TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2023

February 12, 2024

Report Number: 2024-200-015

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

HIGHLIGHTS: Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2023

Final Audit Report issued on February 12, 2024 **Report Number 2024-200-015**

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 2023, the IRS collected approximately $4.7 trillion in Federal tax payments and processed 275 million tax returns and forms. In addition, IRS Federal tax refund and outlay activities were approximately $659 billion.

The IRS employs over 90,000 people in its Washington, D.C., Headquarters and over 470 offices in all 50 States and U.S. Territories, and these employees are engaged in a wide array of tax administration functions from taxpayer service to enforcement of Federal tax laws.

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. Reviews showed that known exploited vulnerabilities issues were communicated across the IRS and that one ransomware attack was mitigated by properly applying incident response procedures. In addition, the IRS met its agency-wide completion goal of 97 percent for training its employees on protecting taxpayer information. However, additional reviews showed that contractors have not taken the required annual privacy awareness training.

The Fiscal Year 2023 IRS Federal Information Security Modernization Act evaluation found that the Cybersecurity program was effective in two and not effective in three of five Cybersecurity Framework function areas. The IRS needs to take further steps to improve its security program deficiencies and fully implement all security program components in compliance with the Federal requirements.

Problems were also reported in the IRS's handling of the privacy of taxpayer data; access controls; system environment security; disaster recovery; and security policies, procedures, and documentation as well as system security training. For example, in one review, the IRS reviewed only 22 and did not review 2,793 of 2,815 unauthorized software it identified. In another review, the IRS did track all on-premises Federally reportable systems in the Cyber Security Assessment and Management application as required.

Reviews of systems development and information technology operations found that, in one review, the IRS completed the first phase of the Continuous Diagnostics and Mitigation Program by installing sensor tools to identify authorized hardware and software assets and ensured that they were properly configured with vulnerabilities mitigated. In another review, the IRS has procedures for hiring information technology staff outside of the Information Technology organization but does not have a process in place to ensure that inherently information technology-related work is not being performed by this staff.

For Fiscal Year 2024, TIGTA has recently completed or is performing several reviews related to data security threats, such as the system security problems identified in the data breach that led to the release of taxpayer information and subsequent prosecution and guilty plea of the accused.

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 2023, TIGTA did not make any further recommendations.

In its management response to this report, the IRS commented on the actions taken since the issuance of the prior audit reports.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20024

February 12, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Matthew A. Weir
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2023 (Audit No.: 202320002)

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 review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenges of *Information Technology Modernization*, *Protection of Taxpayer Data and IRS Resources*, *Tax Law Changes*, and *Taxpayer Service*.

Management's complete response to the draft report is included as Appendix IV. 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

Appendices

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 (FY) 2023.

The IRS collects taxes, processes tax returns, and enforces Federal tax laws. In FY 2023, the IRS collected approximately $4.7 trillion in Federal tax payments and processed 275 million tax returns and forms. In addition, Federal tax refund and outlay activities by the IRS were approximately $659 billion.[2] This was an increase of 3 percent compared to FY 2022.

In FY 2023, the IRS collected approximately $4.7 trillion in Federal tax payments and paid approximately $659 billion in refund and outlay activities.

The size and complexity of the IRS add unique operational challenges. The IRS employs over 90,000 people in its Washington, D.C., Headquarters and over 470 offices in all 50 States and U.S. Territories, and its employees are engaged in a wide array of tax administration functions from taxpayer service to enforcement of Federal tax laws. 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.[3] 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 business systems modernization as well as other areas (*e.g.*, study on a free direct electronic filing tax return system).[4] The business systems modernization area of the legislation 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.

[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 V for a glossary of terms.

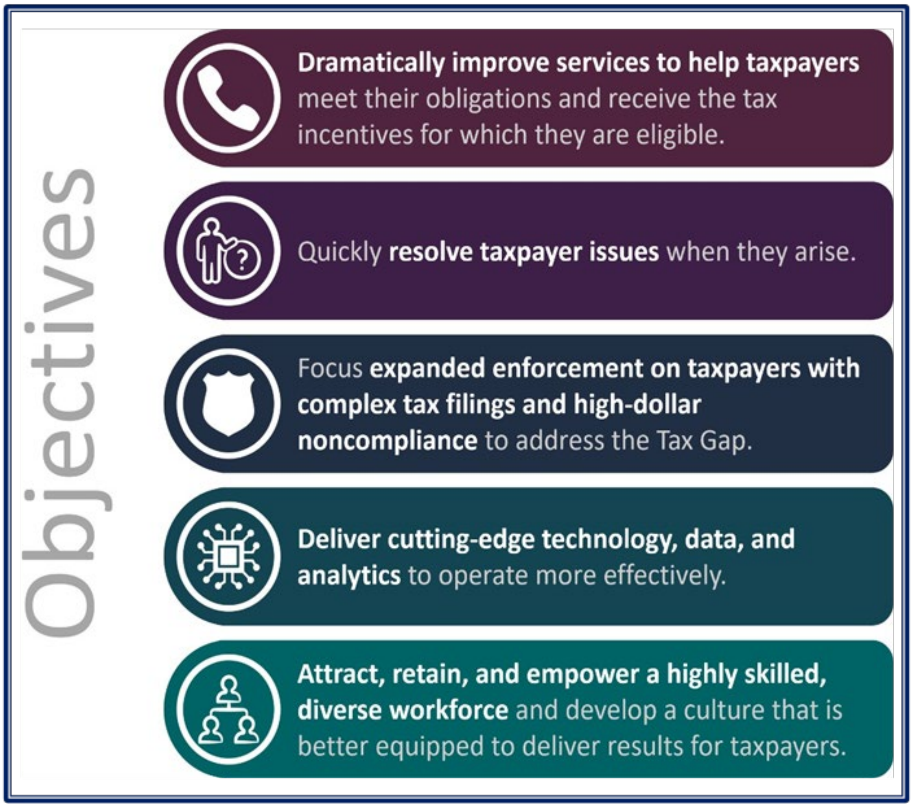
[2] Federal tax refund and outlay activities include refunds of tax overpayments, payments for interest, and disbursements for refundable tax credits, such as the Earned Income Tax Credit.

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

[4] In June 2023, the Fiscal Responsibility Act of 2023 resulted in the rescission of approximately $1.4 billion of Inflation Reduction Act funding provided to the IRS. In addition to the rescission, the Administration agreed to reduce future IRS appropriations by approximately $20 billion.

In April 2023, the Department of the Treasury (hereafter referred to as the Treasury Department) and the IRS developed the *Internal Revenue Service Inflation Reduction Act Strategic Operating Plan, FY 2023 – 2031*. The plan outlines how the IRS will deploy investments from the Inflation Reduction Act to better serve taxpayers, tax professionals, and the broader tax ecosystem. Figure 1 shows that the plan is structured to achieve five objectives, which will be accomplished through a series of initiatives and projects aligned to each.

Figure 1: Five Objectives of the IRS's Inflation Reduction Act Strategic Operating Plan



Objectives

Dramatically improve services to help taxpayers meet their obligations and receive the tax incentives for which they are eligible.

Quickly **resolve taxpayer issues** when they arise.

Focus **expanded enforcement on taxpayers with complex tax filings and high-dollar noncompliance** to address the Tax Gap.

Deliver cutting-edge technology, data, and analytics to operate more effectively.

Attract, retain, and empower a highly skilled, diverse workforce and develop a culture that is better equipped to deliver results for taxpayers.

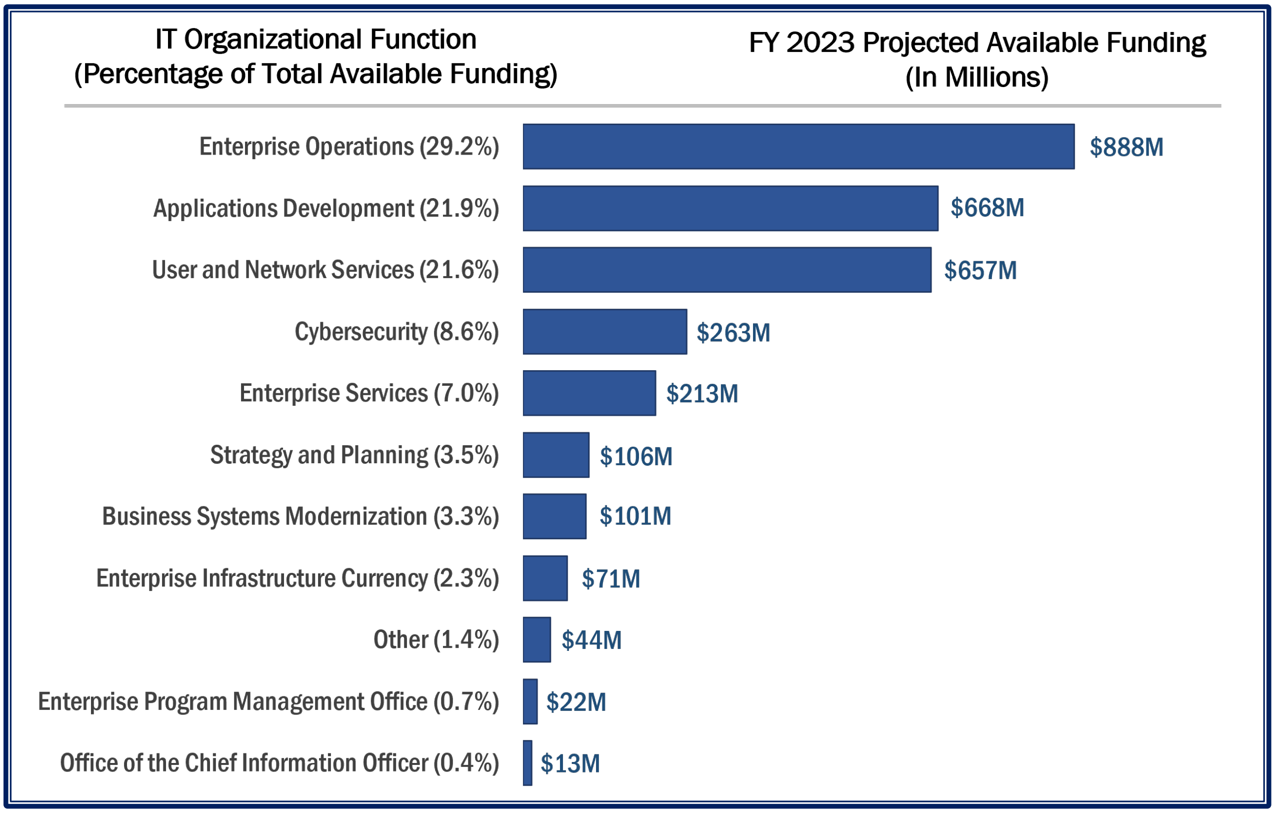
Source: TIGTA's analysis of the Internal Revenue Service Inflation Reduction Act Strategic Operating Plan, FY 2023 – 2031, five objectives.

Information technology budget

In FY 2023, the IRS's appropriations decreased by $275 million to $12.3 billion, designated for taxpayer services, enforcement, operations support, and business systems modernization.[5] 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 FY 2023 projected available funds included approximately $4.8 billion for information technology investments, of which $3.7 billion was received to fund recent legislative requirements. Figure 2 illustrates the IRS's FY 2023 information technology projected available funding by IT organization function and major program.

[5] This amount does not include any of the funds the IRS received from Congress to implement pandemic-related tax benefits, which totaled $3.1 billion when they were enacted.

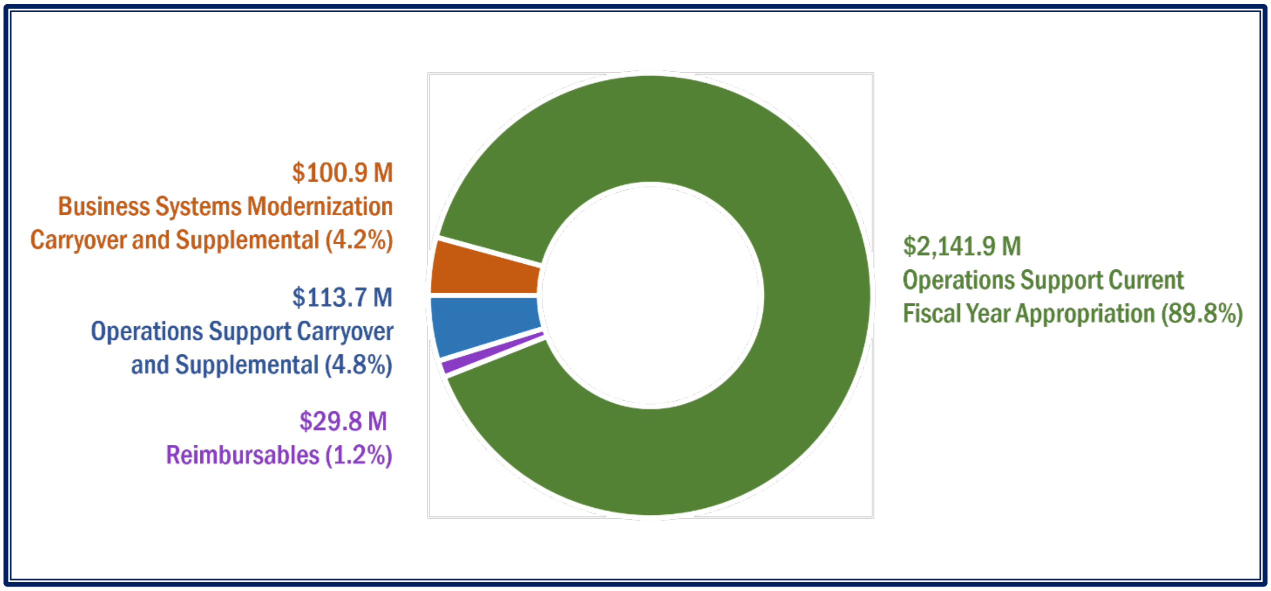
Figure 2: FY 2023 Information Technology Projected Available Funding by IT Organization Function and Major Program



Source: IT organization budget data as of May 2023, 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. The percentages do not add up to 100 percent due to rounding.

Figure 3 shows the IT organization's actual available funding for FY 2023 by funding source.

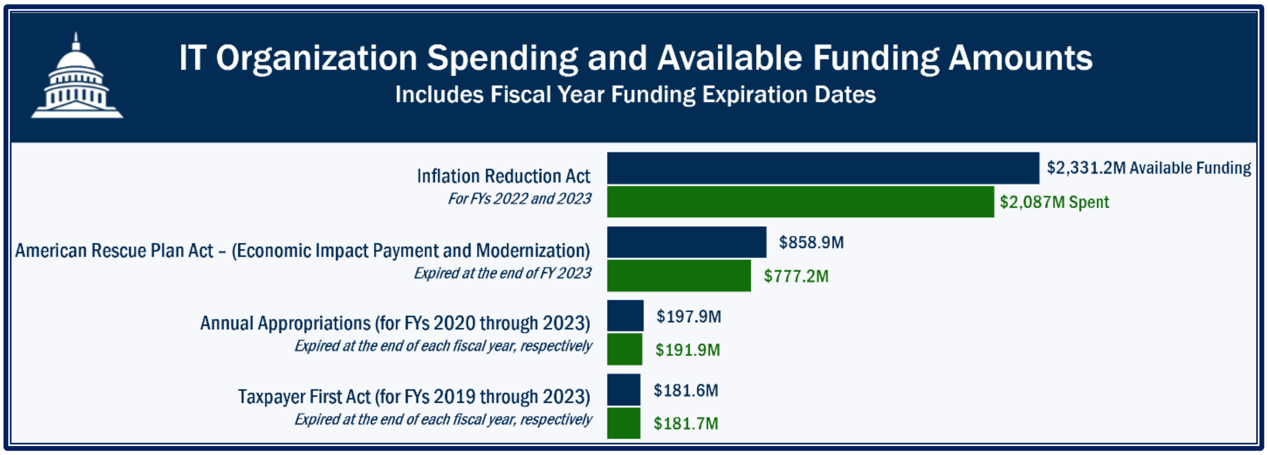
Figure 3: FY 2023 Total Actual Available Funding by Funding Source



Source: IT organization budget data as of May 2023, based on information provided by the Strategy and Planning function's Office of Financial Management Services.

Figure 4 presents the IT organization's total spending and available funding for recent legislative requirements by legislation as of September 30, 2023.

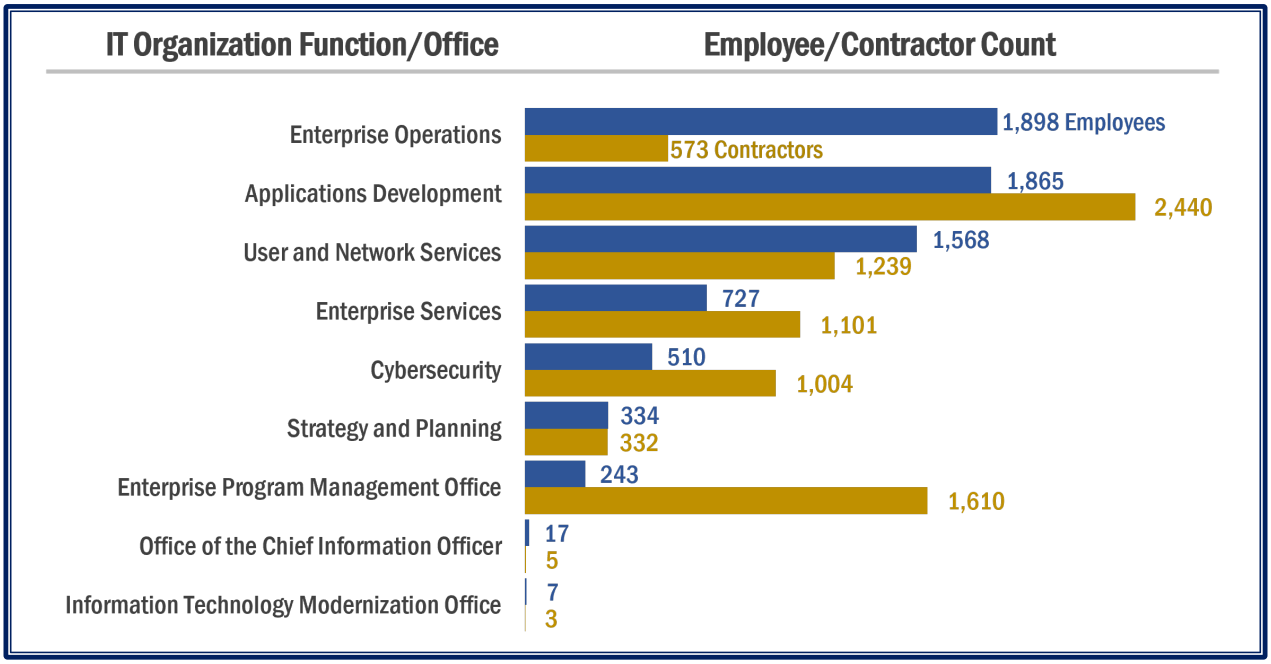
Figure 4: IT Organization Spending and Available Funding for Recent Legislative Requirements by Legislation (in Descending Available Funding Order)



Source: IT organization budget and expense data as of September 30, 2023, based on information provided by the Office of the Chief Financial Officer's Financial Planning and Analysis office.[6]

Figure 5 illustrates that, as of May 2023, the IRS had a total of 7,169 employees and 8,307 contractors working across nine different IT organization functions and offices – 185 more employees and 757 more contractors than reported in FY 2022.

Figure 5: Number of Employees and Contractors by IT Organization Function and Office (in Descending Employee Order)



Source: IRS Human Resources Reporting Center as of May 2023.

[6] 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.) and Pub. L. No. 116-25, 133 Stat. 981 (codified in scattered sections of 26 U.S.C.).

- 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), the Chief Technology Officer, two Deputy CIOs, and their employees.
  - The CIO oversees the development, implementation, and maintenance of information technology throughout the IRS; ensures that the information technology is secure and integrated; maintains operational control over the information technology; and acts as the principal advocate for the IRS's information technology needs.
  - The Chief Technology Officer leads information technology technical activities, including engineering, architecture and design activities, infrastructure, applications development, networks, enterprise information security, and compliance with security standards as well as computer operations support.
  - The Deputy CIO for Operations has oversight responsibility for the day-to-day operations of information systems and services. In addition, the Deputy CIO for Operations is focused on upgrading the 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.
- The Information Technology Modernization Office leads the Service-wide effort to modernize the Individual Master File ecosystem.

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 *Information Technology Modernization*, *Protection of Taxpayer Data and IRS Resources*, *Tax Law Changes*, and *Taxpayer Service*. This report presents a summary of TIGTA and Government Accountability Office (GAO) audit results previously reported for FY 2023.[7] 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.

With the additional funding from the Inflation Reduction Act, 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.

Information System 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) report that provides an overall assessment of the information security program, we performed several audits to assess the IRS's efforts to protect its information and taxpayer

[7] See Appendix II for a complete list of audit reports.

data.[8] Our audits covered privacy of taxpayer data; access controls; system environment security; disaster recovery; security policies, procedures, and documentation; and system security training.[9]

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, 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.

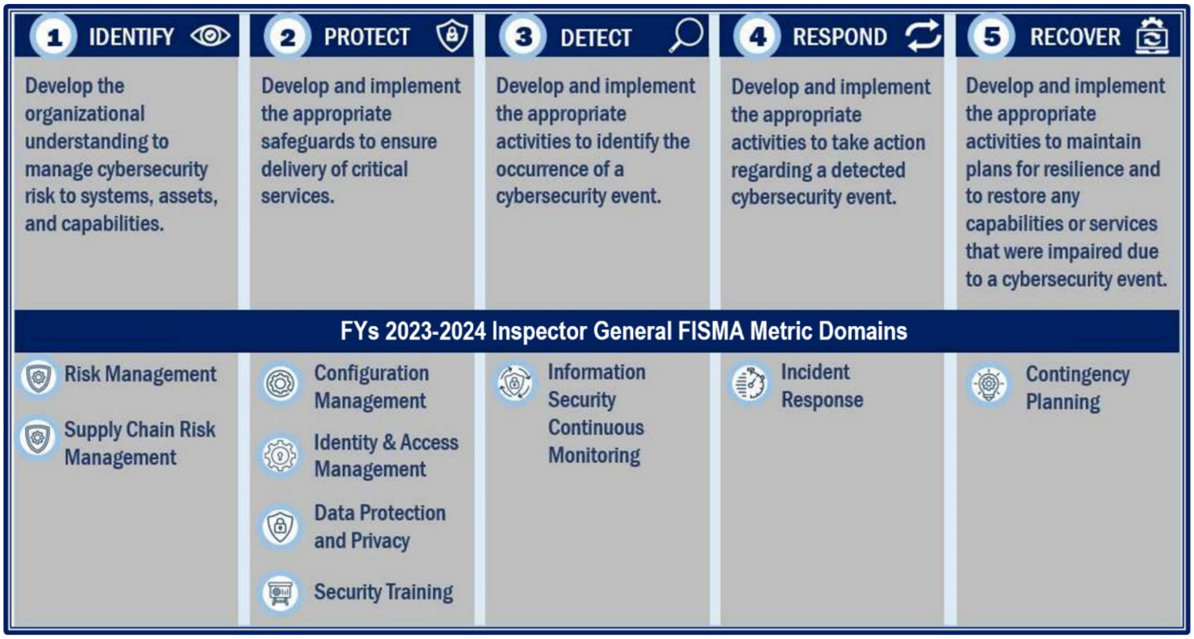
The FISMA directs Federal agencies to report annually to the Office of Management and Budget Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices as well as compliance 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 Office of Management and Budget. 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 Treasury Department's Office of Inspector General is responsible for all other Treasury Department bureaus.

The *Fiscal Years 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (hereafter referred to as the Inspector General FISMA Reporting Metrics) was developed as a collaborative effort among representatives from the Office of Management and Budget, the Council of the Inspectors General on Integrity and Efficiency, and the Federal Civilian Executive Branch Chief Information Security Officers, and aligns with the five cybersecurity function areas in the NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (hereafter referred to as the Cybersecurity Framework), Version 1.1 (Apr. 2018) as shown in Figure 6.

[8] 44 U.S.C. § 3551, et seq. (2018). TIGTA, Report No. 2023-20-041, *Fiscal Year 2023 IRS Federal Information Security Modernization Act Evaluation* (Aug. 2023).

[9] See Appendix III for a complete list of finding categories and associated reports, along with the number of reported findings.

Figure 6: Alignment of NIST Cybersecurity Framework Function Areas to FYs 2023 Through 2024 Inspector General FISMA Metric Domains

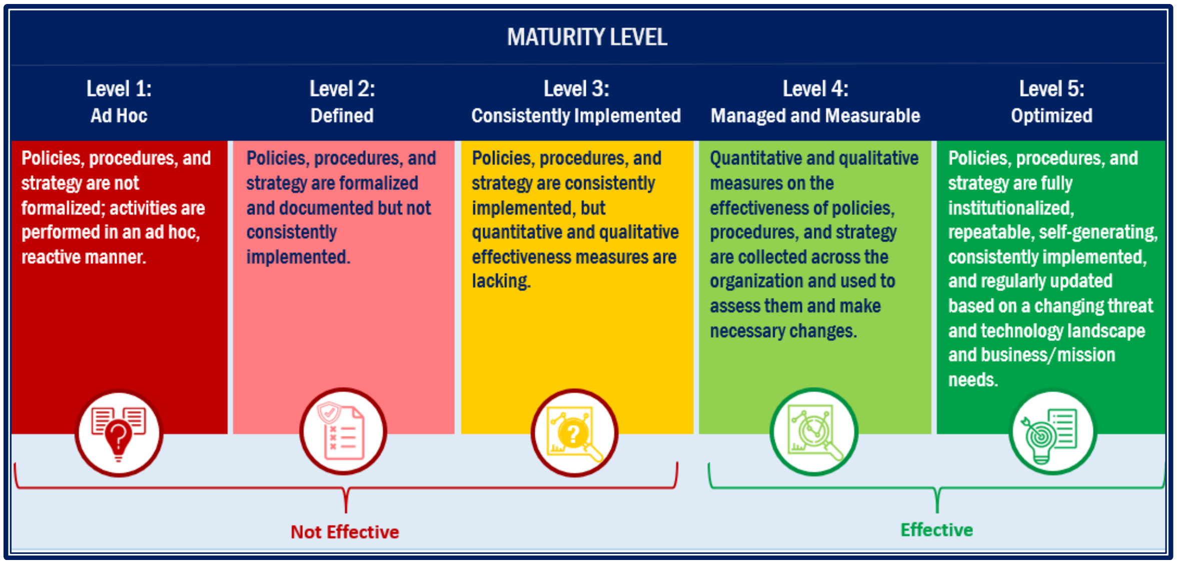


1 IDENTIFY	2 PROTECT	3 DETECT	4 RESPOND	5 RECOVER
Develop the organizational understanding to manage cybersecurity risk to systems, assets, and capabilities.	Develop and implement the appropriate safeguards to ensure delivery of critical services.	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
FYs 2023-2024 Inspector General FISMA Metric Domains				
Risk Management Supply Chain Risk Management	Configuration Management Identity & Access Management Data Protection and Privacy Security Training	Information Security Continuous Monitoring	Incident Response	Contingency Planning

Source: *Inspector General FISMA Reporting Metrics and NIST Cybersecurity Framework.*

The Inspectors General are required to assess the effectiveness of the information security programs based on a maturity model spectrum in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institute 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 7 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 7: Inspector General's Assessment Maturity Levels



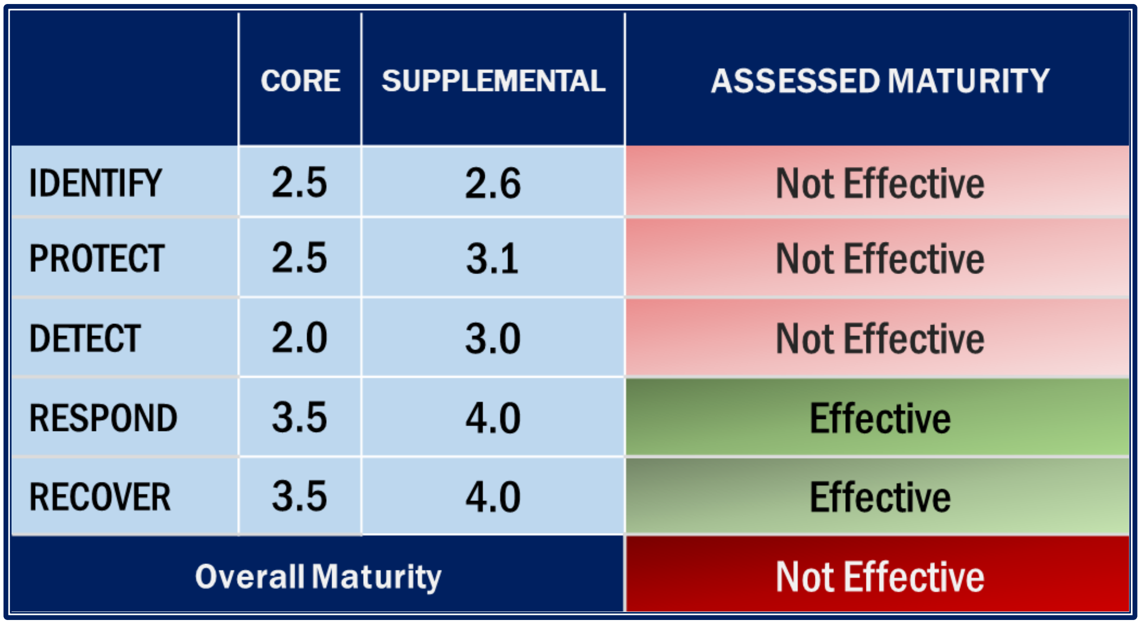
MATURITY LEVEL				
Level 1: Ad Hoc	Level 2: Defined	Level 3: Consistently Implemented	Level 4: Managed and Measurable	Level 5: Optimized
Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.	Policies, procedures, and strategy are formalized and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

Source: *Inspector General FISMA Reporting Metrics.*

To determine the effectiveness of the Cybersecurity program, we evaluated the maturity level of the program metrics as specified in the *Inspector General FISMA Reporting Metrics*. Along with our review of pertinent documents and discussions with IRS subject matter experts, we based our evaluation on a representative subset of seven information systems and the implementation status of key security controls as well as considered the results of TIGTA and GAO audits. These audits, whose results were applicable to FISMA reporting metrics, were performed, completed, or contained recommendations that were still open during the FISMA evaluation period July 1, 2022, to June 2, 2023.

The Cybersecurity program was "not effective" in three and "effective" in two of the five Cybersecurity Framework function areas. Specifically, the IDENTIFY, PROTECT, and DETECT capabilities are "not effective" and the RESPOND and RECOVER capabilities are "effective." As a result, we rated the Cybersecurity program as "not fully effective." Figure 8 presents the Cybersecurity Framework function areas' ratings averaged independently to determine a function's assessed maturity.

Figure 8: FY 2023 Inspector General Cybersecurity Framework Assessment Results



	CORE	SUPPLEMENTAL	ASSESSED MATURITY
IDENTIFY	2.5	2.6	Not Effective
PROTECT	2.5	3.1	Not Effective
DETECT	2.0	3.0	Not Effective
RESPOND	3.5	4.0	Effective
RECOVER	3.5	4.0	Effective
Overall Maturity			Not Effective

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

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; ensuring that its information systems consistently maintain baseline configuration in compliance with IRS policy; implementing flaw remediation and patching on a timely basis; encrypting to protect data at rest; and implementing multifactor authentication on its facilities and network. The IRS needs to take further steps to improve its security program deficiencies and fully implement all security program components in compliance with 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 FY 2023, TIGTA and the GAO performed four audits involving privacy of taxpayer data. We initiated an audit to determine if the IRS randomly selected individual tax returns for Tax Years 2017 and 2019 National Research Program audits.[10] The IRS conducts National Research Program audits to collect compliance data for different types of taxes and various sets of taxpayers. Four computer programs are used to select the sample for audit from the population of tax returns processed each week. The audits are designed to provide a statistically valid representation of the compliance characteristics of taxpayers.

In July 2022, IRS officials requested that a contractor, who was not involved with the Tax Years 2017 and 2019 sample selections, replicate the process. Specifically, the contractor was asked to replicate each week's original sample selection file using the Tax Years 2017 and 2019 historical tax return files and the computer programs developed and implemented at the time. The contractor performed a line-by-line review of the original source code for one computer program to determine whether the Taxpayer Identification Number was improperly coded and would result in a specific taxpayer being selected for a National Research Program audit. This program selects Form 1040, *U.S. Individual Income Tax Return*, series returns for final sample selection case assignment. The contractor concluded that no specific taxpayer information was included in the original source code. The contractor walked us through the program to identify and confirm this information, and we did not identify any sections with specific taxpayer information. Further, we performed an electronic search of the four computer programs for 20 judgmentally selected tax returns to confirm that there were no Taxpayer Identification Numbers associated with these taxpayers improperly coded in the programs.[11]

The contractor also verified that no changes were made subsequent to the completion of the computer program used to select the sample. We reviewed documentation confirming the dates that the Tax Years 2017 and 2019 original source coding were completed (put into production). We also confirmed that no changes were made to three of the four programs once put into production. For the remaining program, the contractor updated the program several weeks into the respective processing years. Our review of the updates made did not identify any changes that would materially impact or change the integrity of the selection process.

[10] TIGTA, Report No. 2023-IE-R002, *National Research Program Tax Return Selection Process for Tax Years 2017 and 2019* (Nov. 2022).

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

We also initiated an audit to follow up on prior audit recommendations, assess the adequacy of Income Verification Express Service modernization efforts, and assess compliance with Taxpayer First Act provisions.[12] In Calendar Year 2006, the Income Verification Express Service Program was created to provide tax transcripts to a third party (*i.e.*, Income Verification Express Service participant) with consent of the taxpayer. Tax transcripts can include return information, account information, and wage and income information. The tax transcripts are often used by third parties (*e.g.*, clients of Income Verification Express Service participants, such as banks) to process mortgages, *etc*.

In July 2019, the Taxpayer First Act was signed into law, which required the IRS to develop a modernized system to receive third-party transcript request forms that is fully automated and accomplished through the Internet in as close to real-time as is practicable and complies with applicable security standards and guidelines. This new modernized system would replace its current system, which relies on secure electronic faxes. Despite the Taxpayer First Act requiring the IRS to create a new online system to process transcripts, IRS management has not yet made a decision to require participants to use the new system.

We previously reported concerns with the lack of validation of taxpayer signatures on transcript requests, noting that this would be resolved by implementing the modernized Income Verification Express Service system. However, until the IRS requires participants to use the new modernized system, participants will be allowed to continue to electronically fax transcript requests. As such, we remain concerned that without proper controls to sufficiently and adequately validate the transcript request form, there will continue to be a risk of releasing taxpayers' information to unauthorized individuals. IRS management should be proactive in ensuring that additional controls are put in place to prevent fraudsters from exploiting the Income Verification Express Service Program.

The GAO initiated an audit to evaluate the extent to which the IRS is following its tax safeguards for protecting taxpayer information.[13] The GAO reported that the IRS has taken steps to develop and maintain an inventory of information systems that process or store Personally Identifiable Information and taxpayer information. However, the IRS has not completed the inventory. As of December 2022, the GAO identified seven information systems that the IRS omitted from its inventory. In addition, inventory entries for 118 systems were not complete. Specifically, the entries did not establish whether the systems process or store Personally Identifiable Information or taxpayer information. Maintaining a comprehensive system inventory will help the IRS ensure that it has implemented safeguards to protect taxpayer information being processed or stored on all of its systems, applications, and databases.

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

[12] TIGTA, Report No. 2023-45-014, *Additional Actions Are Needed to Improve and Secure the Income Verification Express Service Program* (Mar. 2023).

[13] GAO, GAO-23-105395, *SECURITY OF TAXPAYER INFORMATION: IRS Needs to Address Critical Safeguard Weaknesses* (Aug. 14, 2023).

other computing resources. Access controls include both physical and system security access controls (*i.e.*, authentication and identity proofing, authorization, and access management).

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 FY 2023, TIGTA performed an audit on physical security access controls. We initiated an audit to evaluate the deployment of the Enterprise Physical Access Control System (EPACS) and security controls over the system.[14] All Government employees and contractors are required to use standard identification to gain physical access to Federally controlled facilities.[15] The EPACS provides electronic physical access control to IRS facilities by authenticating employees' SmartID when presented to a card reader at a perimeter door or at controlled and limited access doors inside IRS-protected areas.

We conducted walkthroughs at eight IRS facilities to evaluate physical access controls (*i.e.*, card readers and notifications from actionable alarms) over Controlled and Limited Areas. Access to the Controlled Area of a secured facility requires a single authentication mechanism to ensure that only authorized personnel have access. Access to a Limited Area is granted to authorized personnel only and requires two-factor authentication to gain access. We found that Limited Areas were secured with inadequate, improperly configured, or inoperable card readers, and an alarm did not always appear in the EPACS viewer or was not timely addressed.

Limited Areas were secured with inadequate, improperly configured, or inoperable card readers

We used the Door Group Design Document to select a judgmental sample of Controlled and Limited Area doors to determine whether the correct card reader was installed and operational. The Door Group Design Document is used to map out all the components and elements of the door groups based on business rules for site access. All Controlled Areas we tested were properly secured by single-factor authentication card readers. However, five (63 percent) of eight sites visited did not always have two-factor authentication card readers effectively installed to secure Limited Areas. Specifically, three facilities had Limited Areas with incorrect card readers installed. In addition, one facility contained 24 two-factor authentication card readers that were not configured for two-factor authentication. IRS management subsequently stated that there are an additional 1,262 of the same type of noncompliant card readers at other locations. Another facility contained a two-factor authentication card reader that was broken. Without adequate access controls, the IRS is not compliant with Federal requirements, and the sensitive equipment and information in the Limited Area may be at risk of unauthorized access or disclosure.

[14] TIGTA, Report No. 2023-20-062, *The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement* (Sept. 2023).

[15] Department of Homeland Security, *Homeland Security Presidential Directive-12* (Aug. 2004).

An alarm did not always appear in the EPACS viewer or was not timely addressed

Facilities Management and Security Services management provided an Actionable Alarms Report, which lists alarms generated by the EPACS that require action. Examples of alarms include forced entry at input (appears when circumventing the EPACS, such as using keys to open doors), Denied: Bad Personal Identification Number (good card), and Door Open Too Long. When alarms are generated, they appear in the EPACS Event Viewer and can be viewed by any EPACS operator who has permission to view that site.

We performed tests at seven of eight facilities to determine whether alarms are generated when a door is opened too long, when an invalid Personal Identification Number is used, and when a SmartID card is used to enter an area where the card holder is not authorized to enter.[16] We identified one instance at one facility where we held the door open longer than allowed but the Door Open Too Long alarm did not appear on the EPACS Event Viewer.

In addition, we visited two facilities with command centers (one facility was and one facility was not part of the eight facilities originally selected for review because not all facilities have command centers) where guards monitor the EPACS Event Viewer 24 hours a day, every day. The guards at one facility (not part of the original eight facilities) monitor seven campus buildings within its local area, which includes one of the original eight facilities. However, no one constantly monitors the EPACS Event Viewer for the other six locations we visited. Without adequate and timely response to alarms, the IRS increases the risk of unauthorized individuals gaining access to information technology assets and sensitive taxpayer information.

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 (*i.e.*, multifactor authentication), such as a SmartID.

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

[16] For various reasons, this was not tested at four sites.

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 FY 2023, TIGTA performed an audit covering authentication and identity proofing. We initiated an audit to assess the IRS's efforts for its planned implementation of Login.gov.[17] In June 2021, the IRS implemented the Secure Access Digital Identity system as its next-generation identity proofing and authentication solution. The IRS built the Secure Access Digital Identity system with the concept of transitioning to credential service providers, who are independent and trusted third parties, that issue user authenticators and provide electronic credentials for accessing a system and/or an application.

Applications are assigned one of three Identity Assurance Levels based on an assessed risk profile of the sensitivity of information, such as Social Security Numbers, and the potential harm caused if an attacker made a successful false claim of an identity to gain system access. The three Identity Assurance Levels established by the NIST and that are used to verify users before granting system access to sensitive information are:

- Identity Assurance Level 1: No requirement to link the applicant to a specific real-life identity. Authentication process attributes are self-asserted.
- Identity Assurance Level 2: Evidence supports claimed identity and verifies applicant remotely or physically. Attributes can be asserted by credential service providers to relying parties.
- Identity Assurance Level 3: Physical presence is required for identity proofing. Attributes must be verified by an authorized and trained credential service providers representative.

As of June 2023, the IRS was leveraging two credential service providers for the Secure Access Digital Identity system, including Login.gov.[18] Login.gov is not Identity Assurance Level 2 certified but provides identity proofing services for two IRS Identity Assurance Level 1 applications.

According to a memorandum issued by IRS executives, they were directed by the Treasury Department to consider the use of Login.gov as a credential service provider. However, the IRS's planning efforts to use Login.gov to authenticate taxpayers for access to Identity Assurance Level 2 applications created stakeholder concerns. We found that the IRS continued planning efforts and expending resources (*e.g.*, personnel and funds) for the implementation of Login.gov for IRS Identity Assurance Level 2 applications even though Login.gov security concerns (*i.e.*, not complying with NIST Identity Assurance Level 2 standards and not fully implementing Office of Management and Budget's anti-fraud program) raised by IRS leadership and TIGTA's Office of Investigations were not fully addressed by the General Services Administration. In addition, the IRS continued to expend limited resources, at the request of the Treasury Department, towards planning efforts to implement Login.gov for its Identity Assurance Level 2 applications after the General Services Administration postponed Login.gov's implementation.

[17] TIGTA, Report No. 2023-2S-070*, Key Events of the IRS's Planning Efforts to Implement Login.gov for Taxpayer Identity Verification* (Sept. 2023).

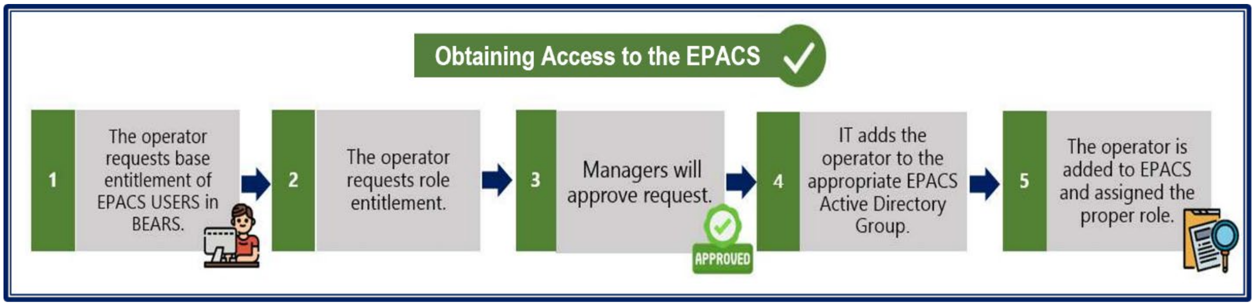
[18] The General Services Administration developed Login.gov to provide identity verification services for Federal Government applications.

Authorization

Authorization is the process of granting access rights and privileges to a system or file. Access rights and privileges specify what a user can and cannot perform in a system, such as to read or write to files and directories. A key component of authorization is the concept of "least privilege," which specifies that users should be granted the least amount of privileges necessary to perform their duties. Effectively designed and implemented authorization controls limit the files and resources users can access and execute based on a valid need as determined by assigned duties. Maintaining access rights and privileges is one of the most important aspects of administering system security.

In FY 2023, TIGTA performed three audits covering authorization. In our audit of the EPACS, we found that the EPACS operator account management process was not effective. Figure 9 depicts the process for granting operators access to the EPACS.

Figure 9: Process for Granting Operators Access to the EPACS


Obtaining Access to the EPACS
1
The operator requests base entitlement of EPACS USERS in BEARS.
2
The operator requests role entitlement.
3
Managers will approve request.
APPROVED
4
IT adds the operator to the appropriate EPACS Active Directory Group.
5
The operator is added to EPACS and assigned the proper role.

Source: TIGTA's analysis of the process for granting EPACS operator access. BEARS=Business Entitlement Access Request System.

We judgmentally selected a sample of 81 EPACS operator accounts for review. We compared the roles for the operator accounts to the entitlements in the BEARS to determine whether they were effectively managed. We determined that 14 (17 percent) of 81 EPACS operator roles did not have a matching entitlement in the BEARS. Specifically, privileged EPACS operator account roles are not consistently applied, EPACS operator roles are changed without matching entitlements, the administrator role does not require approval through the BEARS, and the inactivity control did not always work as intended. The operator account issues identified occurred because the EPACS Operations Guide does not clearly specify the procedures for granting and disabling accounts. Without documented procedures in place, EPACS operators may be able to access more critical data, privileges, and application functions than they need, which may lead to increased system security risks.

We also initiated an audit to determine whether the IRS is effectively implementing the Cyber Security Assessment and Management application (CSAM).[19] The CSAM is developed and maintained by the Department of Justice. The IRS leverages the CSAM to complete NIST security control assessments and to maintain system security plans (SSP) throughout the systems' life cycle. The CSAM also provides an agencywide view of the status of information system security, the implementation of information technology security controls, and information system compliance documentation.

[19] TIGTA, Report No. 2023-20-064, *Actions Need to Be Taken to Improve the Cyber Security Assessment and Management Application Security Controls* (Sept. 2023).

The process to obtain CSAM access requires the user to request access through the BEARS, take the CSAM training course, and create an account in the CSAM. To determine if the CSAM has appropriate access management controls in place for unauthorized users, we obtained user entitlement data from the BEARS and a list of users from the CSAM. BEARS data had a list of 582 production users with authorization to access the CSAM as of January 25, 2023, and CSAM data had a list of 328 active users as of January 30, 2023. We compared CSAM active users to CSAM authorizations in the BEARS and determined that nine (3 percent) of 328 active CSAM users were not authorized in the BEARS.

Management Action: After we informed IRS management of our results, IRS CSAM system administrators approved one pending user request and asked the remaining eight users to initiate and process BEARS requests. We subsequently verified that a BEARS authorization was approved for the nine users.

Access management

Access management helps to protect the confidentiality, integrity, and availability of the services, data, and assets by ensuring that only authorized users are able to access or modify them. Access management implements the policies of information security management.

In FY 2023, TIGTA performed two audits on access management. We initiated an audit to evaluate whether the security controls over the Enterprise Case Management (ECM) system adequately protect its data against unauthorized access.[20] In December 2020, the IRS implemented the first release of the ECM system. The ECM system is designed to modernize and consolidate legacy case management systems, across the IRS, into an end-to-end enterprise solution in the cloud. The system processes and stores sensitive information, providing restricted access to IRS employees via the Internet.

We found that ECM user accounts were not deactivated or disabled timely. Specifically, 401 (44 percent) of 917 user accounts had not signed into the ECM system for at least 90 calendar days as of July 8, 2022. In addition, 315 (79 percent) of 401 user accounts were not deactivated or disabled as required. However, 53 (13 percent) of 401 accounts were deactivated in accordance with agency security policies and an additional 33 (8 percent) of 401 accounts were quarantined within the ECM system.[21]

IRS personnel stated that the ECM system quarantined or deactivated inactive accounts within the application after 120 calendar days in accordance with Internal Revenue Manual 10.8.1, *Information Technology Security, Policy and Guidance* (Sept. 2021). However, Internal Revenue Manual 10.8.24, *Information Technology Security, Cloud Computing Security Policy* (Sept. 2021), is more restrictive and requires accounts be deactivated after 90 calendar days of inactivity. Not restricting user access in a timely manner would allow unauthorized access to taxpayer data and privacy information.

Management Action: During our audit work, we reviewed IRS documentation that illustrated how the ECM program modified the code to deactivate user accounts after 90 calendar days of inactivity.

[20] TIGTA, Report No. 2023-20-018, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements* (Mar. 2023).

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

In our audit of the CSAM, we found that 308 (36 percent) of 863 active and inactive CSAM users had not logged onto the application for 366 to 1,205 calendar days. The users were not removed from the system as required by policy because removing the users would remove any audit logs associated with the accounts. We agreed that maintaining audit log traceability is preferable to account deletion and found that the IRS has mitigating controls in place by locking all 308 user accounts from accessing the CSAM. However, no risk-based decision was created for the exception to policy as required.

System environment security

Management of the information 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; and network monitoring and audit logs.

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 to reduce the exposure to 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 vulnerabilities. Users must be diligent to identify and take appropriate actions to address and minimize the chance of the vulnerabilities being exploited.

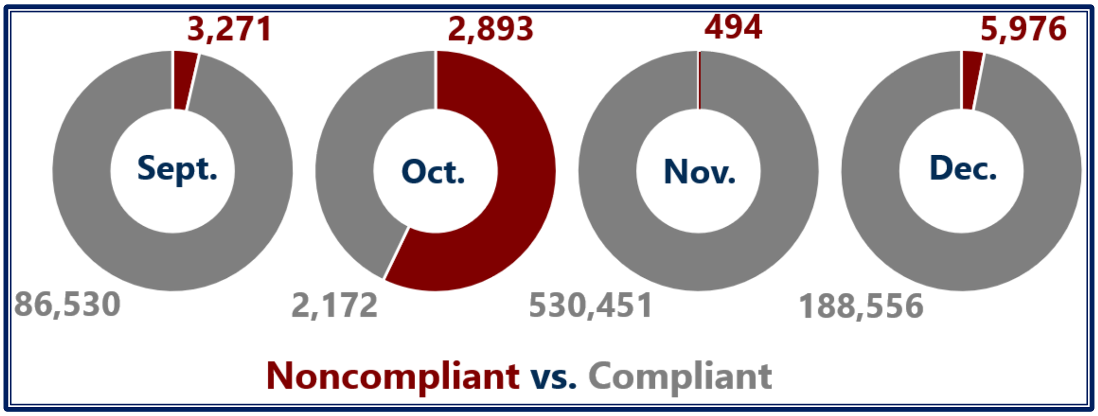
In FY 2023, TIGTA performed five audits involving system scanning and vulnerability patching of IRS systems. We initiated an audit to review the IRS's compliance with the Department of Homeland Security's Binding Operational Directive 22-01, *Reducing the Significant Risks of Known Exploited Vulnerabilities* (Nov. 2021), and whether known exploited vulnerabilities are effectively remediated as prescribed.[22] Binding Operational Directive 22-01 focuses on vulnerabilities that are active threats and should be Federal agencies' top priority. The Directive requires Federal agencies to update internal vulnerability management procedures by January 2022. In addition, the Directive states that if an agency is unable to timely remediate a known exploited vulnerability, the agency must remove or isolate the asset from the agency's network.

We found that known exploited vulnerability issues were communicated across the IRS via meetings held regularly, which allowed an opportunity for individuals to discuss relevant issues such as asset vulnerability status, remediation efforts impacting mission-critical assets, asset isolation, and the Virtual Local Area Network isolation pilot effort. In addition, the IRS reported past due unremediated known exploited vulnerabilities and mitigation actions to the Treasury Department by completing spreadsheets until the process was automated through the Continuous Diagnostics and Mitigation (CDM) Federal Dashboard.

[22] TIGTA, Report No. 2023-20-048, *Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk* (Aug. 2023).

Figure 10 shows that from September through December 2022, there were between 494 and 5,976 known exploited vulnerabilities past the remediation period.

Figure 10: Unremediated Known Exploited Vulnerabilities From September Through December 2022



Source: The IRS's asset and vulnerability repository reports from September through December 2022. Note: an asset may have one or more known exploited vulnerabilities.

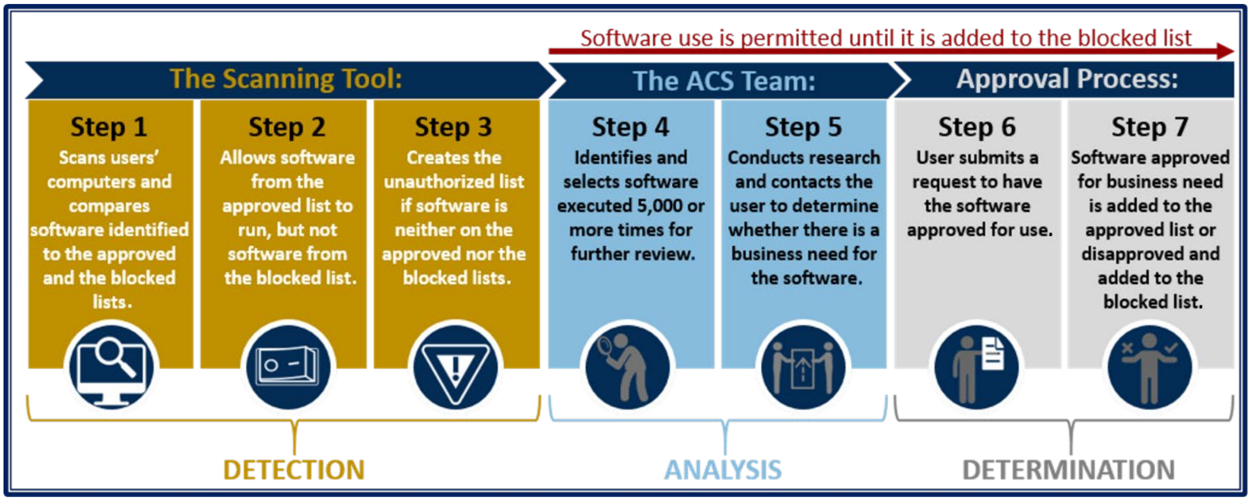
The repository reflected 91,559 assets with at least one known exploited vulnerability as of December 15, 2022. TIGTA was unable to determine the status of each asset with a known exploited vulnerability because the attack signature change data in the IRS's asset and vulnerability repository are not reliable.

We also initiated an audit to assess the efforts to manage hardware, software, information systems, and associated staff outside of the IT organization.[23] We found that the IRS has procedures to manage unauthorized software, but the methodology used to manage unauthorized software needs improvement. We analyzed a March 2022 unauthorized software list by applying the same criteria used by the Application Control Solution team to sample and review unauthorized software that have been executed equal to or more times than an established threshold. We determined that only 22 (1 percent) of 2,815 unauthorized software would have been reviewed and 2,793 (99 percent) of unauthorized software would not have been reviewed. We believe that software with low execution totals may pose a higher security risk because the software is less commonly known and used.

According to the *Application Control Solution Standard Operating Procedures* (Apr. 2021) and Application Control Solution team personnel, a scanning tool is run daily to monitor and check for software that is being executed on users' computers operating in the production domain. The software identified by the scanning tool is compared to lists of approved and blocked software. The scanning tool allows software from the approved list to run, but not software from the blocked list. If the software is on neither the approved list nor the blocked list, it is reported on the Summary of Application Actions by Win32 Executable report (hereafter referred to as the unauthorized list). Figure 11 provides the steps in the process from identifying software being executed on users' computers, to reviewing the software, to approving or disapproving use of the software.

[23] TIGTA, Report No. 2023-25-017, *Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement* (Apr. 2023).

Figure 11: Software Identification, Review, and Approval Process


Software use is permitted until it is added to the blocked list
The Scanning Tool:
The ACS Team:
Approval Process:
Step 1
Scans users' computers and compares software identified to the approved and the blocked lists.
Step 2
Allows software from the approved list to run, but not software from the blocked list.
Step 3
Creates the unauthorized list if software is neither on the approved nor the blocked lists.
Step 4
Identifies and selects software executed 5,000 or more times for further review.
Step 5
Conducts research and contacts the user to determine whether there is a business need for the software.
Step 6
User submits a request to have the software approved for use.
Step 7
Software approved for business need is added to the approved list or disapproved and added to the blocked list.
DETECTION
ANALYSIS
DETERMINATION

Source: TIGTA's analysis of the software identification, review, and approval process. ACS=Application Control Solution.

The time from initial contact with the user to determination of approval for software use can take up to 30 calendar days, during this time the user is permitted to continue using the software. If the software is deemed safe, it is approved and added to the Enterprise Standards Profile and the Common Operating Environment databases and the approved list. If the software is deemed unsafe, it is not approved and added to the blocked list. Allowing a user to continue using the software for up to 30 calendar days during the review and approval process and up to two weeks for the user to respond whether there is a business need unnecessarily increases the exposure of IRS information systems to potential malware and viruses.

In addition, we initiated an audit to evaluate the CDM Program progress to date for deployment of the BEARS and Privileged User Management Access System, and to determine if BEARS access and security controls align with Federal guidance.[24] In April 2016, the IRS developed a CDM Program Project Management Plan to align with the objectives of the Department of Homeland Security CDM Program that covers 15 continuous diagnostic capabilities to be delivered in three phases. Our review focused on Phase 2 of the Program, which supports business capabilities for identity and access management and privileged account management tools. The BEARS and the Privileged User Management Access System together comprise CDM Phase 2.

We reviewed the May 2022 vulnerability scan report for eight on-premises servers that support the BEARS and determined that there were 423 vulnerabilities:

- 348 (82 percent) critical (two unique) vulnerabilities that were timely remediated.
- 31 (7 percent) medium and high vulnerabilities that were timely remediated.
- 44 (10 percent) medium and high vulnerabilities that were not timely remediated:[25]
    - 5 high (one unique) vulnerabilities exceeded the IRS policy of 90 days for remediation.

[24] TIGTA, Report No. 2023-20-013, *The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed* (Mar. 2023).

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

- 39 medium (six unique) vulnerabilities exceeded the IRS policy of 120 days for remediation.

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 FY 2023, TIGTA and the GAO performed three audits of system configuration management controls. In our audit of the ECM system, we reviewed a July 2022 configuration compliance report for the ECM system and found that each of the four production servers were compliant based on having average weighted compliance scores above 90 percent with no failed high-risk configuration compliance checks.

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 to address recommendations from its prior years' reports related to internal control over financial reporting that remained open as of September 30, 2021.[26] The GAO reported that it found one deficiency in configuration management related to configuration settings. The IRS did not configure a database to meet a security configuration setting.

Network monitoring and audit logs

Audit and monitoring involve 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 FY 2023, TIGTA and the GAO performed seven audits involving network monitoring and audit logging. We initiated an audit to determine the effectiveness of controls to respond to and recover from malware (ransomware) attacks.[27] We found that one ransomware attack was mitigated by properly applying incident response procedures. [redacted]. The IRS identified website traffic patterns consistent with ransomware and removed the computer from the network. We compared the details of the incident response report against current policies and procedures and determined that the IRS took appropriate actions to resolve the incident. In

[26] GAO, GAO-23-106401, *MANAGEMENT REPORT: Improvements Needed in IRS's Financial Reporting and Information System Controls* (May 25, 2023).

[27] TIGTA, Report No. 2023-20-002, *Controls to Prevent and Recover From Ransomware Attacks Were Generally Effective* (Nov. 2022).

addition, the IRS stated there have been no successful ransomware attacks against the IRS prior to June 2022.

We also initiated an audit to determine whether the cyber threat hunting program is effectively monitoring, detecting, and addressing indicators of attack or compromise to the IRS network.[28] Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. These threats include unusual network traffic, unusual file changes, and the presence of malicious code. The objective of cyber threat hunting is to track and disrupt cyber adversaries as early as possible in the attack and to improve the speed and accuracy of organizational responses to protect the security and privacy of sensitive information.

The Advanced Threat Analysis team performs threat hunting for the IRS. We found that the team does not formally review and approve access to devices or programs previously restricted. The team's analyst conducts threat hunts on the IRS network based on internal and external information obtained from various sources. When an analyst concludes there is a risk to the IRS network from an outside domain, the analyst may submit a request to restrict access to the domain involved. Analysts restrict access to the IRS network through device or program blocks to stop possible malicious traffic, attack attempts, or any other intrusions. The blocks are placed on the server through an automated process once the analyst submits the request.

Guidance used by the analysts does not require management review and approval to add and remove device or program blocks (designed to restrict access to malicious sites) from a server.[29] By not having a formal or documented review process in place for removing device or program blocks from the server, the IRS risks an analyst accidentally removing a device or program block from a domain that still poses a threat to the IRS network, or intentionally removing a block to cause harm to the IRS network.

Management Action: During our audit work, we discussed the lack of a formal review and approval process for removing device or program blocks from the servers with IRS management. We expressed our concerns regarding the risk of a block being removed incorrectly. In response, IRS management developed and distributed a desk guide to the analysts that provides a workflow process to follow when creating or removing a device or program block request. We reviewed the steps in the desk guide and found they address the need to ensure that analysts fully investigate any proposed device or program block removal to ensure that no risk continues to exist. These steps include sharing and discussing the findings of the investigation with the other analysts on the team prior to executing the removal of the block. Despite these changes, there is still no requirement for management or senior analyst approval before removing the block.

In our audit of the EPACS, we found that audit logs are not being reviewed or monitored. The EPACS SSP states that the Cybersecurity function is responsible for the review and analysis of audit records.[30] The Audit Worksheet documents the auditable and actionable events needed to facilitate the review of IRS information technology applications. The Audit Worksheet is completed by the Cybersecurity function's Enterprise Security Audit Trails team in collaboration with the Access Control Management team. Once the Audit Worksheet is completed, the

[28] TIGTA, Report No. 2023-20-040, *The Cyber Threat Hunting Program Properly Conducts Analysis to Identify Threats; However, Guidance, Documentation, and Controls Need to Be Improved* (July 2023).

[29] IRS, *Desk Guide on Block and Unblock Process via the Content Filtering Recategorization Requests*.

[30] IRS, *IRS System Security Plan for Enterprise Physical Access Control System* (May 2022).

Cybersecurity function's Counter Insider Threat Operations team should begin reviewing and monitoring audit logs. According to Cybersecurity function personnel, they did not begin reviews of EPACS audit logs because the Audit Worksheet was not completed. Without regular reviewing and monitoring of the audit logs, inappropriate activities may not be identified in a timely manner.

Management Action: Access Control management provided an e-mail stating that as of March 2023, the Enterprise Security Audit Trails team is hosting weekly working sessions with the EPACS team to update the Audit Worksheet.

Disaster recovery

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

In FY 2023, TIGTA performed three audits involving disaster recovery. We initiated an audit to assess the effectiveness of software and data recovery processes after a service outage or disaster for systems that support mission essential functions.[31] To carry out its mission, the IRS relies on three mission essential functions: Processing Tax Remittances, Processing Tax Returns, and Processing Tax Refunds. Mission essential functions are a limited set of IRS functions that must be continued throughout, or rapidly resumed after, a service outage or disaster. These functions, which are supported by 50 information systems, enable the IRS to meet its mission and provide vital services to taxpayers.

We found the IRS equipped its enterprise computing centers with dual power supplies, which are now able to provide continuous operations during a service outage. As a result, the enterprise computing centers no longer require three planned power outages annually to test backup capabilities and perform electrical maintenance. In addition, a Supervisory Control and Data Acquisition system was installed to monitor and provide the capability to balance electrical power loads between the power sources. Enterprise Operations function management provided test reports completed in April 2021 after the implementation of the dual power supplies at the enterprise computing centers. Our review of the test reports determined that each of the 1,745 and 1,546 pieces of information technology equipment at the enterprise computing centers received a "passed" status and are equipped to provide dual power supplies.

We also found that while most systems' recovery time objectives (RTO) have been tested, several have recovery time actuals greater than the maximum tolerable downtime. To determine whether the IRS tested the RTO and met recovery time actual requirements, we reviewed the Application Information System Contingency Plan Testing Checklist and the Information System Contingency Plan Testing Observation Report completed during disaster recovery testing.

[31] TIGTA, Report No. 2023-20-023, *Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement* (May 2023).

- The Application Information System Contingency Plan Testing Checklist is used to validate the system's performance and reports the results of the disaster recovery testing.
- The Information System Contingency Plan Testing Observation Report includes additional disaster recovery testing information, such as scope, observations, and results.

During the disaster recovery testing for FISMA Year 2021 (*i.e.*, July 1, 2020, through June 30, 2021), we found that the IRS tested the RTOs for only 20 of 50 systems. The RTOs for the remaining 30 systems were not tested. Because the IRS tested less than 50 percent of the systems and was more than halfway through FISMA Year 2022, we gave the IRS an opportunity to complete the disaster recovery testing of the RTOs for the remaining 30 systems. Our review of the disaster recovery testing documents for FISMA Year 2022 found that the IRS tested the RTOs for 20 of 30 remaining systems. Collectively, the IRS tested the RTOs for 40 (80 percent) and did not test the RTOs for 10 (20 percent) systems during FISMA Years 2021 and 2022.

Of 40 systems' RTOs tested, our review further found that the recovery time actuals for 32 systems were less than 12 hours, meeting maximum tolerable downtime requirements for mission essential functions. However, the recovery time actuals for the remaining eight systems were greater than 12 hours, not meeting maximum tolerable downtime requirements for mission essential functions.

When the IRS does not test all systems for disaster recovery annually as required, it will be unable to assure system owners that their systems can be recovered within the RTOs. In addition, when the IRS is unable to recover its systems within 12 hours during disaster recovery testing, it will be unable to recover systems in a service outage or real disaster and meet its mission to provide taxpayers top-quality service.

Management Action: Cybersecurity function management stated that one system was not tested because they are in the process of removing it from the list of systems supporting mission essential functions because it is not on the IRS's network. Cybersecurity function management also stated that they have entered into a managed service agreement with a new replication vendor to provide disaster recovery environments for six of the nine systems which were not tested during FISMA Years 2021 and 2022 and have received assurances that these systems will be recoverable within the allowable RTOs. For the remaining three systems, they plan to move recovery capabilities to a virtualized environment. In addition, Cybersecurity function management provided documentation to support that the RTOs for six of the nine systems were tested in FISMA Year 2023 and met recovery time actual requirements.

In our audit of the Income Verification Express Service Program, we found that a root cause analysis of the transcript request inventory management system (*i.e.*, the Enterprise File Storage) outages took nearly six months to complete. The IRS originally identified the outages as primarily the result of a retransmission error (*i.e.*, the server fails to acknowledge a transmission and continuously resends the transmission, causing the network to overload and no longer respond). In response, the IRS opened a "priority one" ticket on March 24, 2022.[32] The ticket signified the critical nature of the ongoing outages that were significantly impacting the Income Verification Express Service Program, even though Enterprise File Storage outages predated the

[32] The IRS defines a priority one ticket as any issue causing a severe, mission-critical work stoppage. The impact may be on multiple internal or external customers and service to taxpayers. Immediate action is required (*i.e.*, the ticket should be resolved in four hours).

opening of this ticket. The ticket was closed on June 8, 2022; however, outages continued to occur with less frequency. In August 2022, we notified IRS management of our concern that a root cause analysis had not been completed and recommended that management postpone expanding Enterprise File Storage interfaces or adding workflows until the root cause of the outages had been identified and resolved by the IT organization.

Management Action: IRS management agreed, and a root cause analysis was performed to identify and address the reoccurrence of Enterprise File Storage outages. The root cause of Enterprise File Storage stability issues was identified and provided to the IRS on September 14, 2022, nearly six months after a "priority one" ticket was submitted.

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 FY 2023, TIGTA and the GAO performed eight audits involving security policies, procedures, and documentation. In our audit of the CSAM, we found that all on-premises FISMA reportable systems were tracked in the CSAM.[33] According to the CSAM Standard Operating Procedure, the CSAM team must perform a yearly reconciliation to ensure that the inventory within the CSAM aligns with the current stated FISMA boundaries as outlined in the FISMA Master Inventory. We obtained and reconciled a list of systems tracked by the CSAM and a list of FISMA reportable systems from the Treasury FISMA Inventory Management System as of January 26, 2023. The CSAM had 129 on-premises systems. We identified a discrepancy that was not identified during the last inventory validations performed by the CSAM team. The CSAM team determined that the system in question was accidently not categorized as a FISMA reportable system and provided evidence to show that the discrepancy was corrected.

In addition, we found that SSPs were not always updated to accurately reflect remedial information for controls with identified weaknesses. We selected five sampled systems from the 2023 FISMA annual security controls assessment and traced the control deficiencies from the 2023 FISMA annual assessment plans to the Security Assessment Report and then to the SSP.[34] We identified 32 controls in the SSPs that were not updated to reflect remedial information. The CSAM is used to reflect the status of controls with a real-time update to SSPs. Although the SSPs had the correct status of controls in four of five systems, all five systems were lacking Plans of Action and Milestones (POA&M) information on the deficiencies of the controls.

[33] We did not include an inventory review of cloud systems because the IRS was conducting a proof of concept on a sample of cloud systems.

[34] To test the accuracy and completeness of control assessment information and system security information in the CSAM, we selected a judgmental sample of five systems by leveraging the sample selection process from the FY 2023 FISMA evaluation. The five systems should cover security controls recommended for evaluation for year one, year two, and year three testing.

The IRS stated that the remedial actions are documented in the Treasury FISMA Inventory Management System for POA&Ms and a commercial off-the-shelf product for risk-based decisions. We determined that CSAM FISMA assessors do not have access to the inventory management system where the POA&Ms are tracked and maintained; therefore, the system stakeholders would need to update POA&M information in the SSPs. We also determined that POA&M information should be in the SSP as it documents plans to meet requirements for necessary controls not implemented. Without POA&M information being documented within the SSP, the SSP becomes a less effective tool to summarize the security requirements for the information system and describe the security controls in place or plans for meeting those requirements.

In our audit of hardware, software, and information systems, we found that the oversight of information systems managed by business units outside of the IT organization is not documented. We obtained a data extract of all active information systems in the IRS's current production environment from the As-Built Architecture as of April 2022. Our review of 620 active information systems determined that 517 (83 percent) systems are managed by the IT organization and 103 (17 percent) are managed by business units outside of the IT organization.[35] We requested that the IT organization provide documentation supporting its oversight (*e.g.*, executive steering committees, governance boards, stakeholders' meetings) for the 103 information systems. IT organization management provided documentation that supported oversight for eight (8 percent) of 103 information systems and was unable to provide evidence of any oversight for the remaining 95 (92 percent) systems. Without documented oversight of all information systems, the IRS is unable to demonstrate that it is complying with the Taxpayer First Act provision requiring the CIO to oversee the development, implementation, maintenance, and security as well as maintain operational control of information technology throughout the IRS.

System security training

System security training is a strategy used by information technology and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches. Effective security training helps employees understand proper cyber hygiene, the security risks associated with their actions, and to identify cyberattacks they may encounter via e-mail and the web.

In FY 2023, TIGTA and the GAO performed three audits involving system security training. We initiated an audit to assess the effectiveness of the implementation of new Federal requirements in the NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020) and follow up on prior TIGTA recommendations.[36] NIST, Special Publication 800-53 Revision 5, establishes controls for information systems and organizations. The implementation of its standards and guidelines is mandatory for all Federal systems. Federal agencies are given up to one year to implement the standards and guidelines from the date of their issuance. NIST, Special Publication 800-53 Revision 5, is designed to help organizations identify the security and privacy controls needed to manage risk and satisfy the

[35] The 103 information systems are listed in the As-Built Architecture as unique individual systems, but some systems may be a subsystem or the component of another system.

[36] TIGTA, Report No. 2023-20-034, *Actions Have Been Taken to Improve the Privacy Program; However, Some Privacy Controls Have Not Been Fully Implemented and Assessed* (June 2023).

security and privacy requirements of the FISMA. It is also designed for organizations to manage the privacy requirements of the Office of Management and Budget, the Federal Information Processing Standards, and the Privacy Act.[37]

We reviewed a FISMA Year 2022 year-end privacy awareness training compliance report of IRS contractors and found that 3,881 (21 percent) of 18,688 contractors have not taken the required annual privacy awareness training. Specifically, 2,365 contractors with network access and 1,516 contractors without network access did not take the privacy awareness training. We also found that 14,807 contractors have taken, are not required to take, or still have time to complete the privacy awareness training. Failure to ensure that contractor privacy awareness training is taken places the IRS at greater risk and could lead to potential mishandling or inadvertent disclosure of Personally Identifiable Information and taxpayer data.

We also initiated an audit to assess the IRS's compliance with the Federal Acquisition Regulation and IRS policies and procedures for awarding and administering expert witness contracts.[38] The IRS's Office of Chief Counsel provides legal guidance and interpretive advice to the IRS, the Treasury Department, and taxpayers. The Office of Chief Counsel also represents the IRS in litigation and can obtain the services of expert witnesses. The IRS Office of the Chief Procurement Officer processes all Office of Chief Counsel expert witness contracts under the requirements of the Federal Acquisition Regulation. We reviewed 27 expert witness contract files and found that required Security Awareness Training was not always completed and/or included in contract files.[39] The Office of Chief Counsel and/or Office of the Chief Procurement Officer were unable to provide evidence that the expert completed the required training for 19 (70 percent) of 27 contracts.

In its audit of safeguards for protecting taxpayer information, the GAO reported that in FY 2021, IRS employees met the agencywide completion goal of 97 percent for training on protecting taxpayer information.

Recently completed and ongoing TIGTA security reviews

Data security threats are a continuous concern of TIGTA. For FY 2024, TIGTA has recently completed or is performing several reviews related to data security threats, such as the system security problems identified in the data breach that led to the release of taxpayer information and subsequent prosecution and guilty plea of the accused, as well as other reviews that include:

- Implementation of the Next Generation Enterprise Security Audit Trails program to meet Federal and IRS requirements.[40]
- Security safeguards in place over the Compliance Data Warehouse to protect taxpayer data against unauthorized access.

[37] 5 U.S.C. § 552a (2018).

[38] TIGTA, *Report No. 2023-IE-R012, Federal Acquisition Regulation Requirements Were Either Not Performed or Documented When Awarding and Administering Expert Witness Contracts* (Sept. 2023).

[39] A contract file is a file that documents the basis for the acquisition and the award, the assignment of contract administration (including payment responsibilities), and any subsequent actions taken by the contracting office per Federal Acquisition Regulation 4.802(a).

[40] TIGTA, Report No. 2024-200-005, *The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement* (Oct. 2023).

- Controls in place to prevent the exfiltration of sensitive taxpayer data.
- Assessment of processes to grant access to sensitive systems and to safeguard Federal Tax Information.

Systems Development and Information Technology Operations

In carrying out its responsibilities for 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 human capital/program management, information technology acquisitions, project management, implementation of corrective actions, and updating and modernizing operations/information technology investments.[41]

Human capital/program management

Mission-critical skill gaps across the Federal workforce pose a high risk to the Nation because they impede the Government from cost-effectively serving the public and achieving results. Implementing effective information technology workforce planning practices can better position the IRS to address human capital risks. Accordingly, the GAO identified four key information technology workforce planning practices and supporting activities detailed in various laws enacted and guidance issued over the past 20 years that call for agencies to perform workforce planning activities.[42] These key practices include:

1. Setting the strategic direction for workforce planning.
2. Analyzing the workforce to identify skill gaps.
3. Developing strategies to address skill gaps.
4. Monitoring and reporting on progress in addressing skill gaps.

In FY 2023, TIGTA and the GAO performed three audits covering human capital/program management. In our audit of hardware, software, and information systems, we found that while the IT organization has procedures for hiring information technology staff outside of the IT organization, it does not have a process in place to ensure that inherently information technology-related work is not being performed. We selected for review all 20 staff requests submitted by business units outside of the IT organization for FYs 2021 and 2022 to determine whether they complied with the CIO Memorandum, CIO-09200-0001, *Procedure for Filling Information Technology (IT) Positions – Operating [(Business)] Units (OU) Outside of [the]*

[41] See Appendix III for a complete list of finding categories and associated reports, along with the number of reported findings.

[42] GAO, GAO-18-298, *INFORMATION TECHNOLOGY: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing* (June 28, 2018).

IT [organization] (Sept. 2020). We determined that the CIO approved all 20 staff requests. However, we were unable to determine whether inherently information technology-related work is not being performed by information technology staff outside of the IT organization because management was unable to clarify the inherently information technology-related work duties and responsibilities beyond the general information technology-related work cited in the CIO memorandum.

Specifically, the IT organization has not established the inherently information technology-related work performed by staff in the security administration, computer engineering, and information technology management job series that cannot be performed by staff outside of the IT organization. Without establishing the duties and responsibilities of information technology staff outside of the IT organization, there is an increased risk of inefficient use of resources from duplicating inherently information technology-related work and creating a duplicative IT organization.

We initiated an audit to review the effectiveness of the information technology POA&M process and to determine if it complies with required Federal and agency security policies.[43] Per the IRS's *Enterprise FISMA POA&M Standard Operating Procedures*, Version 10.1 (June 2020), business units are required to identify the resources needed and the source of the funding to resolve an information security weakness. The IRS finalized remediation efforts for 3,139 POA&Ms with total estimated costs of $134.5 million to resolve the information security weaknesses. However, during the closure process, the IRS did not reevaluate the estimated budget and update it with actual costs at closure for the 3,139 completed POA&Ms, as required.

Information technology acquisitions

The mission of the Office of the Chief Procurement Officer is to deliver top-quality acquisition services to ensure that the IRS can meet its mission of effective tax administration. Within the Office of the Chief Procurement Officer, the Office of Information Technology Acquisitions is primarily responsible for managing the procurement of information technology products and services and ensuring that the IRS acquires them for the best value, within budget, and in a timely manner. It is also responsible for ensuring that the information technology acquisition process is managed properly and efficiently, and is conducted with integrity, fairness, and openness. As stewards of taxpayer dollars, the IRS must ensure that it only pays for the procured products or services as authorized and delivered under contract.

In FY 2023, TIGTA performed an audit involving information technology acquisitions. In the hardware, software, and information systems audit, we found that not all information technology purchases were properly approved. The procurement process includes acquisition planning to research whether the procurement meets the IRS's needs by creating a "shopping cart" for the requested products, soliciting contractor proposals, evaluating the proposals, and awarding the contract as well as administering the contract. We reviewed the approval chains of all 17 shopping carts from 17 contracts for the purchase of information technology products initiated by business units outside of the IT organization. We determined that the appropriate IT organization management official properly approved seven (41 percent) shopping carts, totaling approximately $1 million. However, the remaining 10 (59 percent) shopping

[43] TIGTA, Report No. 2023-20-042, *Security Weaknesses Are Not Timely Resolved and Effectively Managed* (Aug. 2023).

carts, totaling approximately $1.2 million, were not properly approved. The appropriate IT organization management official (*e.g.*, Associate CIO, Deputy Associate CIO) authorized to approve the shopping cart is determined based upon the dollar value of the shopping cart and is listed in the Shopping Cart Signature Authority List. None of the individuals who approved the 10 shopping carts were on the signature authority list. As stewards of taxpayer dollars, the IRS must ensure that it only pays for procured information technology products as authorized.

Project management

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

In FY 2023, TIGTA provided coverage of information technology project management in six audits. In our audit of the EPACS, we evaluated the planning for the installation of the EPACS at IRS facilities by reviewing the process to select and prioritize the sites requiring installation and the tools used to guide the project from beginning to end. We obtained an EPACS project status report from July 2022, which contained 319 buildings requiring installation that included the location, security level designation, type of system install, or update needed, and project status. We found that the methodology used to select and prioritize IRS facilities for the EPACS installation was effective. In addition, the planning tool used to guide the installation project from planning to completion was working as intended.

We also initiated an audit to determine the effectiveness of the IRS's enterprise strategy and implementation of Zero Trust Architecture (ZTA) technical solutions which restrict network accesses to trusted users, assets, and resources.[44] In August 2020, the NIST issued ZTA guidance that provided direction for Federal agencies to migrate and deploy ZTA security concepts to an enterprise environment.[45] The ZTA is an end-to-end approach to enterprise resource and data security that encompasses identity, credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure and is based on the premise that trust is never granted implicitly but must be continually evaluated.

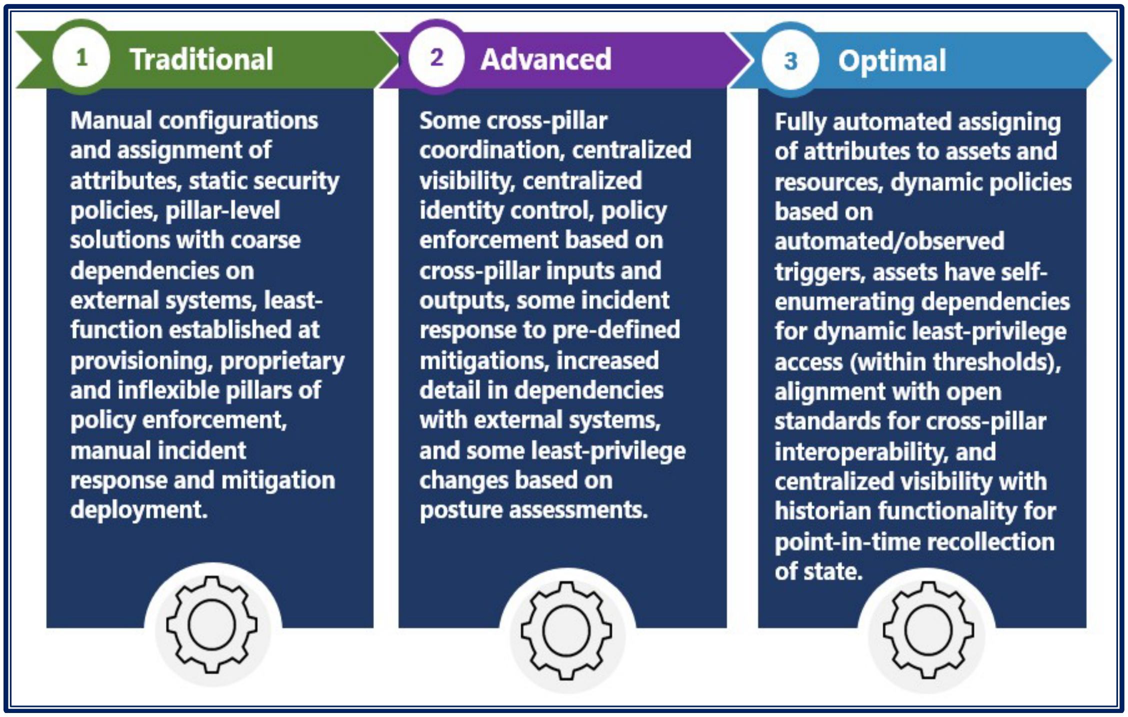
Executive Order 14028, *Improving the Nation's Cybersecurity* (May 2021), requires Federal agencies to advance a zero trust security model. In addition, the Office of Management and Budget Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 2022), established the milestones and criteria that agencies should follow to implement a ZTA. The memorandum described strategic goals that align with five pillars (*i.e.*, Identity, Devices, Networks, Applications and Workloads, and Data) of the draft Zero Trust Maturity Model that was developed by the Cybersecurity and Infrastructure Security Agency. The Cybersecurity and Infrastructure Security Agency drafted the Zero Trust Maturity Model to assist agencies in complying with the Executive Order. In addition to the five ZTA pillars, the draft maturity model provides three stages (*i.e.*, Traditional, Advanced, and Optimal) of maturity

[44] TIGTA, Report No. 2023-20-039, *Actions Are Needed to Improve the Zero Trust Architecture Implementation* (July 2023).

[45] NIST, Special Publication 800-207, *Zero Trust Architecture* (Aug. 2020).

to help agencies identify their maturity level for each pillar. Figure 12 describes the three stages of ZTA pillar maturity.

Figure 12: Zero Trust Stages of Maturity



1 Traditional

Manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response and mitigation deployment.

2 Advanced

Some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to pre-defined mitigations, increased detail in dependencies with external systems, and some least-privilege changes based on posture assessments.

3 Optimal

Fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, and centralized visibility with historian functionality for point-in-time recollection of state.

Source: Cybersecurity and Infrastructure Security Agency Cybersecurity Division Draft Zero Trust Maturity Model, June 2021.

In July 2021, the IRS conducted an internal assessment of its ZTA maturity. The IRS also contracted for an independent maturity assessment of its ZTA efforts that was completed in June 2022. We reviewed the contractor's assessment and compared it to the IRS's assessment of its ZTA implementation and found discrepancies. We determined that the IRS did not accurately assess its zero trust maturity. Specifically, 10 (53 percent) of 19 ZTA controls that were assessed by the contractor had a maturity level rating that differed from the IRS's internal maturity assessment. In March 2023, the contractor completed an assessment of the final two pillars (*i.e.*, Networks and Data); however, the audit team did not complete a comparison with the IRS's results due to the time frame of receiving the documentation. Without an accurate assessment of its ZTA maturity, the IRS may be unable to determine whether its enterprise is protected by appropriate ZTA controls.

In our audit of the Income Verification Express Service Program, we found that no single point of contact was responsible for resolving outages of the Enterprise File Storage, thus contributing to significant delays. For example, there were 72 reported Income Verification Express Service system incidents, which resulted in 292 hours of Enterprise File Storage outages between January 8 and September 10, 2022. At its peak, these outages resulted in transcript requests being worked within 502 hours (over 22 days) as opposed to the IRS's goal of 65 to 72 hours (three days).

Implementation of corrective actions

Internal controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are being achieved. Internal controls protect assets, detect errors, and prevent fraud. 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 TIGTA and GAO 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 FY 2023, TIGTA and the GAO performed 11 audits with coverage on the status of implementing corrective actions. In our audit of the EPACS, we found that the IRS addressed prior audit recommendations to ensure that a computer room is secured with a multifactor authentication card reader. In a prior audit, we found that an Integrated Submission and Remittance Processing domain controller was in an unlocked room with submission processing equipment.[46] The room was accessible by personnel who did not need access to the server. We recommended that the server be physically separated from the submission processing equipment and that computer rooms be made compliant with Federal multifactor authentication requirements. During our site visit to this location, we determined that the IRS implemented both recommendations. The server is secured in its own room and the door to the room is equipped with a Federally compliant multifactor card reader that is configured for two-factor authentication.

We initiated an audit to assess the IRS's efforts to meet the Secretary of the Treasury's expectations for the 2023 Filing Season.[47] The Secretary of the Treasury wants the IRS to firmly move into the digital age. Currently, IRS employees still manually transcribe millions of paper-filed tax returns. For the 2023 Filing Season, the IRS was tasked with the expectation to scan millions of these paper-filed tax returns into a digital copy, which would result in faster processing and faster refunds for taxpayers. The IRS did not achieve this expectation. As of April 30, 2023, the IRS reports scanning a total of 4,154 Forms 1040, of which 1,360 (33 percent) fell out to Error Resolution requiring IRS employee intervention to resolve errors.[48] IRS management indicated that scanning was going well and has continued to increase the number of paper-filed tax returns it scans. As of July 31, 2023, the IRS reports scanning 50,810 paper-filed individual tax forms and expanding to include 25 different attachments that can be included with the paper-filed Form 1040.

We also initiated an audit to assess the IRS's progress in transitioning to electronic records in accordance with Office of Management and Budget/National Archives and Records

[46] TIGTA, Report No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020).

[47] TIGTA, Report No. 2023-IE-R010, *Inflation Reduction Act: Assessment of the IRS's Efforts to Deliver Expected Improvements for the 2023 Filing Season* (Sept. 2023).

[48] IRS management indicated that returns falling out to Error Resolution is an incorporated process and that in some cases, business rules intentionally force some returns to Error Resolution.

Administration Memorandum M-19-21, *Transition to Electronic Records* (June 2019).[49] We previously identified problems with paper document processing and emphasized the need for the IRS to transition to electronic records in prior audit reports. Additionally, other stakeholders have recommended process improvements in attempts to move the agency forward in its digitalization efforts.

In FY 2009, we reported that the IRS uses a labor-intensive, costly, and error-prone system because it has been unable to implement a modernized submission processing system to convert paper tax returns into an electronic format. The IRS agreed to pursue implementing successful processes followed by States that use scanning technology (*e.g.*, Optical Character Recognition, two-dimensional bar codes) to convert paper-filed tax returns prepared by individuals (using a tax preparation software package) into an electronic format.[50] However, in Calendar Year 2015, the IRS determined that there was no longer a sound business case for it to convert paper returns to an electronic format using two-dimensional bar code scanning because paper return filing had decreased from 34 percent to 17 percent and the rate of e-filed tax returns had increased from 67 percent to 87 percent, significantly reducing the need for this technology.

Subsequently, in a FY 2018 report, the GAO reported that the IRS evaluated digitizing some paper returns using two-dimensional barcoding technology, but it had not updated that analysis or expanded it to consider other digitizing technologies.[51] In December 2019, IRS officials reported that the agency planned to begin scanning and digitizing individual tax returns filed on paper in October 2021. However, in August 2021, the IRS requested an additional year to complete the recommended action.

In a December 2021 recommendation to Congress, the National Taxpayer Advocate requested dedicated multiyear funding for the IRS to purchase and implement scanning technology to improve the speed and accuracy of paper return and correspondence processing. The National Taxpayer Advocate subsequently issued a Taxpayer Advocate Directive to the IRS on March 29, 2022, directing it to:[52]

- Work with tax return software companies to develop a plan for the companies to voluntarily place two-dimensional barcodes on returns prepared with their software products during the 2023 Filing Season and beyond.
- Develop a plan to implement Optical Character Recognition or similar technology to automate the processing of handwritten returns and returns without readable barcodes by the start of the 2023 Filing Season or, if not feasible, by the start of the 2024 Filing Season.

As we noted in our February 2022 report, the IRS had not taken any significant actions to review and assess needed equipment upgrades, replacement options, *etc.*, even though the Service

[49] TIGTA, Report No. 2023-10-050, *The IRS Has Experienced Challenges in Transitioning to Electronic Records* (Sept. 2023).

[50] TIGTA, Report No. 2009-40-130, *Repeated Efforts to Modernize Paper Tax Return Processing Have Been Unsuccessful; However, Actions Can Be Taken to Increase Electronic Filing and Reduce Processing Costs* (Sept. 2009).

[51] GAO, GAO-18-544*, TAX FRAUD AND NONCOMPLIANCE: IRS Could Further Leverage the Return Review Program to Strengthen Tax Enforcement* (July 24, 2018).

[52] The National Taxpayer Advocate has the delegated authority to issue a Taxpayer Advocate Directive to direct improvements to IRS operations or to grant relief to groups of taxpayers (or all taxpayers).

Center Automated Mail Processing System has limited technological capabilities and there were frequent requests for maintenance. We had previously notified management of our concerns about their inaction to develop a strategy to update or replace Service Center Automated Mail Processing System equipment. We also noted that since the start of the 2021 Filing Season, Service Center Automated Mail Processing System machines have been serviced almost 300 times.

In our audit of the implementation of the NIST requirements, we found that not all privacy controls have been fully implemented and assessed. We reported previously that the *IRS's Data Breach Response Plan* (May 2018) was not fully integrated with information security continuous monitoring. The IRS agreed that once NIST, Special Publication 800-53 Revision 5, was released, the IT organization's Cybersecurity function would integrate the privacy controls into the security assessments and continuous monitoring methodology. To assess the effectiveness of the implementation of the privacy controls, we selected a judgmental sample of 23 of 220 systems from the FISMA Master Inventory List for review. Of 23 systems selected for review, 15 systems are operating on-premises and eight systems are operating in the cloud. In addition, we identified 96 privacy controls from NIST, Special Publication 800-53 Revision 5, under the responsibility, solely or in part, of the Privacy, Governmental Liaison, and Disclosure Office.

On-premises systems

Our review of the privacy controls in the SSP for each of the 15 on-premises systems determined that 911 of 1,440 [96 controls x 15 systems] privacy controls are inherited controls. An inherited control is a control that is implemented at a shared common functionality level and has no system-level responsibility. We did not include inherited privacy controls in our review. Therefore, we reviewed 529 privacy controls.[53] Our review of the SSPs also determined that 388 (73 percent) of 529 privacy controls were not assessed, and only 141 (27 percent) of the privacy controls were assessed during FISMA Year 2022. Further analysis of the SSPs and assessment documentation for the 141 assessed privacy controls found that 95 privacy controls were implemented; 41 privacy controls were either not implemented, undefined, or missing; and five privacy controls were not applicable.

We discussed the results with Privacy, Governmental Liaison, and Disclosure Office personnel, and they stated that 17 privacy controls with a not implemented status and five privacy controls with a missing status should have been classified as inherited controls. Therefore, 22 of 41 privacy controls were misclassified in the SSPs and should have been identified as inherited controls. As a result, not all the privacy controls classified as inherited were correctly applied to all fields in the new assessment and monitoring system and captured in the SSP.

Cloud systems

TIGTA also found that the IRS did not implement and assess NIST, Special Publication 800-53 Revision 5, privacy controls for the eight cloud systems selected for review. This resulted in 768 [96 controls x eight systems] privacy controls that were not implemented and assessed. As a result, while this planned corrective action to integrate the privacy controls into the security

[53] Our review of privacy controls included hybrid controls, in which the control is part inherited and part operating at the system level. We reviewed only the portion of the privacy control at the system level.

assessments and continuous monitoring methodology was fully implemented, the corrective actions taken were not effective.

Failure to fully implement and assess privacy controls exposes Personally Identifiable Information and tax information on the IRS's on-premises and cloud systems to potential unauthorized access, use, disclosure, disruption, modification, and destruction. In addition, incomplete and inaccurate reporting of privacy control assessments and the status of control implementation may result in unreliable information, which can lead to unidentified weaknesses that are not addressed.

Updating and modernizing operations/information technology investments

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 FY 2023, TIGTA and the GAO performed nine audits covering modernization. In our audit of the CDM Program, we found that the IRS completed the first phase of the CDM Program in April 2020. The CDM Phase 1 entailed installing sensor tools to identify authorized hardware and software assets and ensure that they are properly configured with vulnerabilities mitigated. We evaluated the CDM Program's progress by reviewing documented accomplishments, milestones, lessons learned, and program status updates.

We also initiated an audit to assess the IRS's compliance with § 10301(1)(B) of the Inflation Reduction Act, which required the development of a task force to design a free, IRS-run, direct electronic tax return filing system.[54] Inflation Reduction Act § 10301(1)(B) included an appropriation of $15 million, to remain available until September 2023, to establish a task force to design an IRS-run, free direct electronic filing tax return system, referred to as "Direct File." In addition, § 10301(1)(B) required the task force to deliver a report to Congress within nine months following the date of enactment, to include, for instance, the cost of developing and running a free direct e-file tax return system, including costs to build and administer each release, with a focus on multilingual and mobile-friendly features and safeguards for taxpayer data.

The Direct File Report to Congress included the IRS's estimates, both for a narrow and broad scope of the project and was based upon 5 million taxpayers using the tool. However, we found that direct file cost estimates could not be substantiated. The IRS could not provide any supporting documentation to support its cost estimates or how it determined there would be at least 5 million users. As a result, we had no way to identify the reasonableness of the IRS's cost estimates.

The GAO initiated an audit to describe the IRS's legacy information technology systems environment and its efforts to identify associated costs; determine to what extent the IRS has defined its plans, including cost, schedule, and benefits for modernizing or replacing and retiring its legacy information technology systems; and determine to what extent the IRS's current efforts and plans to move to cloud services are consistent with Office of Management and

[54] TIGTA, Audit No. 2024-408-002, *Inflation Reduction Act: Assessment of a Free and Electronic Direct Filing Tax Return System* (Oct. 2023).

Budget guidance.[55] The GAO reported that key elements of the IRS's modernization planning were either missing or no longer valid. Three key elements increase the likelihood that modernization initiatives will succeed. These elements are milestones to complete the modernization, a description of the work necessary to modernize the legacy system, and details regarding the disposition of the legacy system.

As of August 2022, the IRS had 21 information technology initiatives in its modernization portfolio. The agency documented plans for each of the 21 initiatives, which addressed two of the three key elements (milestones and descriptions of the work to be completed). Of the nine plans for the initiatives associated with legacy systems, three plans included details regarding the disposition of a legacy system. Six of the plans did not address this element. IRS officials stated that this element would be addressed for each of the six initiatives at a later point in their life cycle. However, the officials did not provide time frames for when this would occur. Without establishing time frames for addressing the disposition of legacy systems, the IRS lacks accountability for completing this key element. For the remaining 12 plans, the third element was not applicable because, according to officials, there was no corresponding legacy system to be retired.

In addition, IRS officials added that the schedules for suspended initiatives were now undetermined. The suspension of Customer Account Data Engine 2 Target State and Individual Master File Retirement Acceleration considered essential to replacing the 60-year-old Individual Master File is concerning. The Individual Master File is IRS's authoritative data source for individual tax account data. As the GAO reported last year, the IRS has been working for well over a decade to replace the Individual Master File. However, the IRS has revised the program's cost, schedule, and scope goals on numerous occasions, including seven times between 2016 and 2019. Given these continuing delays, the IRS announced last year that the Individual Master File would not be fully replaced until 2030. However, that date no longer applies due to the suspensions; it is now unknown when the Individual Master File will be replaced. Accordingly, the IRS will face mounting challenges in continuing to rely on a system that has software written in an archaic language requiring specialized skills that are increasingly difficult to find.

[55] GAO, GAO-23-104719, *INFORMATION TECHNOLOGY: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements* (Jan. 12, 2023).

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit 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 levels 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 FY 2023. We also analyzed and prepared summaries of the reported issues.
- Identified and summarized other relevant TIGTA and external oversight assessments addressing information technology security, systems development, and operations.

Performance of This Review

The compilation of the information for this report was performed at various TIGTA offices during the period of July through November 2023. The information presented was derived from TIGTA and GAO reports issued during FY 2023 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; Jason Rosenberg, Acting Audit Manager; Carreen Díaz, Lead Auditor; and Cezary Dyrda, 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 FY 2023. 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 (in month issuance order)

1. GAO, GAO-23-105564, *FINANCIAL AUDIT: IRS's FY 2022 and FY 2021 Financial Statements* (Nov. 10, 2022).
2. TIGTA, Report No. 2023-20-002, *Controls to Prevent and Recover From Ransomware Attacks Were Generally Effective* (Nov. 2022).
3. TIGTA, Report No. 2023-IE-R002, *National Research Program Tax Return Selection Process for Tax Years 2017 and 2019* (Nov. 2022).
4. GAO, GAO-23-104719, *INFORMATION TECHNOLOGY: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements* (Jan. 12, 2023).
5. TIGTA, Report No. 2023-15-022, *Significant Progress Has Been Made Implementing the Taxpayer First Act* (Mar. 2023).
6. TIGTA, Report No. 2023-20-013, *The IRS Implemented the Business Entitlement Access Request System; However, Improvements Are Needed* (Mar. 2023).
7. TIGTA, Report No. 2023-20-018, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements* (Mar. 2023).
8. TIGTA, Report No. 2023-40-021, *Results of the 2022 Filing Season* (Mar. 2023).
9. TIGTA, Report No. 2023-45-014, *Additional Actions Are Needed to Improve and Secure the Income Verification Express Service Program* (Mar. 2023).
10. TIGTA, Report No. 2023-25-017, *Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement* (Apr. 2023).
11. GAO, GAO-23-106401, *MANAGEMENT REPORT: Improvements Needed in IRS's Financial Reporting and Information System Controls* (May 25, 2023).
12. TIGTA, Report No. 2023-20-023, *Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement* (May 2023).
13. GAO, GAO-23-106080, *CYBERCRIME: Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics* (June 20, 2023).
14. TIGTA, Report No. 2023-20-034, *Actions Have Been Taken to Improve the Privacy Program; However, Some Privacy Controls Have Not Been Fully Implemented and Assessed* (June 2023).
15. TIGTA, Report No. 2023-47-036, *American Rescue Plan Act: Continued Review of Premium Tax Credit Provisions* (June 2023).
16. GAO, GAO-23-106470, *IRS Priority Open Recommendations* (July 31, 2023).
17. TIGTA, Report No. 2023-20-039, *Actions Are Needed to Improve the Zero Trust Architecture Implementation* (July 2023).

18. TIGTA, Report No. 2023-20-040, *The Cyber Threat Hunting Program Properly Conducts Analysis to Identify Threats; However, Guidance, Documentation, and Controls Need to Be Improved* (July 2023).
19. GAO, GAO-23-105395, *SECURITY OF TAXPAYER INFORMATION: IRS Needs to Address Critical Safeguard Weaknesses* (Aug. 14, 2023).
20. TIGTA, Report No. 2023-20-041, *Fiscal Year 2023 IRS Federal Information Security Modernization Act Evaluation* (Aug. 2023).
21. TIGTA, Report No. 2023-20-042, *Security Weaknesses Are Not Timely Resolved and Effectively Managed* (Aug. 2023).
22. TIGTA, Report No. 2023-20-048, *Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk* (Aug. 2023).
23. TIGTA, Report No. 2023-40-044, *Indicators Used to Prevent Filing of Tax Returns for Deceased Taxpayers Were Incorrectly Placed on Some Taxpayer Accounts* (Aug. 2023).
24. TIGTA, Report No. 2023-10-050, *The IRS Has Experienced Challenges in Transitioning to Electronic Records* (Sept. 2023).
25. TIGTA, Report No. 2023-20-062, *The Enterprise Physical Access Control System Implementation and Physical Security Controls Need Improvement* (Sept. 2023).
26. TIGTA, Report No. 2023-20-064, *Actions Need to Be Taken to Improve the Cyber Security Assessment and Management Application Security Controls* (Sept. 2023).
27. TIGTA, Report No. 2023-2S-069, *The IRS Implemented Processes to Prevent Future Unauthorized Disclosures of Form 990-T Information* (Sept. 2023).
28. TIGTA, Report No. 2023-2S-070, *Key Events of the IRS's Planning Efforts to Implement Login.gov for Taxpayer Identity Verification* (Sept. 2023).
29. TIGTA, Report No. 2023-IE-R010, *Inflation Reduction Act: Assessment of the IRS's Efforts to Deliver Expected Improvements for the 2023 Filing Season* (Sept. 2023).
30. TIGTA, Report No. 2023-IE-R012, *Federal Acquisition Regulation Requirements Were Either Not Performed or Documented When Awarding and Administering Expert Witness Contracts* (Sept. 2023).
31. TIGTA, Report No. 2024-408-002, *Inflation Reduction Act: Assessment of a Free and Electronic Direct Filing Tax Return System* (Oct. 2023).[1]

[1] This report was issued in FY 2024; however, all audit work was conducted during FYs 2022 through 2023.

Appendix III

List of Finding Categories and Associated Treasury Inspector General for Tax Administration and Government Accountability Office Reports (with number of reported positive and negative findings)

Finding Category and Associated Reports[1]	Number of Reported Findings	
	Positive	Negative
Access Management	**0**	**3**
TIGTA, Report No. 2023-20-018*	0	2
TIGTA, Report No. 2023-20-064*	0	1
Authentication and Identity Proofing	**0**	**1**
TIGTA, Report No. 2023-2S-070*	0	1
Authorization	**1**	**2**
TIGTA, Report No. 2023-20-013	1	0
TIGTA, Report No. 2023-20-062*	0	1
TIGTA, Report No. 2023-20-064*	0	1
Disaster Recovery	**1**	**7**
TIGTA, Report No. 2023-20-002	0	2
TIGTA, Report No. 2023-20-023*	1	4
TIGTA, Report No. 2023-45-014*	0	1
Human Capital/Program Management	**0**	**6**
GAO, GAO-23-106080	0	3
TIGTA, Report No. 2023-20-042*	0	1
TIGTA, Report No. 2023-25-017*	0	2
Implementation of Corrective Actions	**2**	**22**
GAO, GAO-23-105395	0	2
GAO, GAO-23-105564	0	1
GAO, GAO-23-106401	0	1
GAO, GAO-23-106470	0	1
TIGTA, Report No. 2023-10-050*	0	1
TIGTA, Report No. 2023-15-022	0	8
TIGTA, Report No. 2023-20-013	1	0
TIGTA, Report No. 2023-20-034*	0	6
TIGTA, Report No. 2023-20-062*	1	0
TIGTA, Report No. 2023-40-021	0	1
TIGTA, Report No. 2023-IE-R010*	0	1

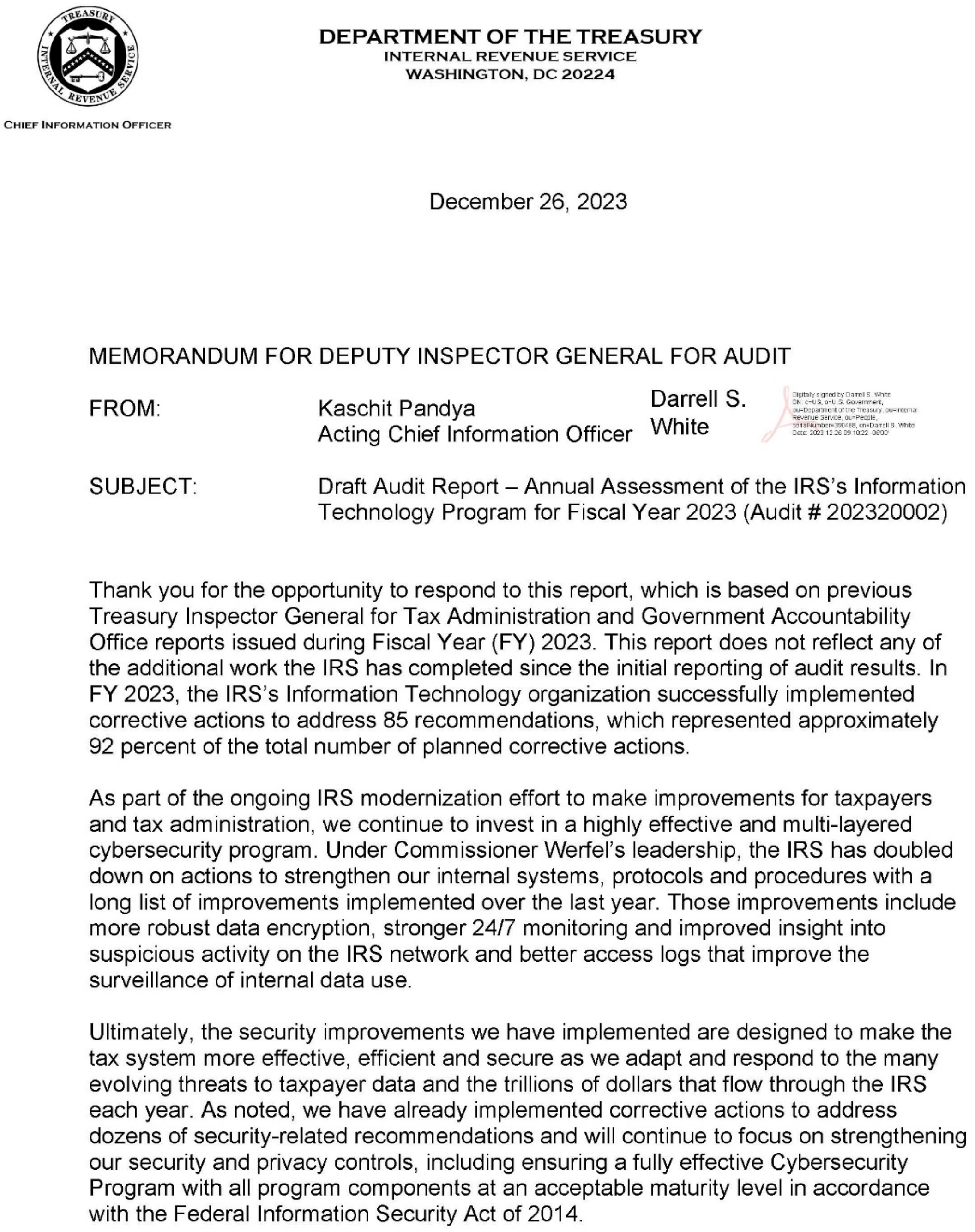
[1] Asterisk (*) indicates finding(s) were discussed in the finding category within the body of this report.

Information Technology Acquisitions	**0**	**1**
TIGTA, Report No. 2023-25-017*	0	1
Network Monitoring and Audit Logs	**2**	**7**
GAO, GAO-23-105395	0	1
GAO, GAO-23-106401	0	1
TIGTA, Report No. 2023-20-002*	1	0
TIGTA, Report No. 2023-20-040*	1	1
TIGTA, Report No. 2023-20-062*	0	1
TIGTA, Report No. 2023-20-064	0	2
TIGTA, Report No. 2023-2S-070	0	1
Overall Assessment of the Information Security Program	**0**	**1**
TIGTA, Report No. 2023-20-041*	0	1
Physical Security Access Controls	**0**	**5**
TIGTA, Report No. 2023-20-062*	0	5
Privacy of Taxpayer Data	**5**	**8**
GAO, GAO-23-105395*	2	7
TIGTA, Report No. 2023-45-014*	0	1
TIGTA, Report No. 2023-2S-069	2	0
TIGTA, Report No. 2023-IE-R002*	1	0
Project Management	**3**	**7**
TIGTA, Report No. 2023-10-050	0	2
TIGTA, Report No. 2023-20-013	1	0
TIGTA, Report No. 2023-20-018	1	0
TIGTA, Report No. 2023-20-039*	0	2
TIGTA, Report No. 2023-20-062*	1	0
TIGTA, Report No. 2023-45-014*	0	3
Security Policies, Procedures, and Documentation	**3**	**9**
GAO, GAO-23-105395	0	1
TIGTA, Report No. 2023-20-002	2	0
TIGTA, Report No. 2023-20-023	0	1
TIGTA, Report No. 2023-20-040	0	2
TIGTA, Report No. 2023-20-048	0	1
TIGTA, Report No. 2023-20-062	0	1
TIGTA, Report No. 2023-20-064*	1	1
TIGTA, Report No. 2023-25-017*	0	2
System Configuration Management	**2**	**1**
GAO, GAO-23-106401*	0	1
TIGTA, Report No. 2023-20-013	1	0
TIGTA, Report No. 2023-20-018*	1	0

System Scanning, Vulnerability Remediation, and Patching	**1**	**15**
TIGTA, Report No. 2023-20-013*	0	3
TIGTA, Report No. 2023-20-018	0	4
TIGTA, Report No. 2023-20-042	0	3
TIGTA, Report No. 2023-20-048*	1	4
TIGTA, Report No. 2023-25-017*	0	1
System Security Training	**1**	**3**
GAO, GAO-23-105395*	1	1
TIGTA, Report No. 2023-20-034*	0	1
TIGTA, Report No. 2023-IE-R012*	0	1
Updating and Modernizing Operations/Information Technology Investments	**9**	**18**
GAO, GAO-23-104719*	1	2
TIGTA, Report No. 2023-10-050	0	5
TIGTA, Report No. 2023-20-013*	1	0
TIGTA, Report No. 2023-40-021	1	4
TIGTA, Report No. 2023-40-044	0	2
TIGTA, Report No. 2023-47-036	1	1
TIGTA, Report No. 2024-408-002*	2	4
TIGTA, Report No. 2023-IE-R002	2	0
TIGTA, Report No. 2023-IE-R010	1	0
Total Number of Findings	**30**	**116**

Appendix IV

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

December 26, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Acting Chief Information Officer

Darrell S. White

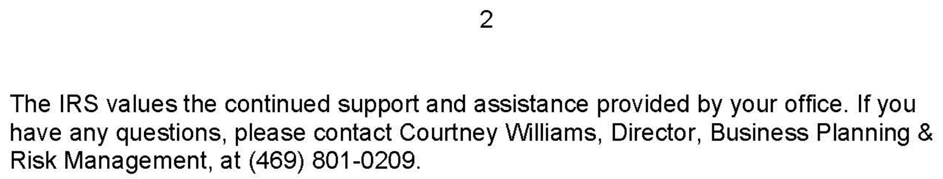
Digitally signed by Darrell S. White
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Internal Revenue Service, ou=People, serialNumber=390468, cn=Darrell S. White
Date: 2023.12.26 09:10:22 -06'00'

SUBJECT: Draft Audit Report – Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2023 (Audit # 202320002)

Thank you for the opportunity to respond to this report, which is based on previous Treasury Inspector General for Tax Administration and Government Accountability Office reports issued during Fiscal Year (FY) 2023. This report does not reflect any of the additional work the IRS has completed since the initial reporting of audit results. In FY 2023, the IRS's Information Technology organization successfully implemented corrective actions to address 85 recommendations, which represented approximately 92 percent of the total number of planned corrective actions.

As part of the ongoing IRS modernization effort to make improvements for taxpayers and tax administration, we continue to invest in a highly effective and multi-layered cybersecurity program. Under Commissioner Werfel's leadership, the IRS has doubled down on actions to strengthen our internal systems, protocols and procedures with a long list of improvements implemented over the last year. Those improvements include more robust data encryption, stronger 24/7 monitoring and improved insight into suspicious activity on the IRS network and better access logs that improve the surveillance of internal data use.

Ultimately, the security improvements we have implemented are designed to make the tax system more effective, efficient and secure as we adapt and respond to the many evolving threats to taxpayer data and the trillions of dollars that flow through the IRS each year. As noted, we have already implemented corrective actions to address dozens of security-related recommendations and will continue to focus on strengthening our security and privacy controls, including ensuring a fully effective Cybersecurity Program with all program components at an acceptable maturity level in accordance with the Federal Information Security Act of 2014.



2

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact Courtney Williams, Director, Business Planning & Risk Management, at (469) 801-0209.

Appendix V

Glossary of Terms

Term	Definition
Application	A software program hosted by an information system.
Appropriation	Statutory authority to incur obligations and make payments out of Treasury Department funds for specified purposes.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Baseline	A benchmark that includes project costs, schedule, and scope against which project performance is measured.
Binding Operational Directive	A compulsory direction issued to Federal Executive Branch agencies for the purposes of safeguarding Federal information/information systems.
Business Process	A set of structured activities or tasks that, once completed, will accomplish specific organizational goals.
Business Unit	A title for major IRS organizations, such as the IRS Independent Office of Appeals, the Office of Professional Responsibility, and the IT organization.
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.
Cloud	The use of computing resources, (*e.g.*, hardware and software), which are delivered as a service over a network (typically the Internet).
Cloud Computing	Model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (*e.g.*, network, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Common Operating Environment Database	A standardized, configured computer image on IRS computers integrated with a set of standard software to support the needs of all IRS employees.
Continuous Diagnostics and Mitigation Federal Dashboard	A means to view customized reports that alerts security personnel to critical cyber risks and vulnerabilities.
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
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.

Term	Definition
Disaster Recovery Testing	Full-scale functional exercise that involves recovering the information system and/or application on nonproduction equipment, in a simulated environment, or at the recovery location.
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.
Domain Controller	A server that is running a version of the operating system and has Active Directory Domain Services installed.
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.
Entitlement	Rights granted to the user of licensed software that are defined within the license agreement.
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.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Firmware	Computer programs and data stored in hardware – typically in read-only memory or programmable read-only memory – such that the programs and data cannot be dynamically written or modified during execution of the programs.
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.
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.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of information or a system. In addition, an incident could constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Information System Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.
Information Technology	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency.

Term	Definition
Information Technology Organization	The IRS organization 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.
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.
Legacy System	An information system that may be based on outdated technologies but is critical to day-to-day operations.
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.
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.
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.
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.
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.
On-Premises	Servers hosted on a network or within a company infrastructure (*e.g.*, remote servers hosted in data centers) that are controlled, administered, and maintained by the organization.
Patch	A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.

Term	Definition
Personally Identifiable Information	Information that, either alone or in combination with other information, can be used to uniquely identify an individual. Some examples of Personally Identifiable Information are: name, Social Security Number, date of birth, place of birth, address, and biometric record.
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.
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.
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.
Risk-Based Decision	A decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analyses, assessments, and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase, and a decision is made taking the entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis assessments, recommended risk mitigation strategies, and business impact.
Secure Access Digital Identity	Uses authentication when an individual attempting to access a protected resource has control of the specified authenticators/credentials. It is a major system that delivers a modern digital identity technology platform and capabilities to protect IRS public-facing applications.
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.
Shopping Cart	Used to request external goods and services and to secure the necessary approval and funding for those goods and services prior to the request being submitted.
Supervisory Control and Data Acquisition	A computer-based system for gathering and analyzing real-time data to monitor and control equipment that deals with critical and time-sensitive materials or events. It was first used in the 1960s and is now an integral component in virtually all industrial plant and production facilities.

Term	Definition
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 Year	The 12-month accounting period for which tax is calculated. For most individual taxpayers, the tax year is synonymous with the calendar year.
Treasury FISMA Inventory Management System	The data maintained in this repository are used as part of the Treasury Department's efforts to comply with the E-Government Act of 2002 as well as NIST and Office of Management and Budget regulations and guidance.
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.
Virtual Local Area Network	Collection of devices that are partitioned in a group in which group members can be nearby (*e.g.*, in the same building) or in widely dispersed geographic locations. The devices deliver data protection and security to enable confident connectivity and sharing between critical resources.

Appendix VI

Abbreviations

BEARS	Business Entitlement Access Request System
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CSAM	Cyber Security Assessment and Management Application
ECM	Enterprise Case Management
EPACS	Enterprise Physical Access Control System
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
RTO	Recovery Time Objective
SSP	System Security Plan
TIGTA	Treasury Inspector General for Tax Administration
ZTA	Zero Trust Architecture

To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at
oi.govreports@tigta.treas.gov.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

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