to Java should be considered. We found one example of a private sector company successfully performing this conversion. However, the scope of the conversion was 10,000 lines of code in total. By comparison, Individual Master File Runs 12 and 15 alone have approximately 146,000 active lines of code and approximately 961,000 lines of code in total. We determined that the scenario-based approach is effective for the project given the size and complexity. We also found that this approach was consistent with Internal Revenue Manual 2.16.1, *Enterprise Life Cycle*,[135] Agile path development guidance, which includes high-level feature definitions and allows for repetitive cycles of development and testing for a product or new solution.

[135] Dated November 26, 2019.

In addition, we found that the Individual Tax Processing Engine Java code we reviewed with regards to declaration and statement controls aligns with Internal Revenue Manual 2.5.3, *Systems Development, Programming and Source Code Standards,*[136] and industry best practices.[137] The IRS provided 235 Java class files so we could review the new code. We reviewed a judgmental sample of 58 (25 percent) Java class files, totaling approximately 42,000 lines of code, and found that 48 (83 percent) of the 58 files had lines in excess of 100 characters. We also found that five (9 percent) of the 58 files contained more than 2,000 lines. Further, every file reviewed had incomplete or missing opening comments. A detailed comment review determined that all files did not consistently use the beginning comments section of the code as outlined by the Internal Revenue Manual. In our sample review of Java files, we identified 14 files (24 percent) that had a blank comment field with no information. One file (2 percent) had beginning comments with no date or class name listed. Two files (3 percent) had beginning comments that were lacking a class name, version, and date entry. Lastly, 58 files (100 percent) contained beginning comments that did not include a class name. All the files we reviewed did, however, comply with guidelines for Java declaration standards and Java statement standards.

Elements described within the best practice guidelines include, but are not limited to, programmers avoiding files longer than 2,000 lines and breaking lines of code at column 100 to maintain readability as well as beginning code within all source files with a C-style comment that lists the class name, version information, and date. According to the IRS, the existence of Java lines of code in excess of 100 characters and files in excess of 2,000 lines of code as well as the lack of opening comments do not affect the quality of the code or have any affect on the code at runtime, but these deviations from best practices could make future maintenance inefficient.

In our RPA audit, we found that maximizing use of the CR BOT would increase cost savings. The objective of the CR BOT project was to significantly reduce the time it took to manually complete the contractor responsibility determination process for each unique vendor. The determination process collects data from external websites to determine if a vendor has the financial resources and capabilities to perform the proposed work and to confirm that the vendor is eligible to receive an award under applicable acquisition laws and regulations.

The IRS estimated that, by using the CR BOT, it would potentially save 11,250 hours annually when performing contractor responsibility determinations,[138] or approximately $1.35 million per year.[139] To measure the CR BOT's use and subsequent cost savings during its first year of deployment, we obtained, from the IRS, an extract of usage data for May 30, 2019, through May 29, 2020.[140] Similarly, we obtained an extract of 2,774 new IRS-administered contracts signed between May 30, 2019, and June 30, 2020, from the Procurement for Public Sector application.[141] Using the Data Universal Numbering System numbers found in both extracts, we were able to associate unique CR BOT usage to specific contracts. Figure 16 presents the results of our comparison.

[136] Dated March 1, 2007.
[137] Sun Microsystems, *Java Code Conventions* (Sept. 12, 1997).
[138] The IRS estimates that the CR BOT saves 2.5 hours per contractor responsibility determination.
[139] For this calculation, the IRS used an average hourly rate of $120 per labor hour.
[140] The first year of the CR BOT deployment was May 30, 2019, to May 29, 2020.
[141] We included June 2020 in our Procurement for Public Sector application contract data extract as some of the CR BOT usage that occurred in May 2020 would have been for contracts signed in June 2020.

Figure 16: Comparison of CR BOT Usage to Procurement for Public Sector Application Contract Information

Category	Contract Count
CR BOT Usage Matched to a Specific Contract	1,096
Data Universal Numbering System Numbers Matched (However, No Distinct Relationship Between Contract Data and CR BOT Usage for Every Contract)[142]	826
Data Universal Numbering System Numbers Did Not Match (Contract Data Did Not Match Any CR BOT Usage)	792
Restricted Data Universal Numbering System Number[143]	60
Total	**2,774**

Source: TIGTA's analysis of CR BOT usage and Procurement for Public Sector application contract information between May 30, 2019, and June 30, 2020.

Comparing the CR BOT usage data to the Procurement for Public Sector application contract data, we estimate that, for the first year of its deployment, the CR BOT saved the IRS 2,740 hours, which equates to a cost savings of approximately $328,800. However, the number of hours actually saved was considerably less than what should have been saved for the same time frame. If the IRS had maximized contracting officer and contract specialist use of the CR BOT to perform contractor responsibility determinations, the expected hour and dollar savings would have been more fully realized. For example, had the IRS maximized the CR BOT's use on the 1,618 contracts for which manual contractor responsibility determinations were potentially made during the first year of its deployment,[144] we estimate that an additional $485,400 in unnecessary costs would have been avoided. If the IRS maximizes the use of the CR BOT, we estimate that it could potentially save approximately $2,427,000 over the next five years.

[142] This category contains several vendors that had multiple new contracts with the IRS. While some of the CR BOT usage matched directly to specific contracts, there were many more contracts than CR BOT queries to match. As an example, a vendor could have had five new contracts signed throughout our review time frame, but we only found one CR BOT usage that matched up with only one of the contracts based on timing.

[143] When a vendor's Data Universal Numbering System number has restricted public access, the CR BOT will not process the request. The contracting officer or contract specialist will need to manually retrieve the contractor registration information for the vendor. Because the restricted number requires manual intervention, we excluded these vendors from any of our CR BOT usage calculations and projections.

[144] This number includes the 826 contracts for which there was no distinct relationship between contract data and CR BOT usage for every contract and the 792 contracts for which the contract data do not match any CR BOT usage. It does not include the 60 contracts with restricted Data Universal Numbering System numbers.

Appendix I

Detailed Objective, Scope, and Methodology

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

- Obtained information on the IRS's budget and staffing of employees and contractors to provide context on the size of the IT organization.
- Reviewed the Security and Information Technology Services Division's Systems Security, Systems Development, and Systems Operations Directorates' audit reports issued during Fiscal Year 2020. We also analyzed and prepared summaries of the information technology security, systems development, and operations issues.
- Identified and summarized other relevant TIGTA and external oversight assessments dealing with information technology security, systems development, and operations.
- Assessed the security, systems development, and operations issues and determined which are at high risk for failing to deliver IRS program objectives and protect tax administration data.

Performance of This Review

The compilation of information for this report was performed at various TIGTA offices during the period of May through September 2020. The information presented is derived from TIGTA and GAO reports issued during Fiscal Year 2020 as well as IRS documents related to its information technology plans and issues. 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.

Major contributors to the report were Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Bryce Kisler, Director; Louis Lee, Audit Manager; Jason Rosenberg, Lead Auditor; and Dave Allen, Senior Auditor.

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 2020. Therefore, we did not evaluate internal controls as part of this review.

Appendix II

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

No.	Report Reference Number	Audit Report Title	Report Issuance Date
1	GAO-20-159	Financial Audit: IRS's Fiscal Year 2019 and Fiscal Year 2018 Financial Statements	November 8, 2019
2	2020-40-004	Actions Are Needed to Improve the Safeguarding of Taxpayer Information at Volunteer Program Sites	November 13, 2019
3	2020-20-006	Active Directory Oversight Needs Improvement	February 5, 2020
4	2020-20-010	The Enterprise Cloud Program Developed a Strategy, but Work Remains to Achieve Cloud-Based Modernization Goals	March 11, 2020
5	2020-20-013	The Continuous Diagnostics and Mitigation Project Effectiveness Would Be Improved by Better Performance Metrics and Tools Data	March 18, 2020
6	2020-20-012	While Progress Is Being Made on Digital Identity Requirements, Completion Dates to Achieve Compliance With Identity Proofing Standards Have Not Been Established	March 23, 2020
7	GAO-20-411R	Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls	May 13, 2020
8	2020-20-022	Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Fully and Effectively Implemented and Documented	June 1, 2020
9	2020-10-039	The Annual Inventory Certification Process for Non–Information Technology Assets Needs Improvement	July 9, 2020
10	2020-20-033	Most Internal Revenue Service Applications Do Not Have Sufficient Audit Trails to Detect Unauthorized Access to Sensitive Information	July 31, 2020
11	2020-20-036	Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action Is Needed to Verify the Identity of Devices	August 10, 2020
12	2020-20-043	Substantial Progress Has Been Made in Implementing the Insider Threat Capability, but Improvements Are Needed	August 19, 2020
13	2020-20-044	Legacy Systems Management Needs Improvement	August 19, 2020

No.	Report Reference Number	Audit Report Title	Report Issuance Date
14	2020-40-067	Improvements Are Needed to Address Continued Deficiencies in Ensuring the Accuracy of the Centralized Authorization File	September 2, 2020
15	2020-30-055	The Accuracy of Currency Transaction Report Data in IRS Systems Should Be Improved to Enhance Its Usefulness for Compliance Purposes	September 4, 2020
16	2020-20-062	The Individual Tax Processing Engine Project Is Making Progress	September 14, 2020
17	2020-20-061	The Enterprise Case Management Solution Deployment Is Delayed and Additional Actions Are Needed to Develop a Decommissioning Strategy	September 21, 2020
18	2020-20-063	Improvements Are Needed to Ensure That Wireless Networks Are Secure	September 21, 2020
19	2020-20-060	Process Automation Benefits Are Not Being Maximized, and Development Processes Need Improvement	September 25, 2020
20	2020-20-073	Fiscal Year 2020 Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act	September 25, 2020
21	2020-20-045	Mainframe Computing Environment Security Needs Improvement	September 28, 2020

Appendix III

Glossary of Terms

Term	Definition
Active Directory	A Microsoft Corporation software system for administering and securing computer networks. It manages the identities and relationships of computing resources that comprise a network. It also enables administrators to assign enterprise-wide policies, deploys programs to many computers, and applies critical updates to an entire organization simultaneously from a central, organized, accessible database. It simplifies system administration and provides methods to strengthen and consistently secure computer systems.
Adobe Acrobat Trusted Identities List	Provides a repository of trusted certificates, which can be a trusted root or self-signed certificate used for signing or validating documents.
Applicant	An individual who opts to be identity-proofed by a CSP.
Application	A software program hosted by an information system.
Artifact	The output of an activity performed in a process/procedure, which is created throughout the life cycle of a project.
Assembler Language Code	A low-level computer language initially used in the 1950s.
Audit Control Response	Addresses security auditing for the application and its infrastructure to include the operating system, database, and middleware products.
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.
Authenticator	The means used to confirm the identity of a user, processor, or device, *e.g.*, user password or token.
Authorization to Operate	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the United States based on the implementation of an agreed-upon set of security controls.
Blanket Purchase Agreement	An option for Federal agencies and schedule contractors alike, providing convenience, efficiency, and reduced costs. Contractual terms and conditions are contained in General Services Administration Schedule contracts and are not to be renegotiated for Blanket Purchase Agreements. Therefore, as a purchasing option, Blanket Purchase Agreements eliminate such contracting and open market costs as the search for sources, the need to prepare solicitations, and the requirement to synopsize the acquisition.

Term	Definition
Business Unit	A title for major IRS organizations such as the IRS Independent Office of Appeals, the Wage and Investment Division, the Office of Professional Responsibility, and the IT organization.
Change Control	The procedures to ensure that all changes are controlled, including the submission, recording, analysis, decision-making, approval, implementation, and post-implementation review of the change.
Change Management	The process responsible for controlling the life cycle of all changes; it enables beneficial changes to be made with minimum disruption to information technology services.
Change Request	The method for requesting approval to change a baselined product or other controlled item.
Cipher	Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text, or in which units of plain text are rearranged, or both.
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, *e.g.*, network, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Common Vulnerability Scoring System	Provides an open framework for communicating the characteristics and effects 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.
Continuous Diagnostics and Mitigation	Provides tools, integration services, and dashboards to all participating agencies to improve their respective agency security postures to defend against cybersecurity threats and vulnerabilities.
Contract Specialist	Identifies and provides resolution of contracting issues based on the correct interpretation of laws, rules, and regulations.
Contracting Officer	An agent of the Federal Government empowered to execute contracts and obligate Government funds.
Credential	An object or data structure that authoritatively binds an identity – via an identifier or identifiers and (optionally) additional attributes – to at least one authenticator possessed and controlled by a subscriber.
Credential Service Provider	A trusted entity that issues or registers the subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or may issue credentials for its own use.
Criminal Investigation	An IRS business unit that serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.
Customer Account Data Engine 2	Establishes a single database that houses all individual taxpayer accounts, including Individual Master File data, which provides IRS employees the ability to view updated account information online.

Term	Definition
Dashboard	A user interface or web page that gives a current summary of key information, usually in graphic, easy-to-read form, relating to progress and performance.
Data Universal Numbering System	A unique nine-digit identifier for businesses, generally used for credit reporting purposes.
Demilitarized Zone	A network segment inserted as a "neutral zone" between an organization's private network and the Internet.
Detailed Design Phase	Involves the development of an application's physical design and relates to how data are entered into a system, verified, processed, and displayed as output.
Digital Identity Risk Assessment Process	A redesign of the IRS's previous Electronic Authentication Risk Assessment process. This process identifies the risks to system security and determines the probability of occurrence, the resulting affect, and additional safeguards that would mitigate the affect.
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.
Domain Architecture Phase	Involves the development of a business system concept, business system requirements, and business system architecture.
Domain Controller	A server that is running a version of the Windows Server operating system and has Active Directory Domain Services installed.
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.
Enterprise Case Management Physical Assessment and Analysis	A set of activities designed to evaluate vendors' solutions and provide the level of confidence that the selected solution will be viable for the IRS. Activities are designed to ensure that the solution meets selected technical and business objectives of the ECM program.
Enterprise Computing Center	A data center that supports tax processing and information management through a data processing and telecommunications infrastructure.
Enterprise Life Cycle	A structured business systems development methodology that requires the preparation of specific work products during different phases of the development process. The ELC 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.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Financial Crimes Enforcement Network	A bureau of the Treasury Department with the mission to safeguard the financial system from unlawful use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

Term	Definition
Firewall	A gateway that limits access between networks in accordance with local security policy.
Firmware Component	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Forest	A complete instance of an active directory. Each forest acts as a top-level container in that it houses all domain containers for that particular active directory instance.
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 electronic authentication.
High-Value Asset	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical Federal operations or house unique collections of data (by size or content), making them of particular interest to criminal, politically-motivated, or State-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the Government.
Hypervisor	Provides virtualization of hardware that allows multiple guest operating systems to run on a single host computer. It enables shared computing resources, such as processors, memory, networking, and hard drives, between all of the guest operating systems.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Information Returns Master File	Part of the IRS taxpayer batch file that contains all taxpayer information return data extracted from various sources.
Information Security 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.
Information Technology Asset Management Program	A critical function of the IRS's strategy to improve information technology asset operations through enhanced asset discovery and tracking as well as to manage the financial, licensing, and contractual aspects of information technology assets throughout their life cycle.

Term	Definition
Information Technology Organization	The IRS business unit responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Integrated Data Retrieval System	IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.
Integrated Submission and Remittance Processing	A system that converts paper tax and information documents and remittances received by the IRS into perfected electronic records of taxpayer data.
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.
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.
Java	A set of several computer software products and specifications that together provide a system for developing application software and deploying it in a cross-platform computing environment.
Joint Audit Management Enterprise System	The Treasury Department system for use by all bureaus to track, monitor, and report the status of internal control audit results. This system tracks specific information on issues, findings, recommendations, and PCAs from audit reports issued by oversight agencies, such as TIGTA.
Legacy System	An information system that may be based on outdated technologies but is critical to day-to-day operations. In the context of computing, it refers to outdated computer systems, programming languages, or application software that are used instead of more modern alternatives.
Limited Area	An area in a building where access is limited to authorized personnel only. All who access a Limited Area must have a verified official business need to enter. Limited Area space can be identified by the Chief, Facilities Management and Security Services Physical Security Section, based on critical assets.
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.
Liveness Checks	A security feature that can ensure that biological identifiers are from the proper user and not from someone else. Traditional forms of detections can include eye or lip movement analysis, prompted motion instructions, texture/reflection detection in video feeds, or zooming motion detection.
Logical Partition	Segments a high-capacity hardware configuration into multiple independent operating units. Each configuration is a distinct operating environment and may be grouped together, but the configurations need to be reviewed individually because they are often configured differently.
Mainframe Policy Checker	An application that validates applicable policies for the mainframe to configuration settings on the mainframe.

Term	Definition
Mechanism	Logical assembly of components, elements, or parts, and the associated energy and information flows, that enable a machine, process, or system to achieve its intended result.
Media Access Control Address	The hardware identification number that uniquely identifies each device on a network.
Media Access Control Authentication Bypass Protocol	A method for a device that is not capable of communicating with the 802.1X protocol to be authenticated by the ISE to access the internal network. The device's media access control address is entered into the ISE on a "whitelist" so the ISE can recognize and authenticate the non-802.1X protocol–compatible device.
Middleware	A software that functions at an intermediate layer between applications and the operating system and database management system or between the client and server.
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.
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.
Network Adapter	A component of a computer's internal hardware that is used for communicating over a network with another computer.
Online 5081	A web-based application that allows users to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems. The application also allows the IRS to track user access history, generate reports, and document an audit trail of user actions.
Operating System	The software that serves as the user interface and communicates with computer hardware to allocate memory, process tasks, and access disks and peripherals.
Organizational Common Controls Security Plan	Documents the current and planned IRS enterprise-wide–level controls and addresses security concerns that may affect the operating environment.
Patch	Updates to an operating system, application, or other software issued specifically to correct particular problems with the software.
Personal Identity Verification Card	A physical artifact, *e.g.*, identity card, "smart" card, issued to an individual that contains stored identity credentials, *e.g.*, photograph, cryptographic keys, digitized fingerprint representation, such that a claimed identity of the cardholder may be verified against the stored credentials by another person or an automated process.

Term	Definition
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.
Physical Security Device	Electronic devices that include badge readers, video surveillance equipment, *etc.*
Plan of Action and Milestones	A corrective action plan to identify and document the resolution of information security weaknesses and periodically report to the Office of Management and Budget, the Treasury Department, and Congress.
Platform	A computer or hardware device, an associated operating system, or a virtual environment on which software can be installed or run.
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.
PowerShell	A task-based, command-line shell and scripting language built on the .NET that helps system administrators and power users rapidly automate tasks that manage operating systems and processes.
Preliminary Design Phase	Involves developing the application's logical design. Logical design pertains to an abstract representation of the data flow, inputs, and outputs of the system.
Procurement for Public Sector Application	An application used by the IRS to request, fund, and award contracts; execute delivery orders; and verify receipt and acceptance of products and services as well as accrue procurement-related liabilities and process payments.
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.
Proof of Concept	An investigative component that demonstrates the feasibility of an idea or proves a theory to mitigate integration, interoperability, and system-level risks.
Relying Party	An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.
Requirements and Demand Management	Provides business-friendly tools that enable creation of requirements that can be imported into Rational RequisitePro, an application used to capture detailed requirement data such as the requirement text and any supporting attributes to organize or clarify the requirement.
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.

Term	Definition
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.
Secure Access Digital Identity Platform	Uses authentication when an individual attempting to access a protected resource has control of the specified authenticators/credentials. Security Access Digital Identity is a major system that will deliver a modern digital identity technology platform and capabilities to protect IRS public-facing applications.
Security Technical Implementation Guidelines	Based on Department of Defense policy and security controls, implementation guides are geared to a specific product and version. They contain all requirements that have been flagged as applicable for the product.
Sequencing	A process of evaluating scalability, business affect, capabilities, and processes to determine the order for migrating systems.
Service Account	Represents a process or a set of processes to manage authentication service operations with the operating system and network resources.
Service Level Agreement	A document that describes the minimum performance criteria a provider promises to meet while delivering a service, typically also setting out the remedial action and any penalties that will take effect if performance falls below the promised standard.
Service Provider	Provides information technology services to internal and external customers.
Simple Mail Transfer Protocol	The primary protocol used to transfer electronic mail messages on the Internet.
Small Business/ Self-Employed Division	The IRS business unit that helps small business and self-employed taxpayers understand and meet their tax obligations.
Statistics of Income Division	Its mission is to collect, analyze, and disseminate information on Federal taxation for the Treasury Department's Office of Tax Analysis, Congressional committees, the IRS in its administration of the tax laws, other organizations engaged in economic and financial analysis, and the general public.
Subscriber	A party who has received a credential or authenticator from a CSP. If the applicant is successfully proofed, the individual is then termed a subscriber of that CSP.
System	A set of interdependent components that perform a specific function and are operational. It may also include software, hardware, and processes.
System Deployment Phase	Involves expanding the availability of the solution to all target environments and users. It results in transferring support to an organization other than the developers and signifies the end of project development.
System Development Phase	Involves coding, integrating, and testing the application. It results in the authorization to put the solution into production.
System Security Plan	Provides an overview of the security requirements for the information system and describes the security controls in place or planned to meet those requirements.

Term	Definition
Tax Counseling for the Elderly	An IRS program that offers free tax assistance to individuals who are 60 years or older.
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.
Technical Enabler	Required Java program components not related to Assembler Language Code lines of code.
Trajectory Model	Captures the progress on the lines of code and framework that need to be completed and projects future conversion velocity based on factors that affect development.
Treasury FISMA Inventory Management System	The official FISMA data repository that includes all Treasury Department bureaus. The data maintained in this repository are used as part of the Treasury Department's efforts to comply with the E-Government Act of 2002[1] as well as NIST and Office of Management and Budget regulations and guidance.
UNIX	An operating system known for its relative hardware independence and portable application interfaces. Some of the popular UNIX derivatives are Linux and Solaris.
Velocity	Measurement of how much work can be completed in each product increment iteration.
Virtual Private Network	A secure way of connecting to a private local area network at a remote location, using the Internet or any unsecure public network to transport the network data packets privately, using encryption.
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 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.
Web Currency and Banking Retrieval System	An online IRS database that contains Bank Secrecy Act[2] information.
Whitelist	If the item is on the "whitelist," then it is allowed access or execution rights in a system or network. If it is not on the "whitelist," then it is denied access or execution rights in a system or network.

[1] Pub. L. 107-347, 116 Stat. 2899.
[2] Pub. L. No. 91-508, 84 Stat. 1114-4.

Term	Definition
Windows Policy Checker	An application that validates applicable security requirements on computers that use the Microsoft Windows operating system.
Wireless Controller	A device that manages wireless network access points that allow wireless devices to connect to the network.
[redacted]	[redacted].
[redacted]	[redacted].
[redacted]	[redacted].

Appendix IV

Abbreviations

CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CR BOT	Contractor Responsibility Determination Robot
CSP	Credential Service Provider
CTR	Currency Transaction Report
DIRA	Digital Identity Risk Assessment
ECM	Enterprise Case Management
ELC	Enterprise Life Cycle
ESAT	Enterprise Security Audit Trails
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
IBM	International Business Machines
IRS	Internal Revenue Service
ISE	Identity Services Engine
ISRP	Integrated Submission and Remittance Processing
IT	Information Technology
JAMES	Joint Audit Management Enterprise System
NIST	National Institute of Standards and Technology
PCA	Planned Corrective Action
POA&M	Plan of Action and Milestones
RPA	Robotic Process Automation
SAAS	Security Audit and Analysis System
TIGTA	Treasury Inspector General for Tax Administration
UBAC	User Behavior Analytics Capability
VPN	Virtual Private Network