TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2022

April 6, 2023

Report Number: 2023-20-006

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2022

Final Audit Report issued on April 6, 2023 **Report Number 2023-20-006**

Why TIGTA Did This Audit

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

Impact on Tax Administration

In Fiscal Year 2022, the IRS collected approximately $4.9 trillion in Federal tax payments and processed 260 million tax returns and forms. In addition, IRS Federal tax refund and outlay activities were approximately $642 billion.

The IRS employs approximately 85,000 people in its Washington, D.C., Headquarters and over 460 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 continues to make progress in many information technology program areas. A review of the Child Tax Credit Update Portal and Secure Access Digital Identity system showed that most required security controls and control enhancements were implemented. Additional reviews found that the Taxpayer Digital Communications platform configuration settings for password length and complexity comply with requirements. However, reviews also found that a related cloud service provider's solution was implemented without an approved agency Authorization to Operate letter and without secure contractual services for fraud analysis and detection.

The Fiscal Year 2022 IRS Federal Information Security Modernization Act evaluation found that the Cybersecurity program was effective in three and not effective in 17 of 20 Fiscal Year 2022 Core Inspector General Metrics. The IRS needs to take further steps to improve its security program and fully implement all security program components in compliance with Federal requirements; otherwise, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure. Problems were also reported in the IRS's handling of the privacy of taxpayer data, access controls, system environment security, system configuration management, network monitoring and audit logs, insider threats, and logical partitions as well as security policies, procedures, and documentation.

Reviews of systems development and information technology operations found that the IRS has taken some preliminary steps to address information technology supply chain risks, such as researching the framework for and developing a strategy on supply chain risk management. Reviews also found that governance boards provided oversight of the American Rescue Plan Act programs and followed the IRS's policy and procedures.

However, the IRS did not have a complete inventory of systems to monitor for its User Behavior Analytics Capability and did not track the remediation with a documented Plan of Action and Milestones or risk-based decision for 20 of 29 vulnerabilities. Problems were also reported with information technology asset management, governance and project management, information technology service and helpdesk requests, implementation of corrective actions, updating and modernizing operations, and the Coronavirus Disease 2019 pandemic response.

What TIGTA Recommended

Because this report was an assessment of the adequacy and security of the IRS's information technology based on previous TIGTA and Government Accountability Office reports issued during Fiscal Year 2022, TIGTA did not make any further recommendations.

In its management response to this report, the IRS reiterated concerns noted from previous audits. TIGTA addressed the IRS's concerns in the original reports.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

April 6, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2022 (Audit # 202220002)

This report presents the results of our assessment of the adequacy and security of the Internal Revenue Service's (IRS) information technology. This review is required by the IRS Restructuring and Reform Act of 1998.[1] This audit is included in our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenges of *Administering Tax Law Changes*, *Improving Taxpayer Service*, *Modernizing IRS Operations, Protecting Taxpayer Data and IRS Resources*, and *Reducing Tax Fraud and Improper Payments*.

Management's complete response to the draft report is included as Appendix III. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

[1] Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2, 5, 16, 19, 22, 23, 26, 31, 38, and 49 U.S.C.).

Table of Contents

Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998 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.[1] 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 2022.

The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In Fiscal Year 2022, the IRS collected approximately $4.9 trillion in Federal tax payments and processed 260 million tax returns and forms. In addition, Federal tax refund and outlay activities by the IRS were approximately $642 billion.[2] This was a decrease of 42 percent compared to Fiscal Year 2021, primarily because of the economic impact payments refunded in Fiscal Year 2021. For Fiscal Year 2022, only the recovery rebate amounts from the economic impact payments were refunded under the Coronavirus Aid, Relief, and Economic Security Act;[3] the Consolidated Appropriations Act, 2021;[4] and the American Rescue Plan Act of 2021 (ARPA),[5] which all included provisions to help stimulate the economy.

The IRS collected approximately $4.9 trillion in Federal tax payments and paid approximately $642 billion in refund and outlay activities.

The size and complexity of the IRS add unique operational challenges. The IRS employs approximately 85,000 people in its Washington, D.C., Headquarters and over 460 offices in all 50 States and U.S. Territories. The IRS relies extensively on computerized systems to support its operations to collect taxes, process tax returns, and enforce Federal tax laws. For that reason, it is critical 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 technologies are necessary to meet evolving business needs and to enhance the taxpayer experience.

New legislation affecting modernization

In August 2022, the President signed the Inflation Reduction Act of 2022.[6] It will increase the IRS's budget by nearly $80 billion over 10 years, designated in the areas of taxpayer services, enforcement, operations support, and modernization as well as other areas (*e.g.*, study on a free direct electronic filing tax return system). The modernization area of the legislation

[1] Pub. L. No. 105-206, 112 Stat. 685 (codified as amended in scattered sections of 2, 5, 16, 19, 22, 23, 26, 31, 38, and 49 U.S.C.). See Appendix IV for a glossary of terms.

[2] Federal tax refund and outlay activities include refunds of tax overpayments, payments for interest, and disbursements for refundable tax credits, such as the Earned Income Tax Credit.

[3] Pub. L. No. 116-136, 134 Stat. 281 (codified as amended in scattered sections of 2, 5, 12, 15, 20, 21, 29, 42, and 45 U.S.C.).

[4] Pub. L. No. 116-260.

[5] Pub. L. No. 117-2, 135 Stat. 4 (codified in scattered sections of 7, 12, 15, 19, 20, 26, 29, 42, and 45 U.S.C.).

[6] Pub. L. No. 117-169, 136 Stat. 1818.

provides $4.8 billion in funding for necessary expenses related to the Business Systems Modernization program that includes the development of callback technology and other information technology to improve customer service; the funding is not to be used for operations and maintenance of legacy systems.

The IRS developed the *IRS Integrated Modernization Business Plan* in April 2019. The plan provides a six-year roadmap for achieving the necessary modernization of IRS systems and taxpayer services in two three-year phases that began in Fiscal Year 2019. The IRS organized the plan around four "Modernization Pillars" that are critical to its mission and future development: 1) *Taxpayer Experience*, 2) *Core Taxpayer Services and Enforcement*, 3) *Modernized IRS Operations*, and 4) *Cybersecurity and Data Protection*. The IRS was working on the *IRS Integrated Modernization Business Plan 2.0* that it had planned to publish by the end of Fiscal Year 2022. However, with the passage of the Inflation Reduction Act, the IRS plans to incorporate the legislation into a *Strategic Operating Plan*, scheduled for February 2023.[7] According to the IRS, the new plan will introduce a long-term approach to technological advances while incorporating information from the last three years of the IRS's modernization efforts.

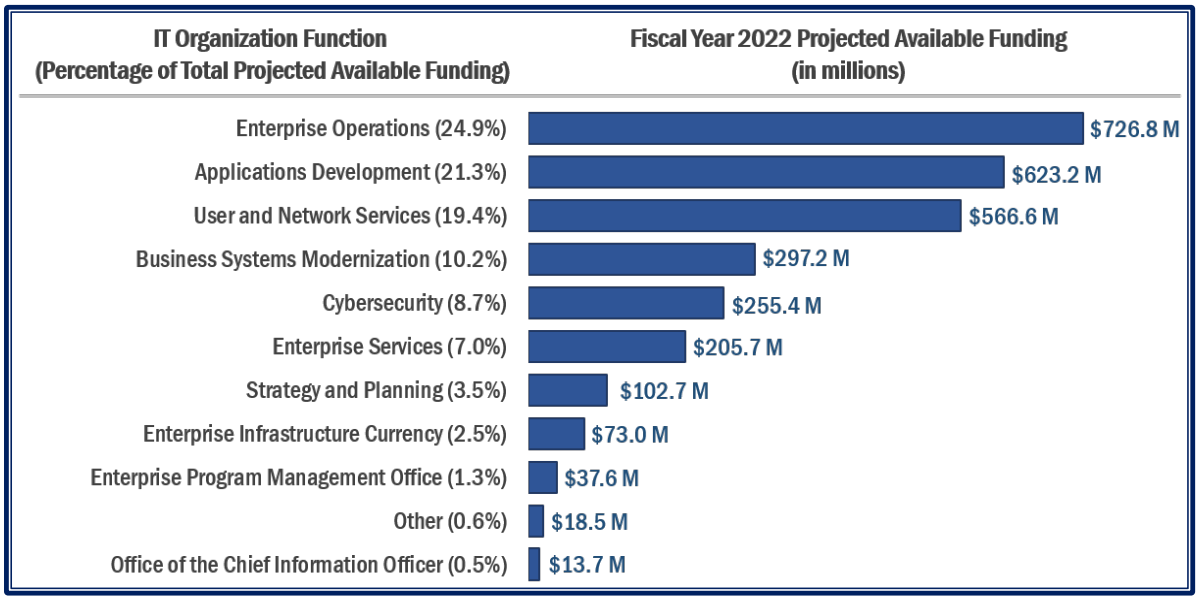
Information technology budget

In Fiscal Year 2022, the IRS's appropriations increased by $676 million to $12.6 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 2022 projected available funds included approximately $3.5 billion for information technology investments, of which $1.4 billion was received to fund recent legislative requirements.[8] Figure 1 illustrates the IRS's Fiscal Year 2022 information technology projected available funding by the IT organization function and major program.

[7] The Treasury Secretary directed the IRS to develop, by February 2023, a plan outlining how it will overhaul its technology.

[8] Recent legislative requirements resulted from the ARPA, the Families First Coronavirus Response Act [Pub. L. No. 116-127, 134 Stat. 178 (codified in scattered sections of 7, 26, 29, and 41 U.S.C.)], the Inflation Reduction Act, the Taxpayer First Act [Pub. L. No. 116-25, 133 Stat. 981 (codified in scattered sections of 26 U.S.C.)], and annual appropriations.

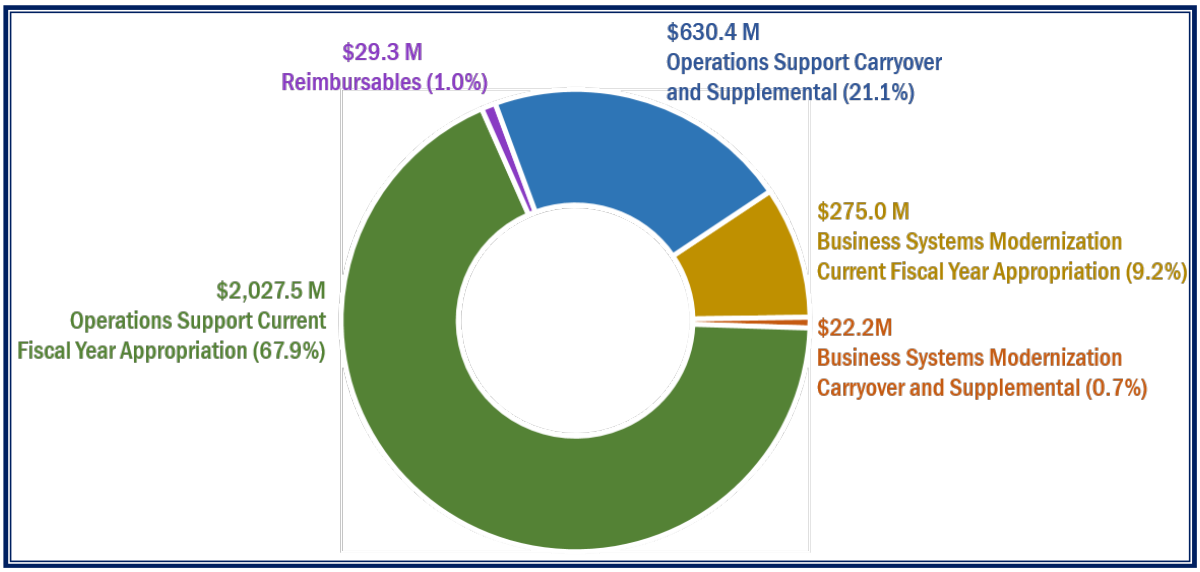
Figure 1: Fiscal Year 2022 Information Technology Projected Available Funding by IT Organization Function and Major Program[9]



Source: IT organization budget data as of June 2022, based on information provided by the Strategy and Planning function's Office of Financial Management Services. The Other category includes Shared Support and other funds not yet distributed.

Figure 2 shows the IT organization's actual available funding for Fiscal Year 2022 by funding source.

Figure 2: Fiscal Year 2022 Total Actual Available Funding by Funding Source[10]



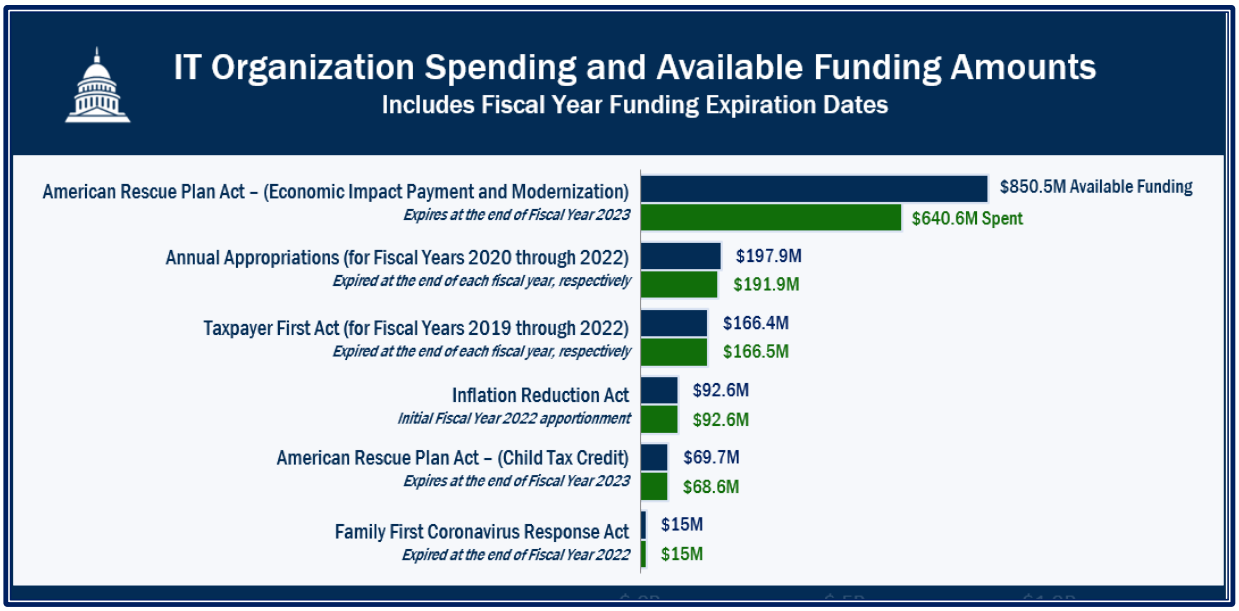
Source: IT organization budget data as of June 2022, based on information provided by the Strategy and Planning function's Office of Financial Management Services.

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

[10] The percentages do not add up to 100 percent due to rounding. The difference of approximately $64 million between Figures 1 and 2 is due to projected versus actual available funding.

Figure 3 presents the IT organization's total spending and available funding for recent legislative requirements by legislation as of September 30, 2022.

Figure 3: IT Organization Spending and Available Funding for Recent Legislative Requirements by Legislation (in Descending Available Funding Order)[11]

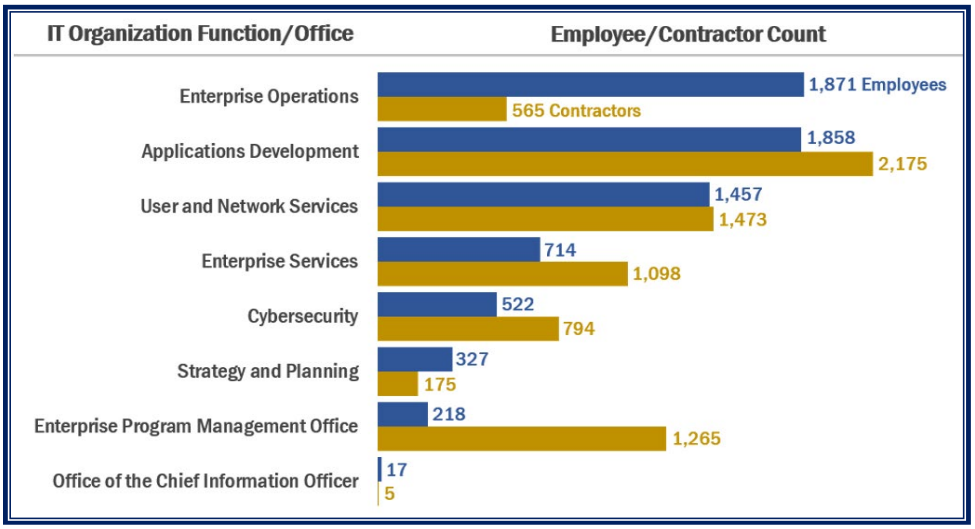


Source: IT organization budget and expense data as of September 30, 2022, based on information provided by the Office of the Chief Financial Officer's Financial Planning and Analysis office. Note: The Inflation Reduction Act provides $4.8 billion in funding for Business Systems Modernization through Fiscal Year 2031.

Figure 4 illustrates that, as of June 2022, the IRS had a total of 6,984 employees and 7,550 contractors working across eight different IT organization functions – 27 fewer employees and 1,001 more contractors than reported in Fiscal Year 2021.

[11] The ARPA available funding amount reflects Fiscal Year 2022 updates and a realignment of funds from the *IRS Integrated Modernization Business Plan*.

Figure 4: Number of Employees and Contractors by IT Organization Function (in Descending Employee Order)



Source: IRS Human Resources Reporting Center as of June 2022.

- The **Enterprise Operations function** facilitates information technology operational activities in the enterprise computing centers, campuses, and call sites.
- The **Applications Development function** is responsible for building, unit testing, delivering, and maintaining integrated information applications to support modernized and legacy systems in production.
- The **User and Network Services function** oversees a portfolio of technology and services that enable communication, collaboration, and business capabilities.
- The **Enterprise Services function** is responsible for strengthening the technology infrastructure across the enterprise by defining the current and target architectures and developing a transition strategy to move towards the target environment.
- The **Cybersecurity function** ensures compliance with Federal statutory, legislative, and regulatory requirements to assure the confidentiality, integrity, and availability of 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, comprehensive and integrated modernization planning, strategic planning and performance measurement, financial management services, vendor and contract management, requirements and demand management, and risk management.
- The **Enterprise Program Management Office** delivers best practices in program management and leads programs to improve business processes and operations as well as the taxpayer experience.
- The **Office of the Chief Information Officer** includes the Chief Information Officer (CIO), two Deputy CIOs, and their employees. The CIO leads the IT organization and advises the IRS Commissioner. The CIO also manages all information system resources and is responsible for delivering and maintaining modernized systems. The Deputy CIO for Operations has oversight responsibility for the IT organization's planning and

execution of filing season as well as the day-to-day operations of information systems and services. In addition, the Deputy CIO for Operations is focused on upgrading the IRS's infrastructure and improving service availability. The Deputy CIO for Strategy and Modernization provides executive oversight for large modernization programs in addition to providing guidance on investment planning and strategic decision making supported by data and analysis.

Results of Review

During this annual review, we summarize information from program efforts in cybersecurity, systems development, and information technology operations. TIGTA audits of the IRS's information technology program addressed the major management and performance challenges of *Administering Tax Law Changes*, *Improving Taxpayer Service*, *Modernizing IRS Operations, Protecting Taxpayer Data and IRS Resources*, and *Reducing Tax Fraud and Improper Payments*. This report presents a summary of TIGTA and Government Accountability Office (GAO) audit results previously reported for Fiscal Year 2022. It does not reflect any additional audit work or corrective actions that the IRS may have taken 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 continues to make 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.

Systems Security and Privacy of Taxpayer Data

Federal agencies are dependent on information systems and electronic data to carry out operations and to process, maintain, and report essential information. Computer systems and electronic data support virtually all Federal activities. 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 or external to an organization. Internal threats include equipment failures, human errors, and fraudulent or malicious acts by employees or contractors. External threats include the ever-growing number of cyberattacks 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.

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)[12] report that provides an overall assessment of the information security program,[13] 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, and system environment security 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 the requirements of the FISMA and is supported by the Office of Management and Budget (OMB), the Department of Homeland Security, agency security policy, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST) related to information security practices.

The FISMA directs Federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices as well as 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 OMB. These independent evaluations are to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General. TIGTA is responsible for the oversight of the IRS, while the Department of the Treasury's (hereafter referred to as the Treasury Department) Office of Inspector General is responsible for all other Treasury Department bureaus.

The *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines* was developed as a collaborative effort among representatives from the OMB, the Council of the Inspectors General on Integrity and Efficiency, the Federal Civilian Executive Branch Chief Information Security Officers and their staff, and the Intelligence Community. The 20 Fiscal Year 2022 Core Inspector General Metrics represent a continuation of work begun in Fiscal Year 2016, when the Inspector General metrics were aligned with the five cybersecurity function areas in the *NIST Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Apr. 2018), referred to as the Cybersecurity Framework. The five Cybersecurity Framework function areas and associated security program component(s) are: IDENTIFY (Risk Management and Supply Chain Risk Management [SCRM]); PROTECT (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training); DETECT (Information Security Continuous Monitoring); RESPOND (Incident Response); and RECOVER (Contingency Planning).

The Inspectors General are required to assess the effectiveness of information security programs based on a maturity model spectrum. Aligning with the Carnegie Mellon Cybersecurity Maturity

[12] 44 U.S.C. § 3551, et seq. (2018).

[13] TIGTA, Report No. 2022-20-040, *Fiscal Year 2022 IRS Federal Information Security Modernization Act Evaluation* (July 2022).

Model Certification, the foundational levels require Federal agencies to develop sound policies and procedures, while advanced levels capture the extent to which agencies institutionalize those policies and procedures. Maturity levels range from *Ad-Hoc* for not having formalized policies, procedures, and strategies to *Optimized* for fully institutionalizing sound policies, procedures, and strategies across the agency. Figure 5 details the five maturity 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: Inspector General's Assessment Maturity Levels

Source: Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines and Fiscal Year 2021 FISMA Reporting Metrics, Version 1.1.

To determine the effectiveness of the Cybersecurity program, we evaluated the maturity level of the 20 Core Inspector General Metrics specified in the *Fiscal Year 2022 Core Inspector General Metrics Implementation Analysis and Guidelines*. 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 TIGTA and GAO audits. These audits, whose results were applicable to the FISMA metrics, were performed, completed, or contained recommendations that were still open during the evaluation period, July 1, 2021, to May 31, 2022.[14]

We found that the Cybersecurity program was effective in three and not effective in 17 of 20 Fiscal Year 2022 Core Inspector General Metrics. Specifically, we found one metric achieved the *Optimized* maturity level 5 and two metrics achieved the *Managed and Measurable* maturity

[14] The FISMA evaluation period is from July 1, 2021, to June 30, 2022; however, OMB Memorandum M-22-05, *Fiscal Year 2021–2022 Guidance on Federal Information Security and Privacy Management Requirements* (Dec. 2021), adjusted the timeline for the Inspector General evaluations of agency effectiveness to align with the budget submission cycle. Due to the early submission cycle, the period covered for this review was from July 1, 2021, to May 31, 2022.

level 4. However, we determined that six metrics were at a *Consistently Implemented* maturity level 3 and 11 metrics were at a *Defined* maturity level 2. As a result, we rated the Cybersecurity program as "not effective." Figure 6 presents the maturity level ratings for the assessed metrics.

Figure 6: Fiscal Year 2022 Core Inspector General Metrics Assessment Results

Maturity Level	Metric(s)	Count
Level 5: Optimized	55	1
Level 4: Managed and Measurable	54 and 63	2
Level 3: Consistently Implemented	1, 5, 10, 37, 42, and 61	6
Level 2: Defined	2, 3, 14, 20, 21, 30, 31, 32, 36, 47, and 49	11
Level 1: Ad Hoc	None	0

Source: TIGTA's evaluation of the 20 Fiscal Year 2022 Core Inspector General Metrics.

As examples of specific metrics that were not considered effective, TIGTA identified that the IRS could improve on maintaining a comprehensive and accurate inventory of its information systems, tracking and reporting on an up-to-date inventory of hardware and software assets, maintaining secure configuration settings for its information systems, implementing flaw remediation and patching on a consistent and timely basis, and ensuring that security controls for protecting Personally Identifiable Information are fully implemented. The IRS needs to take further steps to improve its security program deficiencies and fully implement all security program components in compliance with the FISMA requirements; otherwise, 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 cyber threats and fraud schemes and in protecting trillions of taxpayer dollars.

During Fiscal Year 2022, TIGTA performed three audits involving privacy of taxpayer data. We initiated an audit to **assess the IRS requirements review process and the development of the Child Tax Credit (CTC) Update Portal, including any impacted or associated systems and**

applications.[15] In March 2021, the President signed the ARPA into law, which required the IRS to establish a CTC Advance Payment program. In response to this requirement, the IRS developed the CTC Update Portal, which allowed taxpayers to elect out of receiving payments related to the advance CTC as well as to provide updates to the number of qualifying children, marital status, or significant change in the taxpayer's income. As part of the CTC Update Portal development, the IRS accelerated the initial launch of the Secure Access Digital Identity (SADI) system from a small-scale pilot program to a full-scale production solution that will serve as the IRS's next-generation identity proofing solution to improve taxpayer access to its online services. Both the CTC Update Portal and the SADI system are designated as moderate-impact systems.

We found that most required security controls were implemented. We determined that 37 NIST and IRS-specific security controls and control enhancements were applicable to the CTC Update Portal and 319 were applicable to the SADI system. For the CTC Update Portal, we found that 29 (78 percent) of 37 applicable security controls and control enhancements from eight security control families (*e.g.*, Access Control and Configuration Management) were implemented. The eight security controls and control enhancements within five of the security control families (*e.g.*, Planning and Risk Assessment) that were not implemented, contain specific risk areas that need to be addressed. The IRS has an active Plan of Action and Milestones (POA&M) for each of the five risk areas to reduce these risks, ensure system integrity, and maximize system availability for taxpayers. For the SADI system, we found that 282 (88 percent) of 319 applicable security controls and control enhancements were implemented. For 28 of the controls, the IRS has either an active POA&M or an approved risk-based decision for these risk areas. For the remaining nine controls, the IRS did not satisfy minimum agency requirements for required security control implementation.

Privacy controls

The Privacy, Governmental Liaison and Disclosure organization manages privacy controls at the IRS. Our review of the assessment and implementation of the privacy controls applicable to the SADI system found that each of the 36 NIST privacy controls and control enhancements were implemented. However, the Privacy, Governmental Liaison and Disclosure organization is not effectively managing the selection, implementation, and assessment of privacy controls in accordance with OMB directives and IRS security procedures. For example, none of the formal documentation provided evidence that all privacy controls were properly selected, implemented, and assessed, and no routine verification that the entire NIST control, including control enhancements, was addressed in the implementation decision making. By not having a formal documented process that provides adequate oversight of the selection, implementation, and assessment of privacy controls, the IRS is potentially at risk of being unable to ensure the privacy and security of taxpayers' personal information.

Media protection controls

The Enterprise Operations function's Data Storage and Protection branch is responsible for the implementation and maintenance of media protection controls for IRS systems. However, the Cybersecurity function's Security Risk Management organization is responsible for validating the assessment and implementation of all NIST security controls. Our review of the assessment and implementation of the media protection controls applicable to the SADI system found that only

[15] TIGTA, Report No. 2022-27-028, *The Child Tax Credit Update Portal Was Successfully Deployed, but Security and Process Improvements Are Needed* (May 2022).

one (11 percent) of nine media protection controls was implemented. Eight (89 percent) of the media protection controls were not implemented per agency requirements. By not having a process that ensures the assessment and implementation of all required NIST media protection controls, the IRS is unable to provide a full cadre of safeguards and countermeasures for IRS information systems.

In addition, we found that the cloud service provider's (CSP) solution was implemented without an approved Authorization to Operate letter (authorizing the CSP to operate for the IRS). On June 7, 2021, the IRS leveraged an existing Treasury Department blanket purchase agreement and issued a delivery order for the software licenses and software maintenance credential service provider to provide identity-proofing support.[16] On June 15, 2021, the Director of the Security Risk Management organization signed the completed *Cloud Security Threat Analysis Report*, which provides the authorizing official with systematic analysis of probable threat characteristics, potential security risks, and the overall security posture of the CSP. However, the Security Risk Management organization did not timely provide the completed *Cloud Security Threat Analysis Report* and the CSP's agency Authorization to Operate letter to the authorizing official.

The CTC Update Portal and SADI system went live on June 21, 2021. Approximately two days after the CSP went live, the authorizing official ultimately signed both the *Cloud Security Threat Analysis Report* and the CSP's agency Authorization to Operate letter. By allowing the CSP's solution to be implemented without an approved agency Authorization to Operate letter, the IRS cannot ensure that the CSP operates with an acceptable level of risk to IRS operations and assets, other organizations, and taxpayers.

Further, approximately 16 days after the SADI system went live, the IRS entered into a separate agreement with the same CSP to provide security services related to audit logging, data security, and providing assistance with fraud analysis and detection. During the 16-day period with no contractual services for fraud analysis and detection, the IRS implemented a manual data retrieval fraud monitoring and analysis process with the CSP to address fraud activity. By not securing contractual security services prior to the CSP solution going live, the IRS was operating with increased risk for unauthorized network access that could result in fraudulent activity or the loss of sensitive taxpayer data.

We also initiated an audit to **evaluate the effectiveness of controls to protect taxpayer data on cloud computing services**.[17] During our review, we found that cloud services were implemented with known capability gaps. In late Calendar Year 2019, after 23 cloud services had been fully implemented, the IRS reviewed three applications containing taxpayer data hosted in moderate cloud environments to provide a baseline for the current state of the IRS cloud environment. The IRS also used stakeholders and documentation reviews and assessed the cloud current state against Internal Revenue Manual (IRM) policies and NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and*

[16] The credential service provider provides identity proofing and user authentication through an agreement with an information technology solutions contractor.

[17] TIGTA, Report No. 2022-20-052, *Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk* (Sept. 2022).

Organizations (Sept. 2020), security controls and identified gaps.[18] The IRS identified gaps related to security capabilities that are required to operate in the cloud. These capabilities could apply to all cloud services with taxpayer data. The IRS subsequently presented many of these cloud capability gaps in its migration plan, along with initiatives to address them. Examples of cloud capability gaps include the following:

Continuous security monitoring

- No fully implemented incident management processes.
- No fully defined and implemented plan to integrate native cloud services with on-premise tools for network monitoring.

Program management and integration

- No roadmaps for implementation of core cloud security solutions.
- No training or hiring plans to fill Cybersecurity function cloud workforce gaps.

In addition, we found that, [redacted][19]. [redacted]. The acceleration of cloud deployments coupled with not having a fully implemented cloud security control infrastructure in place prior to turning over control of taxpayer data to the CSPs limits management's ability to fully provide the necessary assurance to protect taxpayer data.

[18] IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (May 2019); IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy* (Mar. 2019); and IRM 10.5.1, *Privacy and Information Protection, Privacy Policy* (Sept. 2019).

[19] [redacted].

In addition, we initiated an audit to **assess the security and access controls of the Taxpayer Digital Communications (TDC) platform**.[20] In an effort to improve customer service and the taxpayer experience, the IRS launched the TDC platform. The platform enables faster communication as well as offers taxpayers and their authorized representatives the ability to securely send and receive electronic messages and documents to and from IRS agents and customer service representatives.[21] The TDC platform uses a commercial off-the-shelf software, which is developed and maintained by the vendor. The vendor of the software is also the dedicated managed service provider (hereafter referred to as the MSP) for the TDC platform. The platform includes various installations that were created to meet IRS requirements. The TDC platform, including the installations, are stored on a customer engagement platform in a cloud, which is Federal Risk and Authorization Management Program (FedRAMP) authorized. FedRAMP is a U.S. Federal Governmentwide program that provides a standardized approach to security assessments, authorizations, and continuous monitoring for cloud products and services.

We found that the IRS is not conducting required FedRAMP security reviews for continuous monitoring to ensure that the cloud's security posture remains sufficient for the TDC platform. Although the cloud was FedRAMP authorized in June 2016, Security Risk Management organization management stated that they have not conducted the FedRAMP security reviews for continuous monitoring.[22] According to both the General Services Administration's *FedRAMP Security Assessment Framework* (Nov. 2017) and *FedRAMP Continuous Monitoring Strategy Guide* (Apr. 2018), the continuous monitoring phase of the FedRAMP authorization process is critical to ensuring that the CSP's security posture continues to meet Federal cloud service requirements. The agency's authorizing official is required to oversee the CSP's continuous monitoring activities for any significant changes and review all security artifacts provided by the CSP, third-party assessment organization, or FedRAMP to ensure that the CSP's security posture remains sufficient for their agency's use of the system. The agency's authorizing official should use this information to make risk-based decisions of the ongoing authorization of the system for their agency.

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.*, authentication and identity proofing, authorization, and access management).

[20] TIGTA, Report No. 2022-20-051, *Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened* (Sept. 2022).

[21] Agents conduct examinations of individuals, businesses, corporations, and Government entities to determine Federal tax liability.

[22] The IRS initially procured the customer engagement platform as a private MSP for the TDC platform, and it was not required to be FedRAMP authorized. In May 2021, the vendor became the Software-as-a-Service solution and was then required to be FedRAMP authorized. In December 2021, the customer engagement platform was FedRAMP authorized.

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 2022, TIGTA performed an audit on physical security access controls. In our audit of the **CTC Update Portal**, we evaluated several IRS-provided documents and determined that 21 (95 percent) of 22 NIST physical and environmental protection controls applicable to the SADI system were implemented. We were unable to evaluate and assess one control related to alternate work site operations because there was no process to ensure the assessment and implementation of all required physical and environmental protection controls. In addition, the entry for the alternate work site operations control was listed as not applicable on the documents reviewed. However, we determined that the control was applicable to the IRS because the control supports the contingency planning activities of an organization and the Federal telework initiative. Without a process for the assessment and implementation of all required NIST physical and environmental protection controls, the IRS risks being unable to deliver a safe, secure, and optimal work environment that promotes effective tax administration.

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. Access control involves identifying a user based on their credentials and then authorizing the appropriate level of access once they are authenticated. Once a user's identity has been authenticated, access control policies grant specific permissions and enable the user to proceed as intended.

Authentication and identity proofing

Identification is the process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an information system. User identification, which distinguishes one user from all others, is important as a means to assign specific access privileges for the information system to recognize. However, the confidentiality of a user identification is typically not protected. For this reason, agencies typically use other means of authenticating users in determining whether individuals are who they claim to be, such as with the use of passwords, tokens, or biometrics. To further increase security, an agency may use a combination of multiple mechanisms (also known as multifactor authentication), such as a password with personal identity verification card credentials.

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 they claim to be. When remote identity proofing is used, there is no way to confirm an individual's identity through their physical presence. Instead, the individual provides information electronically or performs other electronically verifiable actions that demonstrate their 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 their identity.

In Fiscal Year 2022, TIGTA and the GAO each performed an audit covering authentication and identity proofing. In our audit of the **CTC Update Portal**, we found that the Digital Identity

Acceptance Statement met both Federal and IRS security requirements. The IRS must perform risk assessments; select individual assurance levels for identity proofing, authentication, and federation (if applicable); determine which processes and technologies it will employ to meet each assurance level; and document these decisions in a Digital Identity Acceptance Statement. The Digital Identity Acceptance Statement must include the assessed and implemented assurance levels, rationale if the implemented assurance levels differ from the assessed assurance levels, comparability demonstration of compensating controls, and rationale if federated entities are not accepted.

We reviewed the Digital Identity Acceptance Statement and all related documents for the CTC Update Portal and found that the IRS appropriately assessed and implemented level two controls for the identity, authenticator, and federated assurance levels. The NIST defines the components of level two identity, authenticator, and federated assurance as follows:

- *Identity Assurance Level Two:* Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. This level also introduces the need for either remote or physically present identity proofing.
- *Authenticator Assurance Level Two:* Provides high confidence that the claimant controls authenticators bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocols. Approved cryptographic techniques are required at this level and above.
- *Federated Assurance Level Two:* Adds the requirement that the assertion be encrypted using approved cryptography such that the relying parties are the only parties that can decrypt it.

By ensuring that the CTC Update Portal complies with all applicable NIST and IRS security requirements related to digital identity services, the IRS has taken steps to mitigate the risks associated with potential unauthorized access and activities, compromised taxpayer records, and lost revenue due to identity theft and refund fraud.

The GAO initiated an audit to **evaluate the IRS's internal control over financial reporting and to determine the status of the IRS's corrective actions addressing its prior years' recommendations related to financial reporting that remained open as of September 30, 2020**.[23] The GAO reported that it found two deficiencies in access controls related to identification and authentication. The IRS did not enforce multifactor authentication when users accessed a certain information system. In addition, the IRS did not appropriately configure the password for a service account supporting an application.

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

[23] GAO, GAO-22-105559, *Management Report: IRS Needs to Improve Financial Reporting and Information System Controls* (May 2022).

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 2022, TIGTA performed an audit covering authorization. In our audit of the **TDC platform**, we found that not all users were authorized to access the TDC platform. When a user needs access to a system, the user requests access and specifies their user role (*i.e.*, privileged or nonprivileged) through the Business Entitlement Access Request System (BEARS).[24] The user's manager and the system administrator approve the request in the BEARS. Once approved, the system administrator creates a user account and assigns the appropriate user role.

We obtained a list of 3,258 users from the BEARS with authorizations to the TDC platform as of January 6, 2022, and a list of 3,441 users from the MSP who have access to the TDC platform as of February 4, 2022. Our review and comparison of the two lists determined that, of 3,939 distinct total users:

- 2,760 (70 percent) users were authorized in the BEARS and have access to the TDC platform.
- 498 (13 percent) users were authorized in the BEARS and did not have access to the TDC platform.
- 681 (17 percent) users with access to the TDC platform were not authorized in the BEARS.

In total, we identified 1,179 incorrect or missing authorizations. Figure 7 provides a summary of our analysis.

Figure 7: Analysis of TDC Platform User Accounts

Account Type	Users With Authorizations in the BEARS Who Have Access to the TDC Platform	Users With Authorizations in the BEARS Who Do Not Have Access to the TDC Platform	Users With No Authorizations in the BEARS Who Have Access to the TDC Platform	Total Users
Privileged	3[25]	4	12	19
Nonprivileged	2,757	494	669	3,920
Totals	2,760	498	681	3,939

Source: TIGTA's analysis of user account data from the BEARS and the MSP of TDC platform users, dated January 6 and February 4, 2022, respectively.

[24] The BEARS is replacing the Online 5081 system. The Online 5081 system is 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.

[25] Two of the three users with authorizations in the BEARS for privileged access did not have privileged access on the TDC platform.

We also found that, while only seven [three plus four] users have authorizations in the BEARS for privileged access, 70 users had privileged access on the TDC platform. Of the 70 users, 57 users have authorizations, but not for privileged access; 12 users have no authorizations at all; and only one user has an authorization and access for privileged access. Six of the seven users with authorizations in the BEARS for privileged access did not have privileged access on the TDC platform.

In addition, we found users who have a continued business need for access are not timely recertified. Specifically, we determined that 735 (23 percent) of 3,258 [2,760 plus 498] users with authorizations in the BEARS were not timely recertified. Three of 735 users not timely recertified have privileged access to the TDC platform; the remaining 732 users have nonprivileged access. The delays ranged from 24 to 119 calendar days for privileged users, averaging 67 calendar days, and from 1 to 178 calendar days for nonprivileged users, averaging 33 calendar days.

Management Action: On March 28, 2022, the Cybersecurity function opened a POA&M with a planned completion date of December 31, 2022, to resolve the BEARS recertification issue.

Access management

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 2022, TIGTA and the GAO performed three audits on access management. We initiated an audit to **evaluate the effectiveness of IT organization efforts to limit the internal network risk exposure by segmenting key information technology systems**.[26] In Calendar Year 2012, the IRS conducted penetration testing that disclosed significant security vulnerabilities in its internal local area network. These vulnerabilities indicated that the internal network environment was not secure and raised the possibility of undetected accesses to sensitive taxpayer data. As a result, the IT organization initiated the Unified Access project and later the Network Segmentation (SEG) project to resolve these vulnerabilities. The goal of the Unified Access project was to authenticate users and devices regardless of connection type (*i.e.*, through wired, wireless, or virtual private network connections). Specifically, it was to ensure that only valid users and devices were permitted access to the IRS's internal network. The purpose of the SEG project was to implement a solution that would allow users to navigate only to authorized resources within the internal network and initiate cybersecurity alerts when unauthorized users and devices attempt to connect to the internal network or access resources. The IRS has made implementing network segmentation for designated high-value assets (*e.g.*, Individual Master File [IMF] and [redacted]) a priority.

We found that network segmentation reduced the number of users potentially able to access the IMF. According to an *IRS Progress Update Fiscal Year 2020 Report* (Dec. 2020), prior to deploying network segmentation for the IMF, [redacted] were able to reach the mainframe logical partitions where the IMF runs. After network segmentation was deployed for the IMF, the number of users able to reach IMF-related partitions was reduced to [redacted]

[26] TIGTA, Report No. 2022-20-010, *Network Segmentation Reduced Unnecessary Access to Individual Master File Resources; However, Governance and Development Processes Were Not Always Followed* (Feb. 2022).

[redacted], eliminating the unnecessary access of a significant number of users. The [redacted] that run on the same mainframe logical partitions as the IMF.

We obtained audit logs from December 1, 2020, showing more than 1,400 audit log records and selected a judgmental sample of 30 of 75 users who accessed IMF resources during a four-hour period.[27] We verified that all 30 users were properly authorized to access the IMF resources. Further, we reviewed configuration settings and the query results of the two access control software and validated that the classification, propagation, and enforcement phases of network segmentation were enabled.

In our audit of the **TDC platform**, we found that TDC platform configuration settings for password length and complexity (*i.e.*, use of uppercase and lowercase letters, numbers, and special characters) comply with requirements. However, the passwords settings for local user accounts are set to never expire. While the majority of user accounts are accessed using single sign-on, we identified 52 local user accounts that are accessed using a username and password. Local user accounts include both administrator and analyst accounts and are used to perform troubleshooting, validate software updates, and provide technical support to users and taxpayers. Our review determined that the passwords for 10 (19 percent) of 52 local user accounts had not been changed in over 60 calendar days as required. The number of days late ranged from 61 to 944 calendar days, averaging 154 calendar days. By not enforcing password expiration limits, the IRS allows an attacker the time to compromise a user's password and have access to taxpayer data.

In addition, we found that two default vendor accounts (*i.e.*, partition administrator and system administrator) were re-enabled after the TDC platform was launched in December 2016. Both accounts have no production use and the account names and passwords were not changed when they were originally disabled. The MSP senior project manager was unable to provide support but stated that both default vendor accounts were initially disabled when the platform was launched. We also identified two test accounts in the production environment that were created to test and troubleshoot the platform; however, IRS requirements provide that developers do not develop or test on production systems. All systems should be tested prior to being placed into the production environment. While one test account was never logged in, the last log in for the other test account was in December 2020. Re-enabling default vendor accounts and not changing or disabling passwords and having test accounts in the production environment unnecessarily expose the TDC and customer engagement platforms to unauthorized access, which may result in damage or loss of data.

We also found that 1,237 (36 percent) of 3,465 user accounts,[28] of which 20 user accounts have privileged access, should have been disabled, quarantined, or removed due to inactivity.[29] Privileged and nonprivileged user accounts should be disabled after 60 and 120 calendar days of inactivity and quarantined after 90 and 240 calendar days of inactivity, respectively. Both privileged and nonprivileged user accounts should be removed after 365 calendar days of inactivity. The time for inactivity ranged from 78 to 2,057 calendar days, averaging 335 calendar

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

[28] Ten users had an additional 24 user accounts for different TDC installations and user roles.

[29] Quarantined accounts are disabled accounts whose user rights and permissions have been revoked.

days. Two of the privileged user accounts that should have been quarantined both had the ability to make modifications to the system's configurations, manage application security, and add and remove users. We also determined that 646 (52 percent) of 1,237 user accounts were never logged in. Figure 8 presents the result of our analysis.

Figure 8: Analysis of User Accounts for Inactivity

Account Type	User Accounts That Should Be Disabled	User Accounts That Should Be Quarantined	User Accounts That Should Be Removed	Total User Accounts
Privileged	1	16	3	20
Nonprivileged	339	524	354	1,217
Totals	340	540	357	1,237

Source: TIGTA's analysis of the MSP list of user accounts on the TDC platform as of February 4, 2022.

Further analysis of the user account data against the Treasury Integrated Management Information System determined that three accounts belonged to employees who had left the IRS.[30] Two of the user accounts were last logged in 217 and 246 calendar days ago. The third user account was created 345 calendar days ago and was never logged in.

Management Action: We notified Contact Center Support division management of the IRM requirements. On April 20, 2022, a Contact Center Support division contractor stated that they will update the configuration setting to be more restrictive for a maximum inactivity time frame of 60 calendar days to disable both privileged and nonprivileged user accounts.

In its audit of the **IRS's internal control over financial reporting**, the GAO reported that it identified one deficiency in access controls related to boundary protection. Specifically, the IRS did not provide warning banners in certain databases when database administrators accessed them directly.

System environment security

Management of the system environment security provides organizations the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the 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 scanning, vulnerability remediation, and patching; system configuration management; network monitoring and audit logs; insider threats; and logical partitions.

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

[30] The Treasury Integrated Management Information System is the official automated personnel and payroll system for storing and tracking all employee personnel and payroll data. It is outsourced to the U.S. Department of Agriculture's National Finance Center and managed by the Treasury Department.

weaknesses. Users must be diligent to identify weaknesses and take appropriate actions to minimize the chance of these weaknesses being exploited.

In Fiscal Year 2022, TIGTA performed six audits involving system scanning and vulnerability patching of IRS systems. We initiated an audit to **determine whether the IRS effectively identified and addressed vulnerabilities on network devices**.[31] We found that the IRS did not fully implement privileged access scanning for required devices. According to Cybersecurity function personnel, the Enterprise Vulnerability Scanning group uses either scanning agents or remote credentialed scans to conduct privileged access scanning. Specifically, [redacted]. By not fully implementing privileged access scanning, vulnerability assessments are not complete, which potentially increases the risk of exposure for taxpayer data and information.

In addition, we found that the IRS is not timely remediating vulnerabilities in accordance with the IRM's required time frames. We obtained and analyzed the daily vulnerability scan results for January 29, 2021, and found [redacted].[32] [redacted]:

[redacted]

[redacted].[33] [redacted]:

[redacted]

- [redacted].

The IRS is also not ensuring that vulnerabilities exceeding remediation time frames are being tracked as required because it lacks centralized enterprise-wide oversight to provide visibility

[31] TIGTA, Report No. 2022-20-006, *Vulnerability Scanning and Remediation Processes Need Improvement* (Dec. 2021).

[32] [redacted].

[33] [redacted].

and tracking of aging vulnerabilities that would require POA&Ms or risk-based decisions. Failure to resolve or track existing vulnerabilities compromises the security posture of the enterprise, potentially exposing taxpayer data and information to unnecessary risk.

We also initiated an audit to **determine whether the IRS is adequately assessing the risks to its databases when performing vulnerability scans and installing timely patches**.[34] [redacted].

The IRS officially announced the reduction in database vulnerability scanning three years after it had started reducing its database vulnerability scanning. Although the strategy is outlined in a signed February 2021 memorandum, the IRS never changed its formal written policy related to database vulnerability scans. While the IRS's written policy remained in compliance with Federal guidance, the new strategy to not perform privileged database vulnerability scanning on all system databases, including mainframe applications that are considered high-value assets, was not compliant with the IRS's formal written policy or Federal guidance. When privileged vulnerability scanning is not performed on all databases, the IRS could have vulnerabilities that are not detected and therefore are unknown to the system owner.

Management Action: In April 2021, the IRS began increasing database vulnerability scanning. By March 2022, it increased scanning to [redacted] systems. However, the increased scanning capabilities did not include the [redacted].

In addition, we found that the IRS stopped database vulnerability scanning on the Mainframe 1 systems in 2018. Although the Mainframe 1 systems are considered a high-value asset, [redacted]. Mainframe 1 security software for Operating System 1 enables the protection of resources by making access control decisions through resource managers. [redacted].

The IRS stated that mitigation for its [redacted]. However, we determined that the justification the IRS used in its risk-based decision was not compliant with the IRM requirements for risk acceptance because it was [redacted].[35] [redacted]. A commercial database vulnerability scanning component works with the IRS database vulnerability scanning tool, allowing the full scanning of the mainframe databases, including the mainframes installed with the security software. The IRS has known about this component since 2019. [redacted].

[34] TIGTA, Report No. 2022-20-065, *The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls* (Sept. 2022).

[35] The IRS let this risk-based decision expire on March 2, 2022.

[redacted].

We also found that information system security officers did not recommend approval or disapproval for policy deviations. [redacted].

The information system security officer is responsible for the security of the system and informing the authorizing official of security issues. The information system security officer is also responsible for recommending approval or disapproval of deviations from policy. [redacted]. According to Information System Security Management, a formal process does not exist for recommending disapproval of deviations from policy that have a significant impact on IRS systems. Without any formal process for information system security officers to address the security risks from changes in policy, the IRS is putting itself at risk for exploitation of vulnerabilities.

In addition, we initiated an audit to **determine the effectiveness of configuration management controls for the IRS mainframe platforms**.[36] We found that the configuration vulnerability age is not tracked. We reviewed the February 2022 configuration vulnerability assessments and found that none of the mainframe vulnerability assessment tools report the date first seen or date remediated for discovered configuration compliance issues.[37] Management officials from the Cybersecurity function's Architecture and Implementation group stated that these data elements are not available for reporting on mainframe platforms. In addition, they stated that, when the configuration settings management capability for the mainframe platform is matured, this capability will be added as a Continuous Diagnostics and Mitigation requirement. However, this functionality is still in the assessment and planning phase, and there is no timeline for this requirement to be added. Without age tracking capabilities for configuration compliance issues, remediation and prioritization will be inaccurate and inefficient, and mainframes will remain at risk.

In our audit of **database vulnerability scanning and patching**, we also found that the IRS is not effectively providing oversight of cloud databases' vulnerability scan results. Rather than completing its own privileged vulnerability scans or receiving detailed vulnerability scan results, the IRS is relying on FedRAMP requirements for ensuring that vulnerabilities are addressed in the majority of its cloud systems. We identified [redacted] IRS FISMA cloud systems and determined that the IRS conducted monthly privileged vulnerability scans [redacted] systems. The Enterprise Database Scanning office conducted these three scans on the cloud system databases with its database vulnerability scanning tool. [redacted], the IRS

[36] TIGTA, Report No. 2022-20-050, *Mainframe Platform Configuration Compliance Controls Need Improvement* (Sept. 2022).

[37] These tools include the [redacted].

relies on the CSP to provide monthly scanning reports. According to the IRS, the reports are high level and do not provide vulnerability details. Depending on the vendor, the IRS was able to download the reports in some instances but not in others. As a result, the IRS inconsistently received or was unable to review vulnerability details from the CSPs. We also determined that the IRS does not receive monthly vulnerability reports [redacted] cloud systems on the CSP's Government platforms that the IRS could be scanning but is not. The IRS needs to have full access to the scan results and assurance that privileged scans are being performed. The IRS increases the risk of having its data compromised by not knowing what vulnerabilities exist on its databases. In addition, information system security officers cannot effectively perform their jobs with due diligence when they do not know the latest database vulnerabilities they are accountable for.

In addition, we found that database vulnerabilities are not being timely patched. In October 2021, we requested a database vulnerability scanning report to show us open critical database vulnerabilities. The IRS provided a database vulnerability scan report for Relational 1 and Relational 2 databases executed on October 21, 2021, showing [redacted] critical vulnerabilities across the production, disaster recovery, test, and development environments. Our analysis determined that [redacted]. As of March 2022, the IRS has not patched [redacted].

In our audit of the **CTC Update Portal**, we found that the IRS had successfully deployed the necessary tools and implemented procedures to detect software vulnerabilities for both the CTC Update Portal and SADI system. However, security vulnerabilities were not timely remediated. For the CTC Update Portal, we found that 1,334 (312 unique) critical vulnerabilities spread across nine production servers exceeded the IRS policy for timely remediation. In addition, in the *CTC Update Portal Tier 3 Security Assessment Report* (Aug. 2021), the Security Risk Management organization issued a finding to the Web Applications Enterprise Services authorizing official stating that vulnerability scan reports identified 412 critical- and 508 high-severity security vulnerabilities. In response to this finding, the Enterprise Operations function documented a POA&M with a planned completion date of December 2022.

For the SADI system, we found that 492 vulnerabilities spread across 14 production servers exceeded the IRS policy for timely remediation. Specifically, our analysis of the vulnerability scan report found the following:

- 484 (44 unique) critical vulnerabilities spread across 11 production servers that exceeded the IRS policy of 30 calendar days for remediation.
- 6 unique high vulnerabilities spread across two production servers that exceeded the IRS policy of 90 calendar days for remediation.
- 2 unique medium vulnerabilities impacting one production server that exceeded the IRS policy of 120 calendar days for remediation.

Each of the vulnerabilities that were not timely remediated are being tracked via active POA&Ms with planned completion dates ranging from December 31, 2021, to December 1, 2022. Failing to timely remediate security vulnerabilities could compromise the security posture of the CTC Update Portal and SADI system and could lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing, all of which compromise the integrity, confidentiality, and availability of the system.

In our audit of the **TDC platform**, we found that not all critical security vulnerabilities were timely remediated. The MSP uses a scanning tool to identify security vulnerabilities on the customer engagement platform. Identified vulnerabilities are tracked with a software tool that captures when a ticket is created and resolved, among other information. We requested and received a report that identified all security vulnerabilities discovered from July 2016 through February 4, 2022, to determine whether they were timely remediated.

The MSP documented 177 security vulnerabilities in its issue tracking report. Of 177 security vulnerabilities, 162 included a severity rating – nine critical, 52 high, 74 medium, and 27 low. The MSP did not provide a severity rating for the remaining 15 security vulnerabilities. However, 13 of 15 security vulnerabilities were remediated in less than 15 calendar days, which met the minimum required remediation time frame for critical vulnerabilities. As a result, we included them in our population for review, giving the MSP credit for timely remediating the 13 security vulnerabilities. In total, we reviewed 175 security vulnerabilities and determined that the MSP did not timely remediate four (2 percent) critical security vulnerabilities. The remediation time ranged from 16 to 42 calendar days, averaging 24 calendar days. All four critical security vulnerabilities are related to security updates for the same type of servers.

In addition, we found that the customer engagement platform was not running the latest version of antivirus software. We obtained screenshots of the MSP's dashboard to identify the version of the antivirus software running on the customer engagement platform and conducted research on the antivirus software vendor website to identify the most current version of the antivirus software available. Our comparison of the antivirus software versions determined that MSP personnel did not install two critical- and three high-severity rated antivirus software releases and were using an outdated version of the antivirus software for approximately one year. This potentially affected 43 production servers on which the TDC platform resides.

Management Action: In March 2022, MSP personnel upgraded the customer engagement platform with the latest antivirus software version.

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.

In Fiscal Year 2022, TIGTA and the GAO performed three audits of system configuration management controls. In our audit of **mainframe platforms**, we reviewed the process flow and

associated roles and responsibilities for managing and documenting change requests (*i.e.*, emergency, standard, normal, and Tier I code promotion) approved for implementation and subsequent scheduling of the deployment. We found that change management controls for standard, normal, and Tier I code promotion change requests were working as intended. Between October 2021 and March 2022, there were 69 moderate- to high-risk–level code promotion changes implemented on the production mainframe platforms. Of these, we judgmentally sampled nine and evaluated whether they met minimum agency requirements related to change management policies and procedures. We determined that all nine of the code promotion changes satisfied minimum agency change management requirements and were appropriately approved.

However, we found that change management controls for emergency change requests need improvement. We evaluated three moderate-risk emergency change requests that were implemented between January and March 2022 and determined that two did not satisfy minimum agency requirements. We reviewed two Priority 2 incident tickets that were created in the Knowledge Incident/Problem Service and Asset Management tool on February 24, 2022, and March 3, 2022, relating to work stoppages on an application supported by the [redacted] platform. For both incidents, the IRS failed to properly document the required executive-level approval due to the urgency of implementing the required code fixes. Without following the change management procedures, there is an increased risk that changes could expose taxpayer data to unauthorized access or unauthorized data sharing.

In addition, we found that the configuration compliance criteria being used is no longer supported. [redacted][38].

In our audit of the **CTC Update Portal**, we found that configuration compliance controls are insufficient. We reviewed the CTC Update Portal's configuration setting scanning tool dashboard and identified that 14 (64 percent) of 22 production servers were noncompliant because they failed a high-risk compliance check related to the NIST Configuration Management security control family.[39] In response to this configuration compliance issue, the IRS documented a POA&M with a planned completion date of February 2022.

For the SADI system, we found that all 185 production servers were noncompliant for either failing high-risk compliance checks or having weighted compliance scores less than 90 percent. The failed high-risk compliance checks (183 production servers) were related to the NIST Configuration Management and Risk Assessment security control families. The two POA&Ms that were created to track the mitigation of these high-risk configuration compliance issues were completed in November 2021 and are awaiting final validation and closure from the Cybersecurity function. The two remaining production servers were noncompliant due to having

[38] The Defense Information Systems Agency was unable to provide an exact time, but it confirmed that the [redacted].

[39] We also found that each of the CTC Update Portal's 22 production servers had a weighted compliance score above 90 percent.

weighted compliance scores of less than 90 percent based on the total number of failed medium-risk and low-risk compliance checks.

In addition, we found that the configuration setting scanning tool report provides limited historical information, such as client last seen dates. Our review of the scan report determined that the IRS does not keep track of when a configuration compliance issue was first seen or remediated. Configuration compliance issues that are not remediated can allow an attacker the opportunity to access and control servers.

In its audit of the **IRS's internal control over financial reporting**, the GAO identified one deficiency related to configuration management controls. The GAO reported that the IRS did not configure the use of a security mechanism to help protect the integrity of its systems.

Network monitoring and audit logs

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

In Fiscal Year 2022, TIGTA performed three audits involving network monitoring and audit logging. In our audit of the **TDC platform**, we found that audit trails are not being reviewed. Cybersecurity function's Counter Insider Threat Operations branch management stated that audit trail reviews are not being conducted because their personnel's roles and permissions were not properly set up in the network traffic, database, and analytics tool by the Cybersecurity function's Architecture and Implementation group. However, the Architecture and Implementation group provided screenshots from the tool that showed the roles and permissions were set up for Counter Insider Threat Operations personnel.

Counter Insider Threat Operations branch management also stated that they did not perform audit trail reviews because the audit records in the network traffic, database, and analytics tool have a data integrity issue whereby they did not contain Taxpayer Identification Numbers, causing inaccuracies. We reviewed the *TDC Audit Worksheet* (Sept. 2020), which identifies the type of data an audit record should contain. A review of the document determined that only certain audit records contain Taxpayer Identification Numbers, explaining why some of the audit records did not contain them.

In our audit of **cloud computing services**, we found that [redacted][40].

[40] [redacted].

[redacted].

[redacted]. Specifically, [redacted].[41] [redacted].

In addition, we found that [redacted].

Furthermore, we found that [redacted].

In our audit of the **CTC Update Portal**, we found that the CTC Update Portal experienced a complete system outage for approximately 28 hours. On August 8, 2021, multiple IRS servers, to include the CTC Update Portal, were approved for downtime to allow for server patching and system reboots. During this approved downtime, monitoring functions were disabled to prevent ticket generation. Following the maintenance period, monitoring services were re-enabled with the assumption that monitoring would detect if servers were down. As part of the IRS's infrastructure monitoring policy, servers are pinged every five minutes, and a critical event ticket is generated if a server misses two ping cycles.

However, the CTC Update Portal's servers failed to properly come back online, and the issue was not detected due to its Internet protocol addresses not being added to the monitoring list. As a result, the CTC Update Portal project team was unaware of the outage until the morning of August 9, 2021. During the 28-hour CTC Update Portal outage, users of approximately 240,000 unique Internet protocol addresses who successfully authenticated via the SADI system were unable to access the CTC Update Portal's public-facing website.

Management Action: Following the outage, ping monitoring has been deployed to all CTC Update Portal servers to prevent a similar issue from happening in the future. In addition, the Monitoring Solutions branch is investigating automating the ping monitoring process in an effort to reduce human error.

[41] [redacted].

Insider threats

An insider threat is current or former personnel (*e.g.*, employee and contractor) or other business partner who has or had authorized access to an organization's network, systems, or data and could intentionally misuse that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. An insider threat program is intended to deter personnel from becoming insider threats; detect insiders who pose a risk to the organization's resources, including classified information, personnel, and facilities; and mitigate the risks through early intervention and proactive reporting and referral of information.

During Fiscal Year 2022, TIGTA performed an audit involving insider threats. We initiated an audit to **evaluate the effectiveness of the insider threat capabilities and follow up on prior audit recommendations**.[42] After the Calendar Year 2010 leak of classified material by a U.S. Army intelligence analyst, the President issued Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (Oct. 2011). The Executive Order created the National Insider Threat Task Force and directed all agencies that operate or access classified computer networks to designate a senior official to oversee the safeguarding of classified information and establish an insider threat detection program. In Fiscal Year 2016, the IRS began implementing an insider threat capability, and in Fiscal Year 2019, it was incorporated into the *IRS Integrated Modernization Business Plan* and renamed the User Behavior Analytics Capability (UBAC).

We reviewed all incidents documented in the Counter Insider Threat cyber threat management system and identified 229 incidents that occurred from March 2020 through December 2021 that UBAC analysts cataloged into 25 categories (*e.g.*, behavioral risk classification and verbal threats). The primary document used to capture an incident is the *User Behavior Analytics Capability Anomaly Report*. We determined that UBAC analysts performed appropriate reviews of the incidents, documented the reviews in the anomaly report, and either escalated the incidents as necessary or closed the incidents if the analysts determined the risk of insider threats was low. In addition, we reviewed the anomaly report for each of the incidents and determined that 109 (48 percent) of 229 incidents were forwarded to the TIGTA Office of Investigations for review and possible investigation.

After TIGTA investigates a referral, a Report of Investigation is provided to IRS management. We determined that the IRS recorded TIGTA feedback in anomaly reports for only three (3 percent) of 109 incidents. By not receiving feedback in anomaly reports on referred incidents, the UBAC team does not know if it produced credible incidents of potential insider threats. The stakeholders' feedback could improve future incidents produced by the UBAC.

Logical partitions

A logical partitioned server can reduce the number of servers that are needed within an enterprise. Logical partition is the division of a computer's processor, memory, and storage into multiple sets of resources so that each set of resources can be operated independently with its own operating system and application. Typically, logical partitions are used for different

[42] TIGTA, Report No. 2022-20-055, *Improvements Are Needed for an Effective User Behavior Analytics Capability* (Sept. 2022).

purposes, such as database or server operation or to separate test and production environments.

In Fiscal Year 2022, TIGTA performed an audit covering logical partitions. In our audit of **mainframe platforms**, we found that production logical partitions are not in compliance with configuration requirements. The IRS relies extensively on two mainframe platforms to support its financial and mission-related operations. The [redacted] platform employs an infrastructure that includes mainframe computers operating with [redacted]. The [redacted] platform provides primary support for application programs and databases, including the IMF and the Automated Collection System, among others. The [redacted] platform employs an infrastructure that includes mainframe computers operating with [redacted]. The [redacted] platform supports major tax applications, which include the Electronic Filing System and the Integrated Data Retrieval System.

The Department of Homeland Security's *Continuous Diagnostics and Mitigation, Agency-Wide Adaptive Risk Enumeration Technical Design Document* (Nov. 2017), states that each vulnerability found on a network should be given a numeric score, meant to represent the risk of not mitigating that vulnerability. According to the IRS, hosts are considered compliant if their weighted compliance score is 90 percent or higher with no high severity ratings.

[redacted]. The average weighted configuration compliance score for all [redacted] platform production logical partitions was [redacted] with configuration requirements.

In April 2022, the IRS also reported that both [redacted] production logical partitions were compliant with average weighted configuration compliance scores of [redacted].

[redacted] production logical partitions

We reviewed the February 2022 configuration compliance reporting dashboard results for the [redacted] active production [redacted] logical partitions and found that [redacted] check or having a weighted compliance score of less than [redacted]. More specifically, we found that [redacted].

In September 2020, we reported that the follow-on solution to replace the current [redacted] tool had been delayed due to resource constraints and competing priorities.[43] The IRS agreed with our recommendation to prioritize resources to ensure that the [redacted] follow-on solution is delivered without further delay in order to maintain the confidentiality, integrity, and availability of data and information processed by the

[43] TIGTA, Report No. 2020-20-045, *Mainframe Computing Environment Security Needs Improvement* (Sept. 2020).

[redacted] platform. The IRS began using [redacted] to validate the configuration compliance settings for the [redacted] logical partitions.

We reviewed the [redacted] configuration setting scan reports from October 2021 through March 2022 and determined that there were a total of [redacted] we found [redacted].[44] We also found [redacted]. Failing to timely remediate medium- and high-risk [redacted] security vulnerabilities could compromise the security posture of the mainframe platform and could lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing, all of which compromise the integrity, confidentiality, and availability of the platform.

[redacted] production logical partitions

We reviewed the February 2022 configuration compliance reporting dashboard results for the [redacted] production [redacted] logical partitions and found that both were [redacted]. The Cybersecurity function's Counter Insider Threat office has been unable to validate the configuration setting compliance since December 2021 due to the Enterprise Operations function not submitting evidence to support that the security controls are in place and working as intended. Without completing the required monitoring of all production logical partitions, the IRS cannot adequately define its current security posture because [redacted].

[redacted] production logical partitions

[redacted].[45] [redacted]. In July 2021, the IRS reported that this planned corrective action for [redacted] had been fully implemented and closed the recommendation. However, when asked to provide evidence of the completed [redacted] has not been used for at least the past five calendar years. Management further stated that not using the required [redacted] was an administrative oversight. Following our inquiry, the Counter Insider Threat office began using the required [redacted], to validate the configuration compliance for the [redacted] logical partitions.

We reviewed the results of the [redacted] completed on March 31, 2022, for both [redacted] logical partitions and found that [redacted] partitions [redacted]. As a result, we determined that [redacted] logical

[44] Several scanned mainframe logical partitions can have the same unique finding (*i.e.*, vulnerability). Therefore, one unique finding can occur multiple times across the mainframe platform.

[45] TIGTA, Report No. 2016-20-050, [redacted] (July 2016).

partitions [redacted]. In April 2022, the IRS reported that the [redacted] logical partitions were satisfying agency configuration compliance requirements with an average weighted score [redacted]. However, we determined that this reporting only included assessment results from the [redacted]. As a result, the IRS inaccurately reported the configuration compliance status for the [redacted] logical partitions.

Configuration compliance validation

The IRS uses a Defense Information Systems Agency published [redacted] for the [redacted] to validate the configuration compliance settings.[46] The IRS uses a similar Defense Information Systems Agency published [redacted]. In August 2020, the Counter Insider Threat office implemented a new procedure for the [redacted].

Agency security policies state that, if a security requirement cannot be met, then a risk-based decision is needed for the deviation from the existing policy. When asked if a risk-based decision for this deviation from an existing security requirement was approved, the Director, Cybersecurity Operations, stated that there was no risk-based decision. He further stated that, [redacted].

However, in September 2020, the IRS agreed with our recommendation to ensure that the required [redacted] for the [redacted].[47] In November 2020, the IRS reported that a planned corrective action had been implemented to [redacted] and closed the recommendation. We determined that using static documentation does not meet the intent of the security requirement for [redacted]. By failing to properly verify and [redacted], the security posture and the availability of the system could be compromised. In addition, 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.

[46] [redacted].

[47] TIGTA, Report No. 2020-20-045, *Mainframe Computing Environment Security Needs Improvement* (Sept. 2020).

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.

During Fiscal Year 2022, TIGTA performed three audits involving security policies, procedures, and documentation. In our audit of **vulnerabilities on network devices**, we found that the IRS does not have a formal process to document how to identify when changes occur in the IRS networks or to coordinate with the Enterprise Vulnerability Scanning group so that changes can be made to the vulnerability scanning tool.[48] We reviewed various reports of active network blocks maintained by the User and Network Services (UNS) function and compared them to a list of network blocks scanned in April 2021 by the IRS's enterprise vulnerability scanning tool.[49] There were [redacted]. Failing to have a process that identifies changes to active network blocks requiring vulnerability scanning increases the risk that information technology systems not receiving vulnerability scans could be exploited, potentially exposing taxpayer data and information.

In our audit of **network segmentation**, we found that key development artifacts were not completed or lacked critical content. According to the Enterprise Life Cycle (ELC) framework, the simplified design specification report and the system test plan are required documents that are to be developed during the development process. The simplified design specification report is the required document to record a project's software design solution. A system test plan summarizes the complete test effort for the information system release.

While the SEG project's simplified design specification report was approved in December 2020, it does not describe the complexity of the design nor the limits of the design to segment IMF from non-IMF users. In addition, the report does not describe the relationship between the two access control software and the Mainframe 1 security software. Further, the simplified design specification report does not mention the IMF-specific Online 5081 user security groups or system resources that are involved to deploy network segmentation for the IMF. As a result of the IRS not updating the simplified design specification report to reflect the SEG project's current high-value asset focus, it is not complete or relevant because critical design details related to the high-value assets are not included.

When we asked the SEG project team to provide us with the SEG project's system test plan, they provided a system test plan with identical testing content as the Unified Access project's *System Test Plan* (Sept. 2020); no additional testing was documented after the Unified Access project

[48] A change could be starting or stopping the use of a network block, adding new segments to an existing network block, or consolidating multiple smaller networks into a larger network block.

[49] We are substituting the term network block in place of the technical term Classless Inter-Domain Routing Blocks, which are groups of Internet protocol addresses that share the same prefix and contain the same number of bits.

testing was completed in September 2019. In a follow-up discussion, the SEG project manager clarified that additional monthly testing was conducted from June through September 2020, but the tests and results were not documented. This statement is consistent with seven e-mails that were subsequently provided, dated prior to deployment, which identified various actions that UNS function's Network Engineering personnel completed. Therefore, the documentation was insufficient for an independent reviewer to be able to analyze the results and conclude that key SEG project requirements were adequately tested.

In our audit of **mainframe platforms**, we found that there was a configuration settings checklist adjudication process for the vendor-provided [redacted] checklist. However, the IRS stated that the review process is less formal than what has been recently developed for Tier II devices as part of the Continuous Diagnostics and Mitigation program. Configuration settings checklist adjudication is a complex process involving numerous activities to successfully scope, review, approve, and implement approved [redacted]. In addition, we found that the IRS has published guidance related to checklist adjudication, which provides procedures for developing compliance adjudication packages for review and approval.[50] However, we determined that this guidance does not include any information related to checklist adjudication for the mainframe platforms. Without ensuring that this process occurs, critical and unique security requirements may not be applied to IRS mainframe systems.

Systems Development and Information Technology Operations

In carrying out its responsibilities of administering the tax laws, the IRS relies extensively on information technology investments to support its mission-related operations. The IRS's ability to provide high-quality taxpayer service and maintain the integrity of the tax system requires modern, secure, and nimble operations as well as a sustained and talented workforce. Many emerging trends offer challenges and opportunities for the IRS, including changes in the taxpaying public and its expectations, technological disruptions, shifts in the workforce, and an increasingly globalized and interconnected world.

TIGTA and the GAO performed several audits that assessed systems development and information technology operations at the IRS. These audits covered information technology asset management, governance and project management, information technology service and helpdesk requests, risk management, implementation of corrective actions, updating and modernizing operations, and Coronavirus Disease 2019 (COVID-19) response.

Information technology asset management

Information technology 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. Information technology asset management includes information technology SCRM and information technology asset inventory management.

[50] IRS, *Configuration Settings Management, Checklist Adjudication Standard Operating Procedures*, Version 0.43 (Aug. 2021).

Information technology SCRM

Information technology relies on a complex, globally distributed, and interconnected supply chain ecosystem that is long, has geographically diverse routes, and consists of multiple tiers of outsourcing. Information technology SCRM is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information technology product and service supply chains. Information technology supply chain risks may include counterfeits, tampering, theft, and insertion of malicious software and hardware as well as poor manufacturing and development practices.

During Fiscal Year 2022, TIGTA performed an audit covering information technology SCRM. We initiated an audit to **evaluate the IRS's efforts to identify, assess, and mitigate information technology supply chain risks**.[51] The Treasury Department has overall responsibility for developing the strategy and guidance policies to manage information technology SCRM for the department and its bureaus. As of September 2021, the IRS stated that the Treasury Department is still finalizing the guidance policies as well as completing its internal reviews before they are shared with its bureaus for review and feedback. Once approved, the IRS plans to leverage the Treasury Department's guidance policies to create its own.

While the IRS is only in the beginning stages of information technology SCRM planning, we found that it has taken some preliminary steps to address information technology supply chain risks. For example, the Cybersecurity function has conducted some initial research on the Internet for SCRM frameworks that are publicly available to understand what other Federal agencies (*e.g.*, the Department of Defense and the General Services Administration) are undertaking to address information technology supply chain risks. In addition, the IRS created a draft *Supply Chain Risk Management (SCRM) Strategy*, Version 0.1 (May 2021). The strategy will provide a strategic roadmap for implementing effective information technology SCRM capabilities, practices, processes, and tools within the IRS in support of its vision, mission, and values.

Although the IRS has taken some actions to address information technology supply chain risks, we found that additional steps could be taken in the short term to better manage and mitigate information technology supply chain risks. For example, the IRS has not implemented any security controls that would help mitigate information technology supply chain risks. The absence of these security controls increases the risk for disruptions to the IRS's operations and to meet its mission of helping taxpayers comply with their tax responsibilities and enforcing the tax laws with integrity and fairness to all. While waiting on final Treasury Department guidance, the IRS could increase organizational awareness by providing training regarding processes and controls that can help mitigate information technology supply chain risks. As part of its information security program planning, the IRS could also begin documenting relevant SCRM controls and integrating them into ongoing security assessment and authorization activities.

In addition, we identified further steps that the IRS could take in the short term that will help improve its current information technology SCRM posture. We reached out to personnel and management from the Department of Energy and the General Services Administration regarding

[51] TIGTA, Report No. 2022-20-009, *More Interim Steps Could be Taken to Mitigate Information Technology Supply Chain Risks* (Feb. 2022).

their efforts in information technology SCRM. They provided examples implemented at their respective agencies that might help the IRS mitigate some supply chain risks.

- The Department of Energy established a risk-based approach to conduct greater diligence on higher risk vendors.
- The General Services Administration, which maintains the Federal Acquisition Regulation, shared contractual language that requires vendors to provide a SCRM plan detailing how they will address counterfeit and illegally modified products as well as how they will reduce and mitigate information technology supply chain risks, where applicable.

At the end of our audit work, the IRS reached out to the Social Security Administration regarding its best practices to better manage supply chain risks. Personnel from the Social Security Administration provided contractual language they use for solicitations and awards that are subject to supply chain risk assessments.

We also found that the IRS is not reducing its risk exposure when procuring information technology because contracts do not consistently include clauses intended to manage supply chain risks. Personnel from the Office of the Chief Procurement Officer provided a list of 14 contract clauses to manage supply chain risks. Five of the clauses (*e.g.*, basic safeguarding of covered vendor information systems, prohibition on contracting for certain telecommunications, and video surveillance services or equipment) are from the Federal Acquisition Regulation. The remaining nine contract clauses (*e.g.*, notification of change in vendor personnel employment status and submission of security forms and related materials) were created by the IRS and included in the *IRS Acquisition Policy, FY [Fiscal Year] 2021 edition*, Version 2.0 (June 2021). However, while we recognize that not all contract clauses available for use may be applicable, we found that the use of contract clauses in similar procurement contracts detailing vendor responsibilities to protect the IRS from information technology supply chain risks are not consistently applied.[52]

We selected a judgmental sample of 15 contracts procuring information technology products and services from a population of 114 IT organization contracts signed between December 2020 and March 2021.[53] Twelve of 14 potential contract clauses addressing supply chain risks were included in some, but not all six, of the contracts procuring software support and maintenance in our sample. Similarly, seven of 14 potential contract clauses addressing supply chain risks were included in some, but not all four, of the contracts procuring comparable services to support application development activities.

In addition, we identified one contract procuring [redacted] products that included nine of 14 potential contract clauses addressing supply chain risks, including references to safeguards against unauthorized disclosure of sensitive but unclassified information and references to not using any hardware, software, or service developed by a prohibited software development and distribution company. When solely procuring [redacted] products, we do not see the relevance or

[52] Our review of contracts included their respective modifications, where applicable, because some contracts were created from a Governmentwide acquisition contract, which were awarded prior to the required use of some of the supply chain procurement contract clauses. In these cases, the modifications subsequently included some of the required procurement contract clauses after the initial contract was awarded.

[53] The last enacted or requirement date for the use of 14 contract clauses was November 2020. We selected contracts signed after that date for review to ensure the clauses' potential inclusion in the contracts.

application of including these clauses in the contract.[54] Continued reliance on weak SCRM controls could potentially compromise the confidentiality, integrity, and availability of the IRS's information systems as well as increase the risk of disruptions to its mission-critical functions.

Information technology asset inventory management

Information technology asset inventory is the way an organization lists and provides details of the assets it owns. Information technology 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 information technology 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 information technology assets it owns and that the assets are being used in the most efficient and cost-effective manner.

During Fiscal Year 2022, TIGTA performed an audit covering information technology asset inventory management. In our **insider threat capabilities** audit, we found that the IRS did not have a complete inventory of systems to monitor for its UBAC. In September 2021, the UBAC progressed from initial operating capability to full operating capability. The IRS defined full operating capability as the UBAC being able to provide 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 UBAC should be able to provide proactive identification of emerging insider threats through the use of real-time intelligence information and analytics to mitigate risks to data and systems arising from insider threats.

During our audit, the IRS initially was unable to provide an accurate number of systems with Federal tax information and Personally Identifiable Information. Following our request in January 2022, we obtained a list from the Enterprise Security Audit Trails team in March 2022 that contained 365 systems. However, in May 2022, the Enterprise Security Audit Trails team reviewed the accuracy of the number and naming conventions of the systems on the list and provided an updated list that contained 351 systems. We reviewed the list of systems and determined that 234 (67 percent) of 351 systems with Federal tax information and Personally Identifiable Information were missing from the UBAC inventory and were not subject to user behavior analysis.

By not having access to system data for risk indicators and a complete inventory of systems that store or process Federal tax information and Personally Identifiable Information, the UBAC team's improvements to its analytics may be limited and some systems may not have specific use cases for analyses. Consequently, the IRS may be unable to identify insider threat activity that may negatively affect the confidentiality, integrity, or availability of the IRS's information or information systems. An effective insider threat capability is vital to protect taxpayer information and IRS operations.

[54] The remaining four contracts did not procure similar types of information technology products or services. As a result, we were unable to make an association with other contracts to complete our analysis on contract clause usage.

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.

Governance

A governance board is a chartered body responsible for conducting governance as set out in its governance board charter. Executive steering committees are top-level governance boards chaired by IRS senior leadership and have the authority to make key governance decisions or delegate decisions down to a lower governance board. While governance boards do not assist with the day-to-day activities of the IT organization's projects and programs within a portfolio, governance boards play an important role in assisting the programs by monitoring cost, schedule, scope, and risk.

In Fiscal Year 2022, TIGTA performed an audit covering governance. We initiated an audit to **evaluate the effectiveness of the IT organization's planning and governance to modernize and secure systems in accordance with the ARPA**.[55] The ARPA provided the IRS with approximately $1.8 billion in additional funding for the implementation of certain provisions, such as the administration of advance payments and taxpayer assistance. Much of this additional funding will remain available to the IRS through Fiscal Year 2023. The IRS's IT organization was allocated approximately $1.2 billion of the $1.8 billion.[56]

We found that governance boards provided oversight of the ARPA programs and followed the IRS's policy and procedures. We surveyed a judgmental sample of governance board members about the roles and responsibilities of the Information Technology Executive Steering Committee and two subordinate governance boards.[57] According to governance board members, the boards' primary purpose is to ensure that the programs' objectives are met and risks are managed appropriately. The governance boards also provide decision-making support for the programs. The Information Technology Executive Steering Committee oversees the delivery and annual baseline approval of the ARPA program capabilities and the timeline assigned to the Information Technology Modernization portfolio. The subordinate governance boards escalate risks to the higher governance boards when risks are unmitigated or have challenges that need attention. Governance board oversight support is provided through meetings where program status and risks are discussed.

During these meetings, the IT organization program management or program representatives inform governance board members of key topics about the programs subject to oversight; also, meeting minutes are maintained. We reviewed documentation for Information Technology Executive Steering Committee meetings held during September 2021 through March 2022 and two subordinate governance boards' meetings held during February and March 2022. Our

[55] TIGTA, Report No. 2022-27-045, *The IRS Effectively Planned to Use and Provide Oversight of the American Rescue Plan Act Funds; However, Subsequent Reallocation of Modernization Funds Resulted in Significant Replanning* (Sept. 2022).

[56] The IT organization received $1 billion for modernization, $100 million for administration of the Advance CTC provisions, and approximately $121 million for administration of the third round of economic impact payments.

[57] According to IT organization senior management, the Information Technology Executive Steering Committee serves directly as a governance for one of the ARPA programs we tested. Our audit test of governance board meeting documentation shows that the Associate CIOs provide oversight to the program.

review of the documentation determined that meetings were held regularly. The meetings included input from program management, program representatives, subject matter experts, and governance board members including IT organization leadership. The meetings allowed an opportunity for individuals to discuss relevant issues (*e.g.*, program risk, baseline scopes and schedules, approvals, and change requests) that helped to provide an integrated view of program status. While some meeting documentation noted risk discussions, we did not note risk escalation details in any governance board meeting documentation. Therefore, we were unable to analyze how the governance boards handle risk escalation.

In addition, we reviewed baseline information captured in governance board meeting documentation and information from the IRS's baseline capabilities tracking tool used by the IT organization to determine if the information matched. The tool reflects the health status of IT organization programs by considering key elements of management and performance such as cost, schedule, scope, and existing or potential risks. The tool also shows recordings of baseline approvals and baseline change request approvals. In our review, we compared three baseline approvals and three baseline change request approvals for six ARPA programs captured in governance board meeting documentation to the same information recorded in the tool.[58] Our testing covered meeting documentation and tracking tool records from June 2021 to March 2022. We found that approvals from the two different sources of governance board approval information agreed.

The governance boards are also responsible for baseline approvals and changes. This includes approving costs, schedules, and scope plans for a given fiscal year for projects and programs within a respective portfolio, and addressing any requests for re-baselining due to unforeseen circumstances throughout the year.[59] We reviewed baseline documentation to determine if the Information Technology Executive Steering Committee approved the ARPA program baseline capabilities for Fiscal Year 2022. Presentation documentation from the September 2021 and January 2022 Information Technology Executive Steering Committee bi-monthly meetings show that as a result of the meetings, the executive steering committee approved 12 of 19 ARPA programs' baselines and approved with conditions the remaining seven program baselines. According to IT organization senior management, the Information Technology Executive Steering Committee was expected to fully approve the seven ARPA programs' baselines with conditional approvals during the March 2022 Information Technology Executive Steering Committee meeting. However, the March and May 2022 meetings were cancelled, but an ad hoc meeting was held in June 2022 to re-baseline some of the ARPA programs. As a result of the potential reallocation of approximately $400 million in ARPA funding previously aligned to modernization efforts, many capabilities could remain incomplete.

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

[58] We did not validate the accuracy and reliability of the data within the tracking tool.

[59] According to IT organization senior management, the CIO makes the decisions when establishing cost at the baseline level. However, at the governance level, there is management within the already established cost.

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 2022, TIGTA and the GAO provided coverage of information technology project management in six audits. We initiated an audit to **determine the progress of the IRS's Next Generation Infrastructure (NGI) program**.[60] The NGI program is part of the *IRS Integrated Modernization Business Plan*. NGI is a series of packaged initiatives to support a more efficient, scalable, and flexible architecture implemented through advanced information technology infrastructure tools and technologies. The NGI program is comprised of multiple capabilities, including continuous integration/continuous delivery pipeline, the centralized code repository, the standard stack methodology, the container solution architecture, and the legacy code conversion strategy. The technology is planned to allow more interactive relationships between taxpayers and IRS employees. We found that program management for the NGI program was decentralized. No clear or comprehensive program management structure was established for the NGI program because the program relies upon five IT organization functions to implement and manage capabilities. The five functions responsible for the daily operations of NGI capabilities are Enterprise Architecture, Server Services and Support, Development Operations (*i.e.*, DevOps), Technology Strategy Management, and Technical Integration Operations. This decentralized approach makes it difficult to determine ultimate responsibility and accountability over the NGI program.

The management of NGI capabilities (*e.g.*, legacy code conversion strategy and standard stack capability) was inconsistent. Each of the capabilities were at different stages in developing and validating metrics. Formal charters clearly defining the executive sponsor role for the NGI program or the related NGI capabilities were not yet completed when funding was cut in Fiscal Year 2020. Because there was no formally defined NGI program charter, the metrics were not properly collected for the entire NGI program. Even when metrics were collected and reported, the metrics were not used for management decision making. In addition, the metrics for each of the capabilities did not tie into the overall objectives of the NGI program.

The NGI program office did not monitor the implementation of all the capabilities. The decentralized structure of the program contributed to this issue. For example, NGI capabilities do not maintain formal risk registers, and NGI capabilities' project schedules are not reviewed or approved by the NGI program office. During our audit work, we notified NGI management that the continuous integration/continuous delivery pipeline project management plan did not follow the standardized project management template. The IRS acknowledged that the project plan was not in compliance and stated it would make necessary revisions.

While the *IRS Integrated Modernization Business Plan* monthly progress reports identified outcomes for NGI capabilities, the NGI program did not consistently monitor the performance of all of the implemented NGI capabilities. For example, the NGI program office was unable to provide supporting evidence to validate the implementation of NGI capabilities in a specific month and year for seven of nine implemented NGI tasks. Effective program management helps the IRS to coordinate technology investments in a cost-effective and efficient manner and facilitates current accurate reporting.

[60] TIGTA, Report No. 2022-20-001, *Some Next Generation Information Technology Infrastructure Capabilities Were Implemented, but Program Management Improvements Are Needed* (Nov. 2021).

We also found that performance metrics were not linked to overall performance measures. The NGI program reports the progress of the implemented capabilities in the *IRS Integrated Modernization Business Plan* monthly reports, but the NGI program has not established performance metrics for all NGI capabilities and did not link the existing performance metrics with the overall modernization performance measures. For example, the IRS used a combination of expert opinion estimates and automated tools to provide information on internal processes for the continuous integration/continuous delivery pipeline and standard stack capabilities, but the NGI program is not using this information as a performance metric. In addition, the IRS is still in the process of developing return on investment measures for one of the NGI capabilities. Without consistent performance reporting, the IRS may be unable to deliver planned capabilities on schedule.

In addition, we initiated an audit to **determine whether the methodology to estimate the Individual Tax Processing Engine project's velocity and delivery dates was effective and to follow up on the implementation of the independent verification and validation recommendations**.[61] We found that the methodology used in the Trajectory Model to estimate project velocity is consistent with industry best practices. The IRS established a Trajectory Model to track and monitor the Individual Tax Processing Engine project's velocity. The Trajectory Model was initially updated after the completion of every third product increment, a period of 30 weeks. In Product Increment-15 from October 28, 2020, through January 5, 2021, the Customer Account Data Engine (CADE) 2 Program Management Office began updating the Trajectory Model after every product increment, a period of 10 weeks, because the models were being used on a more frequent basis to track project progress. The Trajectory Model's methodology is based on the number of resources at each skill level, the expected output per week at each skill level, and number of weeks in a product increment. The Project Management Institute's *Project Management Institute Practice Standard for Project Estimating* (2011) defines six basic model inputs required to effectively manage project estimates. Figure 9 lists the six basic inputs with their descriptions and how the Trajectory Model accounts for each.

Figure 9: Trajectory Model Inputs

Inputs From Project Management Institute Standards	Input Description	How Inputs Were Applied in the Trajectory Model
Baseline Estimates	An approved plan for the project.	The Individual Tax Processing Engine project team developed the baseline estimate. The Trajectory Model compares the projected and actual output with the baseline estimate.
Approved Changes To Baseline	Approved changes to project scope, modify budget, revise schedules, or change project team.	The CIO approves baseline changes and the Individual Tax Processing Engine project team updates the assumptions and resources in the Trajectory Model.

[61] TIGTA, Report No. 2022-25-029, *The Individual Tax Processing Engine Project's Estimation Methodology Aligns with Best Practices and the Project Addressed the Independent Verification and Validation Recommendations* (Mar. 2022).

Inputs From Project Management Institute Standards	Input Description	How Inputs Were Applied in the Trajectory Model
Resource Plan	How human resources are defined, staffed, managed, controlled, and released.	The Trajectory Model maintains the Individual Tax Processing Engine project resources and their associated skill levels and projected outputs.
Work Performance Information	The actual amount of time and costs associated with achieving the project objectives.	Actual output is recorded in each update to the Trajectory Model.
Organizational Process Assets	The knowledge base or process asset library that contains the approved methodologies, processes, procedures, and templates used for managing the scheduling, costs, and resource estimates.	The Trajectory Model's assumptions contain the reference data used to create the Individual Tax Processing Engine velocity projections and the impact that resources will have on Lines of Code conversions.
Project Estimating Approach	Defines the approach for managing and monitoring the project estimates and forecasts.	This occurs outside the Trajectory Model. The CADE 2 Individual Tax Processing Engine project team meets to assess the impact of legislation, reallocation of resources, and other events on the project.

Source: TIGTA's analysis based on Project Management Institute guidance, discussions with CADE 2 and Individual Tax Processing Engine project management, and information contained in the Trajectory Model.

The standards also describe three activities that should be applied to initial and revised estimates: apply actuals; review and control; and re-estimate. These activities are accomplished in the Trajectory Model updates that are completed after every product increment. The CADE 2 Program Management Office updates the actual outcomes for each product increment and the current resource list and skill level and validates the assumptions used to estimate the project trajectory.

We found that an incorrect formula was used to calculate the work to be completed for Product Increment-14 through Product Increment-19 models from August 19, 2020, through October 12, 2021. We discussed the issue with the IRS and determined that the incorrect formula was used due to a copy and paste error. Despite the error and the corrections made, the overall project development end date was not affected.

Management Action: The IRS performed a comprehensive review of all formulas in the Trajectory Model and corrected the errors. The IRS stated that going forward it will have a secondary reviewer validate the formula updates.

In addition, we found that two of the independent verification and validation recommendations were addressed and one is in progress. In response to the Taxpayer First Act, the IRS contracted a third party to conduct an independent review of the CADE 2 program's Individual Tax Processing Engine project. In July 2020, the independent contractor completed its review and

made the following three recommendations to reduce risk and increase the likelihood of success for the Individual Tax Processing Engine project:

- Implement a more rigorous strategy around unit test coverage and data. We determined that the IRS addressed this recommendation.
- Make a concerted effort to externalize business rules where possible. We determined that the actions to address this recommendation are in progress.
- Resolve the disconnected approach between the Applications Development and the Enterprise Systems Testing functions for scenario testing. We determined that the IRS addressed this recommendation.

The independent verification and validation report stated that, if these recommendations were not addressed, the Individual Tax Processing Engine project will carry significant cost and timeline risk into the final stages of parallel validation.

In our audit of **network segmentation**, we found that insufficient management oversight allowed the SEG project to bypass mandated governance and development processes. The IRS refers to its development process as the ELC framework. The ELC framework is the workflow that projects follow to move an information technology solution from concept to production. The ELC framework includes five phases (*e.g.*, project initiation and system development), and each phase constitutes broad segments of work that encompass activities of similar scope, nature, and detail and provides for a natural breakpoint in the project life cycle. At the end of each phase, a milestone exit review is required.

In April 2020, the SEG project manager signed the *SEG Project Tailoring Plan* agreeing that the SEG project would follow the ELC framework's commercial off-the-shelf development path. The IRS uses this development path when prepackaged vendor-supplied software is used with little or no modification to provide all or part of the development solution. At that time, the SEG project team did not believe that sufficient time was available to complete the ELC framework phases and related artifacts by June 30, 2020 (*i.e.*, the initial completion date for deploying network segmentation for the IMF). As a result, UNS function management proposed combining ELC framework Milestones 1 through 4a, and the ELC office approved the process change.[62] Shortly thereafter, UNS function management approved completing the ELC framework and deploying network segmentation for IMF to production by September 30, 2020. In September 2020, the UNS function's Director, Network Engineering, approved the release of the SEG project to production. At that time, some of the mandatory ELC framework processes and artifacts were not completed, including:

1) The *Simplified Design Specification Report* was not completed prior to the SEG project's release to production and was not approved until December 2020. The *Simplified Design Specification Report* is the primary document to record a project's software design solution.

[62] ELC framework milestones are normally completed sequentially, with the next milestone beginning after the previous milestone exit review has been completed.

2) The UNS Governance Board had not completed, and subsequently did not complete, any of the required milestone exit reviews.[63] From October 2018 through deployment in September 2020, the board held only two meetings in which the SEG project team presented the project's status. According to the IRS, these oversight reviews were not held because the Associate CIO, UNS, and the SEG project's Executive Sponsor were briefed and received communications via Associate CIO briefings and monthly SEG project team meetings. However, the UNS Governance Board has several other executive and senior manager members that were apparently not briefed and did not fulfill their oversight responsibilities.
3) The UNS Governance Board had not approved the decision to release network segmentation for the IMF to production; in fact, the board's approval was not obtained prior to deployment.

The IRS maintains that the necessary sponsor and stakeholder approvals were obtained prior to deploying network segmentation for the IMF to production in September 2020. However, none of their actions equate to obtaining the UNS Governance Board's approval immediately prior to the deployment of the solution. The lack of an approved *Simplified Design Specification Report* during development, the lack of milestone exit reviews, and the lack of compliance with IT organization governance requirements regarding authority to launch releases to production are indicators of insufficient management oversight.

In our audit of the **CTC Update Portal**, we found that most ELC framework artifacts satisfied IRS requirements. We reviewed the project tailoring plans for both the CTC Update Portal and SADI system. The CTC Update Portal and SADI system's project tailoring plans listed 16 and 12 required ELC framework artifacts, respectively. While we found administrative issues with several ELC framework artifacts, we determined that 15 (94 percent) of 16 required CTC Update Portal and 11 (92 percent) of 12 required SADI system ELC framework artifacts satisfied IRS requirements. The administrative issues we found included: a tailoring decision incorrectly documented in the CTC Update Portal project tailoring plan; an unauthorized approver granting use of draft artifact; inaccurate security assessments during milestone exit reviews; artifact owners not timely approving artifacts prior to required milestone exit reviews; secondary and tertiary proxy approvers not formally documented; and not adhering to IRS artifact submission time requirements. However, the ELC framework process was generally effective in ensuring that both the CTC Update Portal and SADI system met accelerated deployment timelines in order to meet legislative requirements. Figure 10 summarizes the two ELC artifacts that did not satisfy IRS requirements.

[63] Members of the UNS Governance Board include the Deputy Associate CIO, UNS; the Director, Contact Center Support; the Director, Customer Service Support; the Director, Enterprise Field Operations; the Director, Network Engineering; the Director, Operations Service Support; the Director, Service Planning and Improvement; and the Director, Unified Communications.

Figure 10: Summary of ELC Artifacts That Did Not Satisfy IRS Requirements

Artifact Name	Artifact Description	Underlying Issues
CTC Update Portal Computer Operators Handbook	Provides all responsible personnel for the operation and support of a solution with operational instructions for supporting daily operations.	• The draft CTC Update Portal Computer Operators Handbook was not completed prior to the CTC Update Portal's Release 1 production deployment date of June 21, 2021. The process owner approved the draft CTC Update Portal Computer Operators Handbook 43 days later on August 3, 2021.
SADI 508 Accessibility and Mitigation Package	Explains the approach and tests to be used to ensure that the solution being developed or implemented will be accessible to users with disabilities and demonstrates compliance via actual test results.	• The process owner did not sign the 508 Package Sign-Off Sheet prior to the SADI system's June 21, 2021, production deployment due to material concerns regarding the number of test procedure failures. The Project team needed additional time to address the concerns and the process owner approved the SADI 508 Accessibility and Mitigation Package on September 7, 2021, 78 days after its production deployment. • Did not adhere to established ELC artifact timelines (completed package not submitted on time).

Source: TIGTA's analysis of the CTC Update Portal and SADI system ELC artifacts.

By not adhering to the approved ELC framework process, including meeting minimum ELC framework artifacts requirements, the projects did not comply with IRS guidelines and overall goals.

Milestone exit memorandum

The milestone exit memorandum provides a list of the security artifacts that were included as part of the review, any artifacts that require additional work, and an exit recommendation. The Director of the Security Risk Management organization signed conditional milestone exit memoranda for both the CTC Update Portal and SADI system.[64] Both memoranda included language that stated, "Cybersecurity will conduct a final review and concur with mitigated findings from outstanding critical risks resulting from security scanning, and Cybersecurity will provide concurrence to go live." When asked if the Cybersecurity function provided this concurrence for the CTC Update Portal and SADI system to go live, Security Risk Management organization management stated that the information was contained on the signature page on each system's preliminary security analysis report. Our review of these documents did not find any evidence in which the Cybersecurity function provided explicit concurrence for either the CTC Update Portal or SADI system to operate in the production environment. In a following discussion, the Security Risk Management organization stated that the appropriate documentation was completed but acknowledged that the memorandum template required updated language to reflect the current process in order to provide explicit concurrence to operate in the production environment.

By providing system authorizing officials with explicit concurrence to operate in the production environment, there is minimal risk that critical and high-risk security findings might not have

[64] The CTC Update Portal's memorandum was not signed until 6.5 hours after the Web Applications Governance Board voted unanimously to approve the CTC Update Portal's milestone exit.

been mitigated or that the authorizing officials are basing their decision to grant an Authorization to Operate on inaccurate or outdated information.

Management Action: On January 28, 2022, the IRS revised the language contained in the milestone exit memorandum template to accurately align with the current process for the Security Risk Management organization to provide explicit concurrence to operate in the production environment.

In our **vulnerabilities on network devices** audit, we found that vulnerability remediation oversight is insufficient. The IRS does not effectively oversee vulnerability remediation across the enterprise. Specifically, the Patch and Vulnerability group only provides remediation oversight for high-priority, enterprise-wide vulnerabilities and remediation efforts for high-visibility programs. The group did not verify or monitor the remediation efforts for all vulnerabilities. In addition, the group did not consistently track and report vulnerability remediation metrics.

Patch and Vulnerability group personnel stated that they helped develop requirements for a dashboard within the centralized reporting application so that it could provide business units with the most accurate, timely, and updated vulnerability information. In addition, the group incorporated monthly and quarterly trending data into the dashboard for users to measure enterprise, vulnerability, and general support system remediation progress. However, Patch and Vulnerability group personnel stated that they do not consistently review and report enterprise-wide trending data. Instead, they focus on vulnerability prioritization and remediation for high-visibility programs.

Further, according to the Concept of Operations, the Patch and Vulnerability group is supposed to collect and track metrics including open and remediated vulnerabilities per severity category as well as the total POA&Ms and their status.[65] The group is also supposed to report these metrics to Cybersecurity function leadership for them to assess enterprise patch management. However, the Patch and Vulnerability group stated that system owners were responsible for using the dashboard to obtain their remediation statuses themselves and report any issues to the Cybersecurity function directly. By not actively monitoring vulnerability remediation efforts, the IRS is exposed to potential threats and vulnerabilities and is at risk of not being in compliance with Federal mandates and legislation.

The GAO initiated an audit to **review the status of the IRS's information technology investments**.[66] In its report, the GAO reported that the IRS stated that three investments (*i.e.*, Enterprise Case Management, CADE 2, and Web Applications [WebApps]) in development selected by the GAO for review were mostly within 10 percent of performance goals. For the selected investments in development, IRS reported cost, schedule, and scope performance information on a quarterly basis for Fiscal Years 2019 and 2020. According to the IRS, the three investments were within 10 percent of cost, schedule, and scope goals for these years (with the exception of CADE 2, which experienced a significant budget underrun in Fiscal Year 2020).

[65] Developed in 2018, Concept of Operations tasked the Patch and Vulnerability group with establishing a systematic and automated approach to patch and vulnerability management and creating remediation and mitigation policies, processes, and methodology.

[66] GAO, GAO-22-104387, *Information Technology: Cost and Schedule Performance of Selected IRS Investments* (Oct. 2021).

The IRS also reported that the selected investments in operations and maintenance met most OMB performance requirements. The IRS conducted operational analyses for the two investments, End User Systems and Services and the IMF, in operations and maintenance for Fiscal Years 2019 and 2020. The operational analyses for End User Systems and Services fully addressed all six OMB factors.[67] The operational analyses for the IMF fully addressed five of six factors and partially addressed the remaining factor. The operational analyses partially addressed the factor associated with greater use of technology or consolidation of investments to better meet organizational goals. The analyses stated that the IRS used new technology to implement processing improvements via a more robust testing approach in order to reduce coding defects.

However, while the analyses noted that the IMF is being replaced with a more modern system, the analyses did not reflect the IRS's modernization progress to date and the associated challenges – a shortcoming that the GAO identified in its review of the IRS's 2016 operational analysis for the IMF and reported on in June 2018.[68] The GAO stressed that this omission was concerning given the risk exposure created by the IRS's continued use of the legacy assembly language code. Consequently, the GAO recommended that the IRS ensure that the operational analysis for the IMF fully addresses greater use of technology or consolidation of investments to better meet organizational goals.

In addition, the GAO reported that the IRS's CADE 2 development has taken much longer and cost significantly more than originally planned. The IRS began developing CADE 2 in 2009 to replace the IMF. To limit risk and demonstrate incremental progress toward modernization, the IRS planned to deliver the investment in three phases, called transition states. The IRS initially reported preliminary estimated life cycle cost estimates for Transition State 1 and 2 of about $1.3 billion through 2024, including approximately $377 million for development and $922 million for operations and maintenance. The GAO also reported that the IRS completed all the work it had originally planned for Transition State 1 in July 2014, two years later than originally planned. Through this phase, the IRS modified the IMF processing cycle to allow for daily (rather than weekly) processing and posting of taxpayer returns. According to the IRS, this enabled faster refunds to taxpayers, among other things.

Further, the GAO reported that the IRS has taken much longer than originally planned to develop Transition State 2. The IRS now expects that it will complete development activities in April 2023, nine years later than originally planned. Due to significant budget cuts and a shortage of skilled staff, the transition state's release plan was revised three times between 2016 and 2017. In addition, in May 2019, the IRS's CIO stated that the agency recognized that the scope for CADE 2 was too broad and complex. As a result, the IRS decided to de-scope several of CADE 2's projects to focus solely on modernizing parts of the IMF, which accounts for a large portion of tax processing activities, rather than retire the IMF. As of July 2021, the IRS was

[67] The OMB's Fiscal Year 2020 Capital Programming guidance states that agencies should conduct an operational analysis for each investment in operations and maintenance that addresses six factors. These factors are 1) the extent to which the investment supports customer processes as designed; 2) how well the investment contributes to achieving the organization's strategic goals; 3) a comparison of current performance with a pre-established cost baseline; 4) alternative methods for achieving the same mission needs and strategic goals; 5) greater (*i.e.*, increased) utilization of technology or consolidation of investments to better meet organizational goals; and 6) annual performance of operational analyses.

[68] GAO, GAO-18-298, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing* (June 2018).

focused on re-engineering the core components of the IMF using a hybrid of Agile and Waterfall software development approaches. The IRS initiated planning efforts for the target state in the second quarter of Fiscal Year 2021. As of July 2021, the IRS estimated that it would complete it in 2030.

In addition, the IRS reported that it had spent $1.47 billion on the development for CADE 2 through September 2020, nearly four times the amount it had estimated it would spend to develop Transition States 1 and 2. Additionally, the IRS reported that it had spent approximately $72 million for operations and maintenance though September 2020. Overall, the IRS has revised or re-baselined its cost, schedule, and scope goals on numerous occasions, including seven times between 2016 and 2019.

The CADE 2 delays and the IRS's continued use of the IMF are troubling given that the IMF: 1) is one of the oldest systems in the Federal Government; 2) has software written in an archaic language that the IRS stated is no longer taught in school; and 3) is supported by a workforce with specialized skills that are increasingly harder to find. In addition, the IRS has reported that a more modern system would provide the foundation for real-time digital taxpayer interactions, agile responses to legislative changes, and rapid access to data for enhanced customer service, compliance, and fraud detection services.

Information technology service and helpdesk requests

An incident is an unplanned interruption to or a reduction in the quality of an information technology service. The incident management process is designed to restore service operations back to normal as quickly as possible while minimizing the impact on business operations and ensuring that the best possible levels of service quality and availability are maintained. The goal of incident management is to have a process that is predictable, stable, and consistently operating at target levels of performance. Incidents are assigned a priority level that is used to identify the relative importance of an incident based on impact and urgency. There are four priority levels for incident tickets.

- Priority 1 – A severe mission-critical work stoppage impacting multiple internal or external users, services to taxpayers, or safety or health. The target resolution time is four hours.
- Priority 2 – A potential work stoppage that could have a direct impact on services to taxpayers or if its scope is multiuser and there is no workaround. The target resolution time is eight hours.
- Priority 3 – A work stoppage for one user with no workaround. The target resolution time is two business days.
- Priority 4 – A noncritical incident that is not a work stoppage and there is a workaround. The target resolution time is four business days.

In Fiscal Year 2022, TIGTA performed an audit covering information technology service and helpdesk requests. We initiated an audit to **determine whether the IT organization is effectively and efficiently managing end-user computer incidents**.[69] We found that management of end-user incident tickets needs improvement. The UNS function provided,

[69] TIGTA, Report No. 2022-20-053, *The End-User Incident Management Process Can Be Improved* (Sept. 2022).

from the Knowledge Incident/Problem Service and Asset Management tool, a data extract of incident tickets that were closed during Fiscal Year 2021 as well as incident tickets that remained open and were being worked as of November 17, 2021. We used the *Assignment* field and identified 96,116 (94,549 closed and 1,567 open) incident tickets that were worked by the UNS function's Enterprise Service Desk or Deskside Operations.[70] We analyzed the closed and open incident ticket data and determined that incident tickets are being categorized without meaningful cause codes. The cause code on an incident ticket is intended to answer the question, "Why did the incident happen?" In addition, we analyzed closed incident tickets and identified that tickets reassigned to service providers were resulting in inefficiencies, and incident tickets were being closed without obtaining user concurrence.

Meaningful cause codes were not always selected

With 185 different cause codes, service desk operators and service providers select the appropriate cause code when they categorize an incident ticket. Our analysis of the closed and open incident tickets determined that specific cause codes are not being selected. Specifically, we identified 79,644 (83 percent) incident tickets that had a cause code of *Not Listed*, *No List Defined*, *Other*, *General Failure*, or a cause code was not selected. Figure 11 provides a summary of our analysis.

Figure 11: Distribution of Closed and Open Incident Ticket Cause Codes

Cause Codes	Number of Incident Tickets	Percentage of Incident Tickets[71]
Not Listed[72]	*61,158*	63.6 percent
No List Defined	*7,847*	8.2 percent
Other	*5,213*	5.4 percent
General Failure	*4,038*	4.2 percent
Configuration Error	*3,957*	4.1 percent
Monitor	*1,648*	1.7 percent
No Cause Code Selected[73]	*1,388*	1.4 percent
Remaining Cause Codes[74]	*10,867*	11.3 percent
Total	*96,116*	99.9 percent

Source: TIGTA's review of incident tickets closed during Fiscal Year 2021 and incident tickets that remained open as of November 17, 2021, from the Knowledge Incident/Problem Service and Asset Management tool.

[70] Telecommunication incident tickets were excluded from the review because they do not pertain to information technology services.

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

[72] *Not Listed* and *No List Defined* are cause codes that mean an appropriate cause code was not available. UNS function management stated that *Not Listed* and *No List Defined* have the same meaning.

[73] The IRS did not make a cause code tool available until November 2020. These incident tickets potentially include tickets closed prior to the availability of the cause code tool and open tickets still being worked.

[74] The remaining 179 cause codes each represents a small percentage of the total cause code population. They are collectively reported here to provide perspective and context.

Incident ticket reassignments were not always justified or appropriately reassigned

An incident ticket is reassigned when an incident cannot be resolved by a particular service provider or has been incorrectly assigned. An incident ticket with multiple reassignments is an indicator of potential workflow inefficiencies resulting from the improper assignment of the ticket. Figure 12 provides the number of closed and open incident tickets by frequency of reassignments.

Figure 12: Closed and Open Incident Tickets by Frequency of Reassignments

Number of Reassignments	Number of Incident Tickets
0 Reassignment	76,695
1 Reassignment	10,899
2 Reassignments	6,470
3 Reassignments	1,168
4 Reassignments	545
5 Reassignments	160
6 Reassignments	83
7 Reassignments	37
8 Reassignments	38
9 Reassignments	7
10 or more Reassignments	14
Total	96,116

Source: TIGTA's review of incident tickets closed during Fiscal Year 2021 and incident tickets that remained open as of November 17, 2021, from the Knowledge Incident/Problem Service and Asset Management tool.

To obtain a perspective of the reassignments and sufficiency of documentation, we selected and reviewed a judgmental sample of 35 closed incident tickets, each having four or more reassignments. We reviewed the actions documented in the *Activities* section of the incident tickets and determined that 28 of 35 incident tickets contained at least one reassignment that did not have a documented justification. The remaining seven incident tickets included justifications for the reassignments. Further analysis of the 35 closed incident tickets selected for review determined that the reassignments for approximately one-third of the tickets were inappropriate as they were reassigned multiple times to the same wrong assignment group or were reassigned without completing required tasks. For nearly another one-third of incident tickets, we were unable to make a determination whether the reassignments were appropriate because there was insufficient documentation. For the almost one-third of incident tickets remaining, the reassignments appeared appropriate.

User concurrence was not obtained

We reviewed a second judgmental sample of 30 closed incident tickets to determine whether service desk operators and service providers properly obtained user concurrence prior to closing the incident tickets. Of 30 closed incident tickets, 14 tickets included the user's concurrence that

the issue was resolved and that the ticket could be closed. Sixteen closed incident tickets did not contain the user's concurrence.

The effectiveness and efficiency of the incident ticket handling process is impacted when incident tickets are categorized with nonspecific cause codes, reassigned multiple times without sufficient justification, and closed without obtaining user concurrence. Inaccurate or incomplete data make it difficult for the IRS to identify trends in incident management and failure to obtain user concurrence may result in closing incident tickets prematurely or untimely.

In addition, we found that incident management performance goals are not being met. We reviewed 21 incident management metrics from the *UNS Balanced Scorecard* and the *UNS Operational Dashboard Report* that the UNS function uses to manage its incident management program. For Fiscal Year 2021, only five of 21 incident management metrics were met consistently for six months or more, including three metrics (*i.e.*, *Call Handle Time*, which measures the average time it takes a service desk operator to complete an inbound service call; *First Level Resolution*, which measures the percentage of interactions closed by the Enterprise Service Desk; and *UNS Percent on Time – Level 1: Priority 3*, which measures the timeliness of resolution for Priority 3 interactions and incidents worked by the Enterprise Service Desk) that were met every month in Fiscal Year 2021. Five metrics were met from two to five months. However, 11 incident management metrics (*e.g.*, *Customer Satisfaction*, which measures the monthly and fiscal year-to-date results of three survey questions for interactions, incidents, and requests worked by the UNS function and *Speed of Answer*, which measures the average amount of time a customer waits in the Service Desk queue before reaching a service desk operator) were not met once in Fiscal Year 2021. It is important to resolve incident tickets within established performance goals to minimize the level of disruption to the IRS and its ability to consistently process taxpayer returns and further tax administration. By failing to meet its established incident management performance goals, there may be an increased level of disruption to users.

We also found that two key industry metrics are not being captured. We compared key industry metrics to metrics captured and measured by the UNS function and found that the *Cost per Contact* and *Agent Utilization* metrics are not captured. *Cost per Contact* measures how efficiently the service desk is conducting its business by taking the annual operating expense and dividing it by the annual contact volume. *Agent Utilization* is the average time that an agent spends handling both inbound and outbound contacts per month divided by the total number of hours worked in a given month. This metric measures labor efficiency. It is important to have realistic performance goals and capture key industry metrics. Without them, the IRS cannot truly measure performance against program objectives, effectiveness, and efficiency.

Risk management

Risk management is the systematic process of identifying, analyzing, and responding to project risk. Risk management is an ongoing process that requires continuous risk identification, assessment, planning, monitoring, and response. Risk assessment is a component of risk management. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses. Management analyzes the identified risks to estimate their significance, which provides a basis for responding to the risks. Risk assessments identify threats, vulnerabilities, harm, and likelihood that harm will occur. The

end result is a determination of risk. Risk assessments can support a wide variety of risk-based decisions and activities.

During Fiscal Year 2022, TIGTA performed an audit covering risk management. In our audit of the **IT organization's planning and governance to modernize and secure systems**, we found that the ARPA program risk is monitored in the Item Tracking Reporting and Control system. The system is a customized tool that allows users to submit and update action items, issues, and risks to the database. According to IT organization senior management, many of the ARPA programs, and the IRS modernization plan more broadly, directly address IRS enterprise risks for Fiscal Years 2021 and 2022, which influenced IRS leadership in the overall decisions around portfolio priorities. We reviewed enterprise risks for the ARPA programs and determined there are multiple risks that the IRS is able to address because of the additional capabilities and functionality made possible by the ARPA funding.

We interviewed the IT organization's portfolio risk manager responsible for ARPA program risk at the Information Technology Modernization portfolio level to gain an understanding of risk management efforts. According to the portfolio risk manager, the portfolio risk management group prepares a consolidated Information Technology Modernization portfolio status report that includes risk information using the Item Tracking Reporting and Control system. The portfolio risk management group meets with the Associate CIOs monthly to discuss risk status, including risk mitigation efforts and any potential new risk included in the status report to ensure that the information is accurate. The portfolio status report is then used by the Associate CIOs to brief the CIO monthly.

We also met with IT organization senior risk management for two ARPA programs. According to the program risk managers, when a risk is initially identified, it is submitted into the Item Tracking Reporting and Control system. Once the risk is submitted, program risk personnel meet to discuss the risk and develop mitigation efforts, which are noted in the system. The program risk managers stated that program risk personnel meet with their respective Associate CIOs weekly or bi-weekly to discuss risk and risk mitigation efforts and any items that may impact cost, schedule, or program scope; briefing documents confirm that risk topics are discussed during these meetings.

In addition, we analyzed eight ARPA programs in the Item Tracking Reporting and Control system to determine whether risks are being monitored. Our analysis was based on risk detail reports as of December 21, 2021. These reports included mitigation status and activity, probable impact dates, projected completion dates, risk identification and submission dates, and risk escalation. Based on our testing criteria, we found that three of the eight programs had risks.[75] We obtained additional risk detail reports as of March 29, 2022, and noted that all risks from December 21, 2021, were addressed and closed. We determined that overall the risks were actively monitored, responded to, and addressed.

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,

[75] Three risk criticality color designations are combined to create the probability of the risk occurring and the risk impact. The "Red" risk criticality color designation is risk that requires attention the quickest. Our audit testing included risks with a "Red" criticality color.

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.

A corrective action is the action of identifying and eliminating the causes of a problem and preventing its recurrence. The Joint Audit Management Enterprise System is the Treasury Department's web-based management controls database tracking system. It is used to track issues, findings, and recommendations extracted from GAO and TIGTA audit reports. It is also used to track the status of planned corrective actions for material weaknesses, significant deficiencies, existing reportable conditions, remediation plans, and action plans.

In Fiscal Year 2022, TIGTA and the GAO performed four audits with coverage on the status of implementing corrective actions. In our **vulnerabilities on network devices** audit, we found that unremediated vulnerabilities lack corrective action plans. When remediation cannot be implemented, system owners are required to develop a POA&M for remediation or authorizing officials must document the accepted risk to the network through a risk-based decision. The IRS did not track the remediation with a documented POA&M or risk-based decision for 20 (69 percent) of 29 vulnerabilities reviewed. We also found that the IRS did not have POA&Ms or risk-based decisions in place for devices that were not receiving network vulnerability scans. Specifically, 71 (97 percent) of 73 devices on the May 2021 Vulnerability Scanning Exception List did not have a POA&M or risk-based decision in place for not meeting the vulnerability scanning requirements. Failure to resolve or track existing vulnerabilities compromises the security posture of the enterprise, potentially exposing taxpayer data and information to unnecessary risk.

Management Action: During our audit work, the IRS removed the 71 devices without POA&Ms from the scanning exception list. The devices were added back to the vulnerability scanning footprint as of July 2021.

In our **insider threat capabilities** audit, we found that implemented planned corrective actions generally addressed prior TIGTA recommendations. In the Fiscal Year 2020 report, TIGTA reported that the IRS had made substantial progress in implementing an insider threat capability but that additional improvements could assist the IRS in achieving an effective full operating capability.[76] Specifically, TIGTA recommended that:

- The IRS should ensure that the UBAC project implementation plan included actions to determine and assess the risk posture of high-value assets and that those risks should be addressed as part of the capability implementation.
- The CIO should ensure that status reports align with the National Insider Threat Task Force recommendations and include sections to address program improvement and major impediments or challenges.
- The CIO should ensure that the UBAC project implementation plan includes the National Insider Threat Task Force's recommended training for UBAC personnel. In addition, the

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

IRS should document all UBAC training efforts and, at least annually, ensure that all UBAC personnel have completed the required training.

We reviewed the recommendations, the actions taken by the IRS to addresses those recommendations, and the documentation to support those actions. Overall, we determined that the IRS met the intent of the recommendations and addressed the weaknesses identified. The IRS assessed the risk posture of the high-value assets, updated its status reports to include sections to address program improvements and major impediments or challenges, and ensured that all UBAC personnel completed the required training.

However, according to the Joint Audit Management Enterprise System report and the documentation provided, we determined that the IRS did not update the UBAC project implementation plan as recommended in the first and third recommendations. Instead, IRS officials updated a standard operating procedure with an appendix containing three numbered items addressing each of the three recommendations made in the prior report.[77]

In our **database vulnerability scanning and patching** audit, we found that the IRS completed a corrective action to address and close a recommendation from a prior TIGTA report.[78] We recommended that the IRS fully implement its database vulnerability scanning tool. The IRS implemented the database vulnerability scanning tool in March 2016. However, we also found that POA&Ms were not created for database vulnerabilities. We judgmentally sampled 10 FISMA systems from the IRS's database vulnerability scanning tool's report requiring POA&Ms on outdated software patches that need to be applied to the databases. Specifically, we found that the IRS created POA&Ms for only [redacted] FISMA systems we reviewed. For [redacted], the IRS provided various reasons for not creating POA&Ms, such as database administrator error or a vendor patch installation issue. The IRS did not explain why POA&Ms were not created for the remaining [redacted].

Overall, we concluded that the IRS lacked managerial oversight to ensure that it appropriately documented corrective actions. Without a sound remediation process, the IRS cannot ensure that it is correcting and managing its information security weaknesses. Without sufficiently documenting POA&Ms, the IRS may not effectively remediate information security deficiencies in a timely manner, thereby exposing its systems to increased risks that nefarious actors will exploit the deficiencies to gain unauthorized access to information resources.

In its audit of the **IRS's internal control over financial reporting**, the GAO reported that the IRS continued to address many of the control deficiencies and associated recommendations related to internal controls over financial reporting from its prior years' reports. As of September 30, 2020, the GAO reported 96 information systems recommendations and 14 safeguarding recommendations from prior years' reports as open in its May 2021 reports.[79] During its Fiscal Year 2021 audit, the GAO determined the following:

[77] Information Technology Cybersecurity Operations Standard Operating Procedures, *UBAC Anomaly Reporting* (SO-013-2020) (Jan. 2021).

[78] TIGTA, Report No. 2011-20-099, *The Mainframe Databases Reviewed Met Security Requirements; However, Automated Scans Were Not Being Performed* (Sept. 2011).

[79] GAO, GAO-21-401R, *Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls* (May 2021), and GAO-21-400RSU, *Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls* (May 2021).

- The IRS completed corrective actions to address and close 63 of 96 information system recommendations from prior years' reports. Closed corrective actions include: identification and authentication, authorization, boundary protection, audit and monitoring, sensitive system resources, and configuration management. As a result, the IRS needs to address 41 information system recommendations, including 33 from prior years' reports and eight new recommendations (*i.e.*, identification and authentication, boundary protection, and configuration management) made by the GAO.
- The IRS completed corrective actions to address five of 14 safeguarding recommendations from its prior years' reports. As a result, the IRS needs to address nine safeguarding recommendations.

Updating and modernizing operations

Successful modernization of systems and the development and implementation of new information technology applications are critical to meet the IRS's evolving business needs and enhance services provided to taxpayers. Modernization is necessary to deliver efficient taxpayer services and enforcement with enhanced user experiences.

In Fiscal Year 2022, TIGTA and the GAO performed seven audits covering modernization. We initiated an audit to **assess the processing of the Recovery Rebate Credit claims during the 2021 Filing Season, including ensuring that taxpayers are properly reconciling advanced economic impact payments received during Calendar Year 2020**.[80] The Coronavirus Aid, Relief, and Economic Security Act created a refundable tax credit, the Recovery Rebate Credit, of up to $1,200 per eligible adult to be applied toward the taxpayer's Tax Year 2020 tax liability. Eligible individuals can also receive up to $500 for each child in their family who is under 17 years old. In addition, the Consolidated Appropriations Act, 2021, created an additional Recovery Rebate Credit of up to $600 for each eligible individual and child. We found that the IRS correctly calculated the Recovery Rebate Credit amount for 26.1 (99 percent) of 26.3 million tax returns processed as of May 27, 2021, with a Recovery Rebate Credit claim. The 181,743 returns for which the IRS's calculation of the Recovery Rebate Credit amount was incorrect include:

- 117,314 returns for which the calculated Recovery Rebate Credits were $218.7 million more than the taxpayers were entitled to receive.
- 64,429 returns for which the calculated Recovery Rebate Credits were $80 million less than the taxpayers were entitled to receive.

In addition, our review of the 26.3 million Recovery Rebate Credit claims processed as of May 27, 2021, found that the IRS's Recovery Rebate Credit fraud filters were generally working as intended. However, a programming error prevented 7,478 tax returns with potentially erroneous Recovery Rebate Credits totaling $29.4 million from being identified for additional review before the credits were paid. IRS programming did not identify married filing joint returns for additional review when the spouse had a nonwork Social Security Number. To be eligible for the Recovery Rebate Credit, an individual must have a Social Security Number that is

[80] TIGTA, Report No. 2022-46-032, *Processing of Recovery Rebate Credit Claims During the 2021 Filing Season* (May 2022).

valid for work. In addition, the IRS's programmed Recovery Rebate Credit dollar tolerance prevented 348 tax returns with credits totaling $85,446 from additional review.

We also initiated an audit to **assess the IRS's implementation of the expanded Child and Dependent Care Credit eligibility requirements**.[81] The Child and Dependent Care Credit provides a tax credit for paid expenses for the care of a qualifying individual to enable the taxpayer, and their spouse if filing a joint return, to work or actively look for work. Provision 9631 of the ARPA temporarily makes the credit fully refundable for Tax Year 2021 for taxpayers whose main home is in the United States for more than half the tax year.[82] The Act also increases the amount of the credit for Tax Year 2021. These changes will make the credit one of the largest refundable tax credits administered by the IRS. Our prior and extensive reviews of the IRS's administration of refundable credits has identified that, although refundable credits help low-income individuals reduce their tax burden and provide incentives for specific activities, such as seeking or obtaining a job, unintended consequences are that they can result in the issuance of improper payments and can be the targets of unscrupulous individuals. As such, they pose a significant risk as an avenue for those seeking to defraud the Government. Not collecting or analyzing sufficient taxpayer information may lead to erroneous credits and improper payments.

Our review found that the IRS developed filters used to identify Child and Dependent Care Credit claim errors before e-filed tax returns posted to the Master File. For example:

- Modernized e-Filing Business Rules – For Tax Year 2019, there were 21 active Modernized e-Filing business rules that systemically check information specific to Form 2441, *Child and Dependent Care Expenses*, claims.
- Error Resolution System – The IRS uses its Error Resolution function to identify and address tax return errors. Codes are programmed into IRS systems to identify errors for paper and electronically filed returns with a Child and Dependent Care Credit claim.

In addition, recognizing the significant risk of potentially improper/fraudulent Child and Dependent Care Credit claims, we analyzed nearly 6.3 million Tax Year 2019 tax returns that received the credit to evaluate IRS processes to detect potentially fraudulent and erroneous claims. Our review identified a number of weaknesses in the controls over the processing of the credit. We issued 11 alerts to the IRS so it could address the processing deficiencies before taxpayers began filing claims for the refundable Child and Dependent Care Credit during Processing Year 2022. For example, we found 5,669 tax returns with erroneous claims, totaling more than $3.3 million, whereby the taxpayer incorrectly claimed qualified care expenses paid to the primary taxpayer, secondary taxpayer, or a dependent on the tax return. The e-file business rules only rejected tax returns when the care provider Taxpayer Identification Number matched the primary or secondary taxpayer's and not the dependent's Taxpayer Identification Number. The IRS agreed to add a business rule that will reject an e-filed tax return when the care provider matches a taxpayer's dependent Taxpayer Identification Number.

[81] TIGTA, Report No. 2022-47-023, *American Rescue Plan Act: Assessment of Processes to Identify and Address Improper Child and Dependent Care Credit Claims* (Mar. 2022).

[82] A refundable credit is not limited to the amount of an individual's tax liability and can result in a Federal tax refund that is larger than the amount of Federal income tax withholding for that year.

In addition, we initiated an audit to **assess the IRS's customer service efforts to assist taxpayers with the CTC Update Portal and nonportal update methods**.[83] The ARPA enhances the CTC for Tax Year 2021 by increasing the amount of the credit from $2,000 to $3,000 per child under the age of 18 ($3,600 per child under age 6) and making the credit fully refundable for taxpayers who meet the principle residence requirements. In addition, this legislation directed the IRS to establish a program to allow taxpayers to receive advance periodic payments during Calendar Year 2021 equal to 50 percent of the IRS's estimate of the credit allowed for Tax Year 2021. Taxpayers should have received the remaining half of the credit in Calendar Year 2022 when they filed their Tax Year 2021 tax return.

In preparation for issuing advance monthly CTC payments, we found that the IRS launched a series of comprehensive and far-reaching education and awareness campaigns. This was to ensure that taxpayers understood changes to the eligibility requirements as well as inform taxpayers of the CTC Non-filer Sign-up Tool and the CTC Update Portal to unenroll or update their information. For example, the IRS partnered with the Free File Alliance to develop the CTC Non-filer Sign-up Tool to help taxpayers who do not have a Federal tax return filing requirement to submit the needed tax return for eligibility for the advance CTC payments or economic impact payments. As of December 2021, the IRS accepted approximately 390,200 tax returns filed through the nonfiler tools (including the CTC Non-filer Sign-up Tool and the third-party filing tool).[84]

In addition, the IRS created processes to update tax accounts associated with taxpayers initiating specific actions on the CTC Update Portal, thereby ensuring that the IRS had the most current information needed to update the advance CTC payment amounts. Depending on the specific action initiated, the IRS developed separate codes that would post to the taxpayer's account to identify these updates. Our review of these codes identified several concerns that we brought to management's attention. For example, as of November 2021, we identified 1,895 taxpayer requests for a paper check that did not receive the appropriate update to prevent a direct deposit. IRS management stated that there was a known issue with taxpayers in a married filing jointly status for which one taxpayer does not have a tax account on which to post the paper check request. IRS management stated that, due to other priorities, programming updates were not implemented because the taxpayers still received an advance payment. The IRS is continuing to analyze these cases to ensure that all taxpayers identified are associated with this known issue. The IRS also created a new filter in the [redacted] to detect potentially fraudulent tax returns filed through the CTC Non-filer Sign-up Tool. Additionally, all tax returns filed through the CTC Non-filer Sign-up Tool, including the third-party tool, were run through the identity theft filters. As of December 2021, the IRS selected 133,057 nonfiler tax returns as potential identity theft, of which 1,349 tax returns were confirmed identity theft.

Further, we found that programming to identify discrepancies resulting from the reconciliation of Advance CTC payments is being developed. The ARPA also required the taxpayer to reduce their CTC by the amount of advance payments received when filing their Tax Year 2021 tax return. In response to this provision, the IRS updated Schedule 8812, *Credits for Qualifying*

[83] TIGTA, Report No. 2022-47-042, *American Rescue Plan Act: Assessment of the Child Tax Credit Update Portal's Capabilities and Related Processes* (July 2022).

[84] On September 1, 2021, a third-party entity, in collaboration with the White House and the Treasury Department, developed a similar nonfiler tool to allow taxpayers another tool to gain eligibility for advance payments through November 15, 2021.

Children and Other Dependents, and the instructions to assist taxpayers with this required reconciliation. Schedule 8812 assists taxpayers with reducing their CTC by the amount of advance payments, thus reconciling their advance payments. Taxpayers will receive Letter 6419, *2021 Total Advance Child Tax Credit Payments*, that reports to the taxpayer the aggregate amount of advance payments received during Calendar Year 2021 and the number of qualifying children used to determine the amount of advance payment.

In our audit of the **IT organization's planning and governance to modernize and secure systems**, we found that the IT organization's effective program selection process may contribute to the timely use of the ARPA funds. The IRS's IT organization was allocated $1 billion for modernization efforts. According to the IRS, the Business Systems Modernization portfolio and the new ARPA-funded initiatives will form the evolving Information Technology Modernization portfolio to drive technology transformation and enhance the taxpayer experience.[85] It will accomplish this by accelerating existing initiatives and introducing new initiatives based on emerging needs and technologies. The Information Technology Modernization portfolio consists of 21 different IT organization programs with scheduled deliverables and capabilities. Of 21 programs, 19 received ARPA funding (*e.g.*, Live Assistance and Taxpayer Accessibility), which enabled the expansion of six programs and the initiation of additional capabilities for 13 programs. As of April 2022, approximately $260 million (or 26 percent) of ARPA modernization funds have been obligated, expended, or disbursed.

We interviewed IT organization leadership and reviewed briefing documents to determine how the IT organization selected the programs to be included in the expanded Information Technology Modernization portfolio enabled by the ARPA funding. IT organization leadership collaborated with other IRS leadership to align and gain approval of the ARPA program selection, including the IRS Commissioner's approval of selections. IT organization leadership also briefed OMB and Treasury Department leadership on proposed funding allocation, planning, and execution time frames, along with other key factors.

The documents reviewed revealed what was entailed in forming the ARPA portfolio, including progress made on selecting the programs, an initial set of initiatives, and proposed ARPA program descriptions. The documents also showed the IT organization leadership's input on the scope and outcomes for programs with large taxpayer and employee impacts, goals, and next steps. The ARPA program selection discussions were held from March through May 2021. Our review did not evaluate whether the IT organization will use the ARPA funds timely and effectively; however, active engagement of stakeholders and senior leadership support are critical factors to the success of information technology investments.[86] In addition, IT organization leadership stated that stakeholders (*i.e.*, IRS, OMB, and Treasury Department leadership) are still supportive of the ARPA program. This, in part, may signify a well-planned program and contributes to the timely and effective use of the ARPA funds.

In addition, we discussed with IT organization senior management some of the challenges and areas of concern regarding the ARPA funding. According to the IRS, the IT organization needs consistent and predictable funding to last over a longer period of time to meet its long-term

[85] One of the IT organization's primary appropriations with funds provided to help modernize eight IT organization programs, including Web Applications, CADE 2 Transition State 2, Enterprise Case Management Acceleration, and Security Operations and Management.

[86] GAO, GAO-12-7, *Critical Factors Underlying Successful Major Acquisitions* (Oct. 2011).

modernization initiatives, but the ARPA funds cannot be used after Fiscal Year 2023. This short deadline could impact the IT organization's ability to effectively use all the funding. Although the ARPA funding could result in significant progress for modernization, the IRS's Omnibus report for the second quarter of Fiscal Year 2022 stated that the funds were realigned and will require replanning of multiple modernization programs during the third quarter of Fiscal Year 2022. This could significantly reduce the amount of ARPA funding available to the IT organization. IT organization leadership confirmed that approximately $400 million of the $1 billion in ARPA funds previously aligned to modernization efforts will be reallocated to assist with the taxpayer service backlog and to address a significant deficit within the operations support appropriation. They also stated that a redirection of ARPA funds means that the scope of the programs in the Information Technology Modernization portfolio will be replanned based on available funding, with many programs coming to a stop. Many modernization capabilities will remain incomplete if the IRS does not receive additional funding in the future. The IT organization has begun assessing for replanning, pending any final decisions on the IT organization's overall budget.

In our audit of **cloud computing services**, we reported that Governmentwide mandates required Federal agencies to expand the use of shared services to enable broader use and adoption of cloud computing.[87] In addition, these mandates direct the Federal Government to accelerate movement to secure cloud services. As part of its modernization efforts and to align with the Federal mandates, the IRS is engaged in a significant migration of services to the cloud. One of the goals of this migration is to maintain application efficiency and overall service agility. The IRS plans to accomplish this by transitioning data, applications, and services from an on-site presence to the cloud environment.

While cloud deployments can bring many operational benefits to an organization, security control weaknesses over cloud computing services can pose a substantial risk to the data residing on these services. For IRS cloud deployments, these data include taxpayer data. The potential harm includes breach and unauthorized access to and disclosure of taxpayer data. To facilitate and guide its cloud security implementation efforts, the IRS developed its Cloud Security Reference Architecture in September 2019 and Cybersecurity Cloud Operations Framework in November 2019. The IRS also issued its updated Cloud Strategy and a cloud security specific IRM 10.8.24 in March 2021 and September 2021, respectively. In addition to establishing numerous security controls, the IRS indicated that it performed a number of security-related activities as of June 2021. For example,

- The Cybersecurity function established the Cloud Security Assessment and Authorization program in July 2019. The Security Risk Management team has performed a variety of initial, event-driven, and annual security assessments for cloud projects.
- The Cybersecurity function identified tools within the Cybersecurity Inventory of Tools and Technologies that support the IRS's migration to the cloud and outlined the variety of service and deployment models and the capability areas that these tools support. It

[87] Governmentwide mandates include the Federal Cloud Computing Strategy (*"Cloud First" and "Cloud Smart"*) (Feb. 2011 and June 2019, respectively); OMB Memoranda M-16-19, *Data Center Optimization Initiative* (Aug. 2016), and M-19-19, *Update to Data Center Optimization Initiative* (June 2019); and Executive Orders 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017), and14028, *Improving the Nation's Cybersecurity* (May 2021).

also identified and prioritized approximately 60 tools for cloud migration based on tool complexity and business benefit analysis.

- The IRS continued to perform analysis for implementing and adopting capabilities to manage encryption keys and protect data in transit and at rest across the IRS's future hybrid multicloud information technology environment. The Cyber Cloud team drafted a Key Management System whitepaper to detail the approach for the management and storage of encryption keys across the enterprise for cloud-based services, which included an analysis of scenarios whereby the IRS is and is not the originator of the master keys.

In our audit of the **NGI program**, we found that some NGI capabilities were implemented. In February 2020, the IRS redefined the NGI program from the *IRS Integrated Modernization Business Plan* as an overarching, collaborative effort to explore, select, and implement relevant modern technologies to attain the Future State Computing Infrastructure. The Future State Computing Infrastructure envisions the use of technology to provide a more proactive and interactive relationship between taxpayers and IRS employees that will improve taxpayer service, enforcement, and operations. The IRS modified the NGI program's capabilities to reflect the new definition and redefined the capabilities with new milestones to achieve the goals of the new NGI definition. The IRS adjusted priorities and eliminated certain capabilities. Some of the adjustments to the NGI program included:

- In April 2020, the IRS removed the automated desktop performance assurance and automated network provisioning (software-defined networks) capabilities from the modernization business plan because they did not fit the new definition. According to the Fiscal Year 2019 Key Insights report, automating desktop performance assurance will provide insights into the computing performance of desktops and workstations and more quickly resolve issues that might otherwise disrupt taxpayer service operations. The Key Insights report also provided that, by automating the provisioning of software-defined networks, the IRS can further modernize its technology operations.
- The IRS aligned both Enterprise Online Storage and the Tapeless Backup Solution requirements to the Managed Infrastructure and Data Services Acquisition.

Figure 13 shows the NGI capabilities in the *IRS Integrated Modernization Business Plan* that were implemented in Calendar Years 2019 and 2020.

Figure 13: Implemented NGI Capabilities

Capability	Implementation Date
Centralized code repository: onboard initial 10 projects	May 2019
Centralized code repository: onboard additional 15 projects	July 2020
Continuous integration/continuous delivery pipeline: onboard initial 40 projects	May 2019
Continuous integration/continuous delivery pipeline: onboard additional projects	July 2020
Converting legacy code and reducing the application footprint: strategy on legacy code conversion	December 2019
Develop containerization solution architecture	May 2019
Standard stack: develop and validate 3 to 5 stack solutions	September 2019
Standard stack: deploy 3 to 5 standard stacks via automation	November 2019
Standard stack: develop and deploy additional standard stacks	April 2020

Source: TIGTA's analysis of the IRS Integrated Modernization Business Plan and project documentation for NGI capabilities.

In December 2020, Strategy and Planning function management instructed the NGI program to stop all work and take steps to perform an orderly shutdown. The programs were directed to assess the status of their in-progress capabilities to conduct an orderly shutdown or request additional resources to deliver a capability already significantly underway. The IRS deemed the containerization program important to continue on its own regardless of the existing shutdown of other NGI capabilities. As of August 2021, NGI program funding had not been restored.

In its audit of the **IRS's information technology investments**, the GAO reported that the IRS stated that it is completing most of its 2019 *IRS Integrated Business Modernization Plan* activities within schedule and cost estimates. The IRS reported that, by the end of Fiscal Year 2020, it had completed most of the updated list of 59 *IRS Integrated Business Modernization Plan* activities associated with its revised plans for Fiscal Years 2019 and 2020 early or on schedule and within cost. Specifically, the IRS reported that it had completed 54 (*e.g.*, expanded toll-free capacity, deployed cyber architecture, and cyber cloud strategy) of 59 activities early or on schedule. The IRS also reported that it completed the remaining five activities (*e.g.*, procure an Enterprise Case Management solution, and procure and deliver cloud computing services required to deploy the Enterprise Case Management solution) three to seven months later than initially planned.

The GAO also reported that the IRS stated it took several information technology-related actions to maximize telework capabilities for its employees and continue to operate during the COVID-19 pandemic. These actions included procuring information technology equipment to continue to support agency operations and upgrading its infrastructure bandwidth. According to IT organization officials, the actions taken were not funded from the IRS's information technology budget for Fiscal Year 2020; however, the actions contributed to delays in the agency's plans for information technology modernization and operations. Specifically, between May and July 2020, the CIO established a mechanism for the Deputy and Associate CIOs to report impacts on ongoing and planned work due to the COVID-19 pandemic on a weekly

basis.[88] The weekly reports identified issues, such as delays and risks to programs and initiatives, and their effects on information technology programs and initiatives for the Fiscal Year 2021 filing season and nonfiling season activities. Among the issues identified in the reports were a delayed infrastructure refresh due to hardware supply chain back orders and delays of procurement activities because staff were reassigned to accelerate the move to maximum telework.

COVID-19 response

COVID-19 is a virus that causes respiratory illness in people and can spread from person-to-person. In January 2020, the first case of the COVID-19 in the United States was confirmed. In March 2020, the President officially declared a national emergency due to the outbreak of the COVID-19. The pandemic caused by COVID-19 impacted how we live and work across the country and around the world.

In Fiscal Year 2022, TIGTA performed two audits covering the IRS's response to the COVID-19 pandemic. We initiated an audit to **determine whether the IRS effectively used its telework program to reduce the impact of the COVID-19 pandemic on IRS operations**.[89] Telework is a work flexibility arrangement under which employees perform their duties and responsibilities from an approved worksite other than the location from which employees would otherwise work. A robust telework program and ensuring that as many employees as possible are prepared to telework are critical components of a plan to allow employees to work effectively from alternative sites and continue tax administration and mission-critical operations. Telework is a critical component of the IRS's Continuity of Operations Plan because telework allows the IRS to continue fulfilling its mission through emergencies that would result in a change of operating status, such as a pandemic.

The COVID-19 pandemic began to have a significant impact on IRS operations in March 2020. Between March 14 and March 28, 2020, the number of employees who reported any time worked at IRS facilities decreased from approximately 71,000 to 19,000 employees (a 73 percent decrease). The IRS issued an evacuation order and closed all of its facilities effective March 30, 2020. The number of employees reporting to IRS facilities continued to decline until April 27, 2020, when the IRS began recalling employees back to work at IRS facilities on a voluntary basis. In June 2020, the IRS began reopening facilities to employees, and by July 2020, the IRS reported that the majority of its facilities had reopened to those employees with nonportable work or mission-critical functions. The IRS offset the initial impact of office closures by allowing as many employees as were equipped and ready to telework to do so. However, the IRS had to place nearly 35,000 employees on Weather and Safety Leave with evacuation pay by the end of March 2020 because employees were unable to work from the office or telework.

We found that the IRS effectively leveraged its telework program to continue operations during the pandemic. At the beginning of Fiscal Year 2020 and prior to the pandemic, 50 percent of the IRS workforce (approximately 39,000 of 78,000 employees) were identified as telework

[88] The documented weekly impact reports were discontinued after July 2020, though Associate CIOs and Deputies were instructed to report issues in their meetings with the CIO.

[89] TIGTA, Report No. 2022-IE-R003, *The IRS Leveraged Its Telework Program to Continue Operations During the COVID-19 Pandemic* (May 2022).

eligible.[90] Between October 2019 and early March 2020, an average of 26,000 employees (about one-third of the IRS workforce and two-thirds of telework-eligible employees) teleworked at least once per week. Between March 14 and March 28, 2020, the number of employees who reported any time to telework increased from approximately 27,500 to 41,000 employees (a 49 percent increase). The IRS continuously increased the number of teleworkers through January 2021, when the number of employees recording time to telework peaked at 65,000. However, the number of employees recording any time to telework began to slightly decline after January 30, 2021, when more employees returned to their regular duties within IRS facilities. By the first week in July 2021 (the end of our assessment period), the number of employees recording any time to telework declined to 61,000.

Our review also determined that IRS employees were not required to complete telework training prior to teleworking under the evacuation order. IRS management stated that the IRS does not require evacuated employees who are teleworking to complete telework training. Evacuated teleworkers are instead encouraged to complete the training. During the week ending March 12, 2022, approximately 64,600 IRS employees have charged time to telework. According to IRS records, during this same period, nearly 3,200 evacuated employees (5 percent of teleworking employees) charged time to telework without having a telework agreement and had not taken telework training. IRS management stated that they continue to strongly encourage employees and managers to take telework training to become more familiar with program requirements and that this approach has been and continues to be the IRS's posture during the evacuation period.

Management Action: On March 23, 2022, the IRS announced its return-to-office plan, which requires all IRS employees to return to the office by May 8, 2022, if they do not have an approved telework agreement. Therefore, all employees who telework after May 8, 2022, should have an approved telework agreement and have completed telework training.

In addition, we found that employee telework participation increased as the IRS distributed laptops. Prior to the evacuation order in March 2020, the IRS issued approximately 1,000 laptops. Between March 2020 and January 2021, the IRS issued nearly 19,300 laptops to IRS employees through a set of IRS information technology initiatives designed to make previously non-telework-ready employees ready to work remotely and to convert employees from desktops or shared workstations to individually assigned laptops. Each IRS business unit was responsible for identifying those employees who had portable work and required a laptop to telework and for determining the priority or order in which employees should receive the laptops and other information technology equipment.

Although the IRS issued over 19,000 laptops to expand its employees' ability to telework while evacuated, other information technology-related concerns impacted teleworking employees. For example, TIGTA's Office of Audit performed a series of site visits at four tax processing centers, and managers in those centers noted several information technology-related concerns impacting teleworking employees including delays at the helpdesk, issues logging in through the virtual private network, issues with equipment, and issues with the SharePoint sites not working.

[90] Telework-eligible employees are those employees who are authorized to apply for telework.

The IRS confirmed that it experienced several information technology-related challenges during the pandemic that correlated to the concerns identified previously. IRS management stated that some of the challenges included:

- Information Technology Staffing – The service desk was understaffed, and in November 2020, the call volume rose from 1,200 calls to over 6,000 calls (a 400 percent increase in call volume) over a period of two to three weeks.
- Network and Software Issue – Employees had issues connecting to the IRS network using remote access and virtual private network software.
- Employees New to Telework – Employees were required to telework even if they had not teleworked previously and were unaware of how to use the software to connect to the IRS network. Information technology staff were required to support many of these employees virtually or over the telephone.

We identified several IRS time and attendance codes used to capture downtime related to information technology issues. Total information technology downtime consists of downtime charged by employees due to:

- System Downtime – idle time when enterprise-wide systems/applications are down, preventing the accomplishment of work in the enterprise.
- Computer Downtime – idle time when an employee's individual computer is unavailable due to computer-related issues preventing the accomplishment of work.
- Information Technology Helpdesk Downtime - idle time when waiting for information technology helpdesk assistance, including idle time while information technology staff are resolving the issue.

Between late January and April 2020, total information technology downtime hours were generally below 10,000 hours per week. However, between May 2020 and early January 2021, total information technology downtime increased significantly, ranging from 13,000 to as high as 74,000 hours per week. Since early January through June 2021, total information technology downtime hours trended downward, ending below 14,500 hours for the week ending July 3, 2021.

We also initiated a **review of cybersecurity related to IRS telework during the COVID-19 pandemic**.[91] In June 2021, the U.S. House of Representatives Committee on Oversight and Reform requested that an assessment of any vulnerabilities created or exacerbated by the Treasury Department's use of remote access software to facilitate telework during the COVID-19 pandemic, and whether any such vulnerabilities were effectively mitigated, be included with the annual FISMA reporting. Due to the scope of the work requested, we performed an audit separate from our FISMA audit work to address the Committee's concerns.[92] Our review reported on the acquisition, deployment, and management of remote access tools.

[91] TIGTA, Report No. 2022-20-007, *Cybersecurity and Telework During the COVID-19 Pandemic* (Dec. 2021).

[92] TIGTA, Report No. 2021-20-072, *Fiscal Year 2021 IRS Federal Information Security Modernization Act Evaluation* (Sept. 2021).

Remote connections

The IRS stated that it did not acquire new remote connections software to support telework during the COVID-19 pandemic and instead only purchased additional licenses. The Enterprise Remote Access project, operational since 2004, is the IRS's virtual private network solution for remote network access. It provides IRS employees the ability to securely connect to the IRS network while working remotely. The application uses security protocols to establish a secure remote connection to one of three IRS Treasury Internet Connection sites. The user account is authenticated before access to the network is granted. The Enterprise Remote Access project provides a virtual private network-based remote access solution that meets the remote access requirements of all IRS employees and approved contractors. The IRS reported that it completed upgrades to double the bandwidth capacity to support 60,000 employees working remotely by the end of Fiscal Year 2020.[93]

In September 2021, the GAO issued a report from which we concluded that the IRS:[94]

- Used a virtual private network and had established methods for employees to log in to agency systems and services remotely.
- Documented elements of a telework security policy, all relevant security controls and enhancements, and that it had assessed all of the relevant security controls and enhancements for protecting its systems that provide remote access.
- Demonstrated that it consistently monitored progress toward completing remedial actions for any identified weaknesses.

Collaboration platforms

The IRS stated that it uses or has plans to start using five collaboration platforms to connect internal and external stakeholders virtually. The use of such applications allowed the IRS to minimize the impact of the COVID-19 pandemic; however, it also increased the potential for data breaches and unauthorized disclosure. For example,

- The IRS stated in the Fiscal Year 2020 Information Technology Annual Key Insights Report that it deployed Collaboration Platform 1 to resume national settlement days virtually. The IRS stated that the Collaboration Platform 1 can support 800 users per server license and that it has 1,495 Martinsburg and 640 Memphis server licenses.
- In September 2020, the IRS stated that it purchased 1,100 Collaboration Platform 2 licenses, and it deployed them to all IRS workstations. The UNS function's Collaboration Platform 2 team manages the administration of the application, including user roles. The application is implemented using single sign-on, which is by default a multifactor authentication mechanism. In the Fiscal Year 2020 Information Technology Annual Key Insights Report, the IRS also reported that it delivered the Collaboration Platform 2 to enable IRS Office of Chief Counsel to participate in virtual court sessions. The IRS stated

[93] IRS, Publication No. 5453, *Information Technology Annual Key Insights Report: Fiscal Year 2020 Successes and Accomplishments* (2021).

[94] GAO, GAO-21-583, *Selected Agencies Overcame Technology Challenges to Support Telework but Need to Fully Assess Security Controls* (Sept. 2021). The GAO identified the audited agencies that were not meeting the listed standards, indicating that the agencies not specifically identified had met the standard.

that for the Collaboration Platform 2, it has 1,050 licenses, which can each host 500 users, and 50 large meeting licenses, which can each host 1,000 users.

- The IRS is working to complete its testing of Collaboration Platform 3. It is beginning the implementation of Collaboration Platform 3 with a small group of pilot users in the production environment. The Cybersecurity function and the Privacy, Governmental Liaison and Disclosure organization are partners in the implementation of the Collaboration Platform 3 and working to create a secure, protected environment. The Collaboration Platform 3 product was included in a subscription plan and purchased in 2019. The Strategy and Planning function holds the licensing agreement. The IRS stated that its Applications Development function reviewed a messaging application for businesses, but that the IRS did not acquire it.

Security of collaboration platforms

The IRS stated that, for meetings supported by both Collaboration Platform 1 and Collaboration Platform 2, participants can only attend by a direct invitation from the IRS host. In addition, file sharing is disabled for both platforms. The IRS had existing guidance in the IRM to prevent the unauthorized dissemination of controlled unclassified information, Personally Identifiable Information, and sensitive but unclassified information. The policies state that all collaborative technology must be approved by the appropriate authorizing official following an assessment of risk with mitigation. It also states that e-mail messages, appointments, and other collaborative mechanisms containing confidential data must be encrypted when transmitted and stored.

Access management

The IRS stated that it used two-factor authentication since 2005. The IRS uses smart cards with a personal identification number for access. Prior to the COVID-19 pandemic, the IRM required two-factor authentication for all remote access to an IRS system and that systems must monitor and control remote access methods. Personal identity verification cards are used to authenticate users on a virtual private network. The IRS stated that, in the event of a card failure, the user is granted temporary access to a secure site to obtain a grid card. To accommodate potential card failures, the IRS purchased 40,000 additional grid card licenses. Procedures are in place to remove inactive accounts and for emergency removal of accounts when a user is no longer authorized to have one. From March 15, 2020, through October 27, 2021, 350 unauthorized user accounts and more than 16,000 inactive user accounts were removed from IRS system access.

We also reported on distribution and management of virtual and physical assets. The IRS stated that, in September 2020, the Information Technology Asset Management program implemented a scalable data integration and analytics platform, which improved the accuracy of compliance and other internal inventory reporting needs. In addition, the Information Technology Asset Management program operationalized a data remediation process and tool to improve overall asset data quality. In Calendar Year 2021, the Information Technology Asset Management program matured these capabilities by integrating additional configuration and asset inventory data of assets, such as laptops, and personal digital assistants.

The IRS reported in the Fiscal Year 2020 Information Technology Annual Key Insights Report that, through the *Depot to Home* initiative, laptops were shipped directly to more than 2,000 employees. The IRS stated that it accounted for all laptop shipments and no

shipments resulted in permanent loss. In our March 2021 interim report,[95] we stated that, by May 2020, the IRS distributed more than 12,600 laptops and nearly an additional 6,000 laptops by October 2020. No details were provided on smartphones or other information technology-related equipment. Our report also indicated that growth of telework during this period was limited by the IRS's ability to identify, prioritize, and issue laptops and other information technology equipment to employees who previously had not participated in the telework program.

The IRS stated that, in July 2020, it received approximately $1.6 million to procure desktop and portable printers and monitors. In September and October 2020, the IRS issued product awards for nearly 5,000 printers and more than 1,700 monitors. The equipment began arriving in February 2021. By August 31, 2021, all of the printers were delivered, while all but three monitors were delivered by October 31, 2021. The IRS also reported that, in December 2020, it received nearly $2 million of additional funding for desktop and portable printers. In April 2021, the IRS issued the second product award and items began arriving at the end of that month. As of October 15, 2021, 5,543 (57 percent) of 9,780 printers ordered were received and 4,237 printers are awaiting delivery from the vendor.

In May 2021, we issued another interim report that identified a spend plan in May 2020 allocating $35 million to Continuity of Operations for costs associated with purchasing laptops, wireless devices, and software licenses in support of employees teleworking.[96] A September 2020 amendment to the spend plan separated Continuity of Operations into $22 million funded by the Coronavirus Aid, Relief, and Economic Security Act and $15 million funded by the Families First Coronavirus Response Act. The September 2020 quarterly report on actual expenditures reported that more than half of the total funds had been spent but did not provide details on expenditures in each area.

Security policy changes for telework

The IRS stated that information technology security policy is set at an organizational and system level and that there were no updates to the security policies specific to the COVID-19 pandemic. However, a June 2021 memorandum provided guidance on several items, including the connection of personally owned and non-Government–furnished equipment to IRS systems and network. The IRS also issued several operational updates regarding telework, which included:

- Teleworking from a vehicle with a wireless Internet connection – The IRS stated that vehicles generally do not provide reasonable security and protection of Government equipment and data. If an employee is working with taxpayer data in their vehicle, there is a risk that bystanders could see through the vehicle's windows, which could allow for inadvertent disclosure of Personally Identifiable Information.
- Disposal and destruction of waste material containing Personally Identifiable Information or sensitive but unclassified data – The operational requirements stated that under no circumstance can employees burn paper with Personally Identifiable Information or sensitive but unclassified data and information at their telework locations. In addition, employees under no circumstance are permitted to use non-Government equipment

[95] TIGTA, Report No. 2021-IE-R002, *Interim Report – The IRS Leveraged Its Telework Program to Continue Operations During the COVID-19 Pandemic* (Mar. 2021).

[96] TIGTA, Report No. 2021-16-026, *Interim Report – Status of Coronavirus Response Funding* (May 2021).

(such as shredders) to process IRS data. Further, the IRS requires employees while teleworking to bring paper with sensitive but unclassified data into the office for proper disposal and to protect the data during transport to the office for proper disposal.

The Privacy, Governmental Liaison and Disclosure organization published a Privacy and Records Telework Policy checklist. This included the requirements to follow a Clean Desk Policy while on telework, use IRS e-mail accounts to conduct official IRS business, and immediately report any breach of sensitive information or record loss.

Our March 2021 interim report stated that the IRS waived the requirement for employees to have an approved telework agreement and encouraged, but did not require, new teleworkers to complete the telework training program. The Human Capital Office stated that the IRS waived several other telework policies. On September 30, 2021, the IRS extended the waiver of telework policies through March 23, 2022. The IRS stated that it plans to reassess the situation periodically and may lift the waiver earlier. It would provide employees with at least 30 days advance notice before requiring them to return to the office.

Continuous monitoring

The IRS stated that it has continuous monitoring and network scanning in place to identify vulnerabilities and that these processes were not impacted by the IRS's transition to telework. The IRS performs vulnerability scanning six days a week, and the scan results are ingested into an analytics and reporting tool, providing stakeholders continuous visibility into vulnerability data about their assets. The IRS has various network management programs, including configuration compliance scanning, audit log management, incident monitoring, and malicious code detection. In its September 2021 report, the GAO concluded that the IRS has assessed all of the relevant security controls and enhancements for protecting its systems that provide remote access. The IRS also demonstrated that it consistently monitored progress toward completing remedial actions for any identified weaknesses.

In September 2021, we reported that the IRS purchased and deployed an Endpoint Detection and Response solution, which analyzes various items such as processes running on workstations, memory artifacts, and other data points.[97] As of September 21, 2021, 86,593 (98 percent) of 88,595 eligible workstations had a successful deployment of the Endpoint Detection and Response solution. The collected data are correlated and compared to rules that have been established or associated with known indicators of compromise. If anything is detected, an alert is generated. We found that the alerts generated were properly tracked and worked. No alerts in the sample period were elevated to an incident.

Network protection

The IRS fully implemented the Common Communication Gateway, which was approved by the Department of Homeland Security to be a Trusted Internet Connection up to Version 2.0. According to the IRS, there are no identified and approved use cases for Trusted Internet Connection, Version 3.0. Until the Version 3.0 standard is finalized and the IRS receives direction from the Treasury Department, the IRS will continue with the traditional use case and the Version 2.0 implementation.

[97] TIGTA, Report No. 2021-20-065, *The Endpoint Detection and Response Solution Has Been Deployed to Most Workstations and Is Operating As Intended, but Improvements Are Needed* (Sept. 2021).

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the adequacy and security of the IRS's information technology. 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 business unit's Systems Security, Systems Development, and Systems Operations Directorates' audit reports issued during Fiscal Year 2022. 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 information technology security, systems development, and operations issues and determined which ones are at high risk for failing to deliver IRS program objectives and protect tax administration data.

Performance of This Review

The compilation of the information for this report was performed at various TIGTA offices during the period of May through December 2022. The information presented was derived from TIGTA and GAO reports issued during Fiscal Year 2022 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); Louis Lee, Director; Catherine Sykes, Audit Manager; David Allen, Lead Auditor; Cindy Harris, Senior Auditor; and Carreen Diaz, 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 2022. 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 Number	Audit Report Title	Report Issuance Date
1	GAO-22-104387	Information Technology: Cost and Schedule Performance of Selected IRS Investments	October 19, 2021
2	2022-20-001	Some Next Generation Information Technology Infrastructure Capabilities Were Implemented, but Program Management Improvements Are Needed	November 29, 2021
3	2022-20-007	Cybersecurity and Telework During the COVID-19 Pandemic	December 17, 2021
4	2022-20-006	Vulnerability Scanning and Remediation Processes Need Improvement	December 21, 2021
5	2022-20-009	More Interim Steps Could Be Taken to Mitigate Information Technology Supply Chain Risks	February 2, 2022
6	2022-20-010	Network Segmentation Reduced Unnecessary Access to Individual Master File Resources; However, Governance and Development Processes Were Not Always Followed	February 2, 2022
7	2022-47-023	American Rescue Plan Act: Assessment of Processes to Identify and Address Improper Child and Dependent Care Credit Claims	March 14, 2022
8	2022-25-029	The Individual Tax Processing Engine Project's Estimation Methodology Aligns with Best Practices and the Project Addressed the Independent Verification and Validation Recommendations	March 30, 2022
9	2022-27-028	The Child Tax Credit Update Portal Was Successfully Deployed, but Security and Process Improvements Are Needed	May 18, 2022
10	2022-46-032	Processing of Recovery Rebate Credit Claims During the 2021 Filing Season	May 19, 2022
11	2022-IE-R003	The IRS Leveraged Its Telework Program to Continue Operations During the COVID-19 Pandemic	May 23, 2022
12	GAO-22-105559	Management Report: IRS Needs to Improve Financial Reporting and Information System Controls	May 25, 2022
13	2022-20-040	Fiscal Year 2022 IRS Federal Information Security Modernization Act Evaluation	July 18, 2022
14	2022-47-042	American Rescue Plan Act: Assessment of the Child Tax Credit Update Portal's Capabilities and Related Processes	July 25, 2022

No.	Report Number	Audit Report Title	Report Issuance Date
15	2022-27-045	The IRS Effectively Planned to Use and Provide Oversight of the American Rescue Plan Act Funds; However, Subsequent Reallocation of Modernization Funds Resulted in Significant Replanning	September 2, 2022
16	2022-20-051	Taxpayer Digital Communications Platform Security and Access Controls Need to Be Strengthened	September 21, 2022
17	2022-20-055	Improvements Are Needed for an Effective User Behavior Analytics Capability	September 21, 2022
18	2022-20-053	The End-User Incident Management Process Can Be Improved	September 26, 2022
19	2022-20-052	Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk	September 27, 2022
20	2022-20-050	Mainframe Platform Configuration Compliance Controls Need Improvement	September 30, 2022
21	2022-20-065	The IRS Needs to Improve Its Database Vulnerability Scanning and Patching Controls	September 30, 2022

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

January 3, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer
Nancy A. Sieger Digitally signed by B3CCB Date: 2023.01.03 12:25:09 -05'00'

SUBJECT: Draft Audit Report – Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2022 (Audit #202220002)

Thank you for the opportunity to respond to this report, which is based on previous TIGTA and Government Accountability Office reports issued during Fiscal Year (FY) 2022. In FY 2022, the IRS's Information Technology organization successfully implemented corrective actions to address 78 recommendations, while continuing to invest in a highly effective and multi-layered cybersecurity program.

Some audit findings included in this report are inaccurate, and as noted in the management response to those audits, we disagree with some TIGTA findings. For example, the audit report issued in September 2022 on the IRS deployment of cloud services (TIGTA Report 2022-20-052) does not accurately reflect the agency's cloud security posture and also includes several misleading statements without appropriate context. The IRS continues to make progress deploying secure cloud services and we have a detailed corrective action plan to make additional process improvements.

We recognize that to achieve the agency's strategic goals, we must complete significant and highly complex technology transformations. The additional multi-year funding provided by the Inflation Reduction Act marks a transformational moment for our agency – and an opportunity for the future of tax administration. The IRS has struggled for many years without sufficient resources to fulfill our important mission. During the next decade, this funding will help us in many areas, including adding important resources for technology.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at 202-317-5000, or a member of your staff may contact Darrell S. White, associate chief information officer of strategy and planning, at 512-358-6671.

Appendix IV

Glossary of Terms

Term	Definition
Adjudication	The formal processes of judgment or ruling that render a final decision.
Agent (in the context of information technology)	A software routine that waits in the background and performs an action when a specified event occurs. For example, an encryption agent would transform information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
Agile	Software development methodologies centered around the idea of iterative development, where requirements and solutions evolve through collaboration between self-organizing cross-functional teams.
Antivirus Software	Scans computer files and memory to detect and eradicate malicious code.
Appropriation	Statutory authority to incur obligations and make payments out of Treasury Department funds for specified purposes.
Artifact	The output of an activity performed in a process/procedure, which is created throughout the life cycle of a project.
[redacted]	[redacted].
Audit Trail	A chronological record of information system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.
Authenticator	The means (*e.g.*, user password or token) used to confirm the identity of a user, process, or device.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Baseline	A benchmark that includes project costs, schedule, and scope against which project performance is measured.
Business Process	A set of structured activities or tasks that, once completed, will accomplish specific organization goals.
Business Unit	A title for major IRS organizations, such as the IRS Independent Office of Appeals, the Wage and Investment Division, and Information Technology.
Call Site	Provides telephone assistance for individual and business taxpayers on tax-related issues.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.

Term	Definition
Change Request	The method for requesting approval to change a baselined product or other controlled item.
Claimant	A subject whose identity is to be verified using one or more authentication protocols.
Cloud (or Cloud Computing)	The delivery of computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet to offer faster innovation, flexible resources, and economies of scale.
Cloud Service Provider	An entity offering a cloud-based platform, infrastructure, application, or storage services.
Code Repository	A repository for active builds that have traceability from source code to deployed artifacts in controlled environments that also supports staging for testing and contains build artifacts destined for controlled environments.
Common Communication Gateway	The demilitarized zone, which provides Internet connectivity and external data connectivity to Federal, State, and local government agencies and tax partners.
Containerization	When an application is "containerized," the application is segregated or isolated from the underlying operating system. The container that holds the application only uses a few libraries from the underlying operating system. This isolation of the application now allows that application to run on any standard container platform, no matter the underlying operating systems being used.
Continuous Delivery	The ability to make changes of all types (including new features, configuration changes, or bug fixes) safely and quickly, in a sustainable way; aims to build, test, and release software faster and more frequently via team practices and delivery automation.
Continuous Diagnostics and Mitigation	Provides tools, integration services, and dashboards to all participating agencies to improve their respective agency security postures to help defend against cybersecurity threats and vulnerabilities.
Continuous Integration	The regular practice of merging all developers' working copies into a shared mainline once a day (or more). Its practices drive the pipeline, and the automated build (compile) verifies integrations (check-in) to detect integration errors and provides feedback as quickly as possible, reducing integration problems and speeding development of more cohesive software.
Continuous Monitoring	The process implemented to maintain a current security status for one or more 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 and 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.

Term	Definition
Controlled Unclassified Information	A designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, *Classified National Security Information* (Apr. 1995), as amended March 25, 2003, but 1) is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and 2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation controlled unclassified information replaces sensitive but unclassified.
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.
Credentialed Scan	A scan in which the scanning computer has an account on the computer being scanned that allows a scanner to perform a more thorough check for problems that cannot be seen from the network.
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.
Default Vendor Account	A user account already created on the operating system that allows a system administrator to make changes to the system. The system administrator can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.
Defense Information Systems Agency	An agency that oversees the information technology/technological aspect of organizing, delivering, and managing defense-related information.
[redacted]	[redacted].
Enterprise Computing Center	A data center that supports tax processing and information management through a data processing and telecommunications infrastructure.
Exploit	A general term for any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.
Federal Acquisition Regulation	The primary acquisition regulation for use by all Federal executive agencies in their acquisition of supplies and services with appropriated funds.
Federal Tax Information	Consists of Federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code and subject to the § 6103(p)(4) safeguarding requirements including IRS oversight.
Federation	A collection of realms (domains) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.

Term	Definition
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Firmware	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.
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.
Governance Board Charter	Documents the roles, responsibilities, and authorities of board members and executive steering committees in advising, directing, and managing the information technology portfolio.
Grid Card	A method of identifying users in which the user is asked to input a series of characters based on a preregistered pattern on a grid (that the user knows) and a grid of pseudo-random characters generated by the authenticator. This method results in a different series of characters each time the user authenticates.
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.
Host	Any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, servers, personal electronic devices, and multifunctional devices.
Human Capital Office	Provides strategies and tools for recruiting, hiring, developing, and retaining a highly skilled and high-performing workforce.
Identity and Access Management	Provides direction for all development activities for external authentication and authorization as well as technical integration and coordination of other public-facing applications in support of the IT organization's secure data access activities, both within the IRS and with other Government agencies.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.

Term	Definition
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency. The term information technology includes computers, ancillary equipment, software, firmware, services (including support services), and related resources.
Information Technology Organization	The IRS business unit responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Infrastructure	The hardware, software, and network resources and services required for the existence, operation, and management of an enterprise information technology environment. It allows an organization to deliver information technology solutions and services to its employees, partners, and customers.
Initial Operating Capability	A point in time during the production and deployment phase when a system can meet the minimum operational (Threshold and Objective) capabilities for a user's stated need.
Insider Threat Capability	The ability to identify and take action related to insider threats.
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 unique number assigned to every computer or device that is connected to the Internet.
Key Management Solution	A solution used to manage encryption keys of various activities, including key generation, exchange, distribution, rotation, replacement, storage, access, backup, and destruction. Encryption cannot be deployed without an associated working key management solution, also referred to as a key management system.
Legacy System	An information system that may be based on outdated technologies but is critical to day-to-day operations.
Mainframe	A powerful, multiuser computer capable of supporting simultaneously many hundreds of thousands of users.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Managed Service Provider	A third-party company that remotely manages a specified set of information technology processes, such as security, infrastructure, maintenance, support, *etc.*, for end-user systems.
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.

Term	Definition
Milestone	A management decision point placed at a natural breakpoint in the life cycle, at the end of the phase, where management determines whether a project can proceed to the next phase.
Modification	Any formal change to the terms and conditions of a contract, delivery order, or task order, either within or outside the scope of the original agreement.
Multifactor Authentication	Verifying the identity of a user, process, or device using two or more factors to achieve authentication, often as a prerequisite to allowing access to resources in an information system. Factors include: 1) something you know (*e.g.*, password/personal identification number); 2) something you have (*e.g.*, cryptographic identification device and token); or 3) something you are (*e.g.*, biometric).
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines to provide adequate information security for all Federal agency operations and assets.
National Settlement Days	A program in which the IRS spends certain days 1) coordinating efforts that aim to resolve/settle cases in U.S. Tax Court and 2) coming to a settlement agreement with taxpayers who owe back taxes.
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.
Nonprivileged	Any user right assignment that is at the organization's baseline.
Onboard	The process whereby the continuous integration/continuous delivery pipeline runs the code through a series of validations for security, code quality, and unit tests to make sure it meets all standards. At least once each day, all newly developed code is deployed to the development environment.
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.
Parallel Validation	Compares legacy IMF output with the output generated by the Java code for Runs 12 and 15 and will occur prior to the Individual Tax Processing Engine moving into production.
Patch	Updates to an operating system, application, or other software issued specifically to correct particular problems with the software.
Personal Identity Verification Card	A Government-issued identity credential that contains a contact and a contactless chip. The cardholder's facial image is printed on the card along with other identifying information and security features that can be used to authenticate the user for physical access to Federally controlled facilities and logical access to Federally controlled information systems.

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 that is linked or linkable to a specific individual, such as date of birth, place of birth, and mother's maiden name.
Ping	A signal sent to a host that requests a response to check if the host is available.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Platform	A computer or hardware device, an associated operating system, or a virtual environment on which software can be installed or run.
Portal	A web-based infrastructure (hardware and software) that serves as the entry point for web access to applications and data.
Portfolio	The combination of all information technology assets, resources, and investments owned or planned by an organization in order to achieve its strategic goals, objectives, and mission.
Privileged (or Privileged Account)	Accounts with set "access rights" for certain users on a given system. Sometimes referred to as system or network administrative accounts.
Processing Year	The calendar year in which the tax return or document is processed by the IRS.
Production (or 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.
Project Tailoring Plan	A documented agreement between the project manager, organization, and process owner(s) regarding how the project will meet the established process requirements. This document identifies the process artifacts and reviews required to be completed by the project and any provisions or exceptions to the processes.
Release	A specific edition of software that is deployed into production.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Requirement	Describes a condition or capability to which a system must conform, either derived directly from user needs or stated in a contract, standard, specification, or other formally imposed document. A desired feature, property, or behavior of a system.
Risk-Based Decision	A decision made when meeting a requirement is technically or operationally not possible or is not cost effective. It is required for any situation in which the system will be operating outside of IRS information technology security policy or NIST guidelines, whether related to a technical, operational, or management control.

Term	Definition
Security Assessment Report	Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.
[redacted]	[redacted].
Security Update	A widely released fix for a product-specific, security-related vulnerability.
Sensitive But Unclassified	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under the Privacy Act that could result from inadvertent or deliberate disclosure, alteration, or destruction.[1]
Software-as-a-Service	Software that is provided by an independent vendor and typically hosted on the cloud.
Sprint	A process that develops a piece of functionality of the system with repeated cycles of requirements discovery, planning, design, development, and testing. The goal of each sprint is to get a subset of the project's functionality to a production-ready state.
Standard Stack	A set of standardized software and server configurations used in the provisioning of systems, applications, and services in a rapid, repeatable fashion.
Subscriber	A party who has received a credential or authenticator from a credential service provider. If the applicant is successfully proofed, the individual is then termed a subscriber of that credential service provider.
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Tax Processing Center	The arm of the IRS that processes paper-filed and electronic tax returns, payments, and refunds.
Tax Year	The 12-month accounting period for which tax is calculated. For most individual taxpayers, the tax year is synonymous with the calendar year.
Telework	A work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work.
Tier I	A computing infrastructure consisting of mainframe computers that handle a high volume of critical operational data.
Tier II	Minicomputers (*i.e.*, computers usually containing multiple microprocessors) capable of executing multiple processes simultaneously. They may serve multiple users by way of a communications network, including hardware, software, and peripheral subsystems used in that environment.

[1] 5 U.S.C. § 552a.

Term	Definition
Trusted Internet Connection	A Federal initiative for which the primary goals are to consolidate and secure Federal agency external connections using a common set of security controls and to improve the Federal Government's incident response capability.
Unauthorized Access	The willful unauthorized access and inspection of taxpayer returns or return information.
Unit Testing	Ensures that program modules perform in accordance with requirements.
User Behavior Analytics	A type of analytic that detects actions taken by a human user, versus by a system.
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.
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.
Waterfall	Distinguished by development of a solution with frequent reviews and formal approvals required at multiple points in the life cycle prior to additional work being performed.

Appendix V

Abbreviations

ARPA	American Rescue Plan Act of 2021
BEARS	Business Entitlement Access Request System
CADE	Customer Account Data Engine
CIO	Chief Information Officer
COVID-19	Coronavirus Disease 2019
CSP	Cloud Service Provider
CTC	Child Tax Credit
ELC	Enterprise Life Cycle
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
IMF	Individual Master File
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
MSP	Managed Service Provider
NGI	Next Generation Infrastructure
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SADI	Secure Access Digital Identity
SCRM	Supply Chain Risk Management
SEG	Network Segmentation
TDC	Taxpayer Digital Communications
TIGTA	Treasury Inspector General for Tax Administration
UBAC	User Behavior Analytics Capability
UNS	User and Network Services

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

(800) 366-4484

By Web:

www.tigta.gov

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 23291

Washington, D.C. 20026

Information you provide is confidential, and you may remain anonymous.