

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Annual Assessment of the IRS's Information Technology Program for Fiscal Year 2024

June 23, 2025

Report Number: 2025-2S0-007

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Why TIGTA Did This Review

The IRS Restructuring and Reform Act of 1998 requires us to annually assess and report on IRS information technology. This audit was initiated to assess the adequacy and security of the IRS's information technology based on 24 audit reports issued by us (19) and the Government Accountability Office (5) during Fiscal Year 2024.

Impact on Tax Administration

In Fiscal Year 2024, the IRS collected approximately \$5.1 trillion in federal tax payments and processed 267 million tax returns and forms. In addition, IRS federal tax refund and outlay activities were approximately \$553 billion.

The IRS employs more than 90,000 people in its Washington, D.C. Headquarters and more than 470 offices in all 50 states and U.S. Territories. IRS employees are engaged in a wide array of tax administration functions, from taxpayer service to enforcement of federal tax laws. However, staffing levels and the number of offices may change due to the implementation of Executive Orders and other directives.

The IRS relies extensively on computerized systems to support its financial and mission-related operations. Weaknesses within the IRS's computer operations could 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 the Direct File pilot sufficiently assessed and implemented assurance levels for identity proofing, authentication, and federation. In addition, the IRS is blocking more than 1,000 email websites and effectively preventing users from using email website services to exfiltrate sensitive taxpayer data. While the IRS has made progress in its modernization efforts and is adhering to its strategic goals, these efforts are being reassessed with the elimination of the Transformation and Strategy Office.

The Fiscal Year 2024 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. Effective is defined as being at or above maturity level 4, *Managed and Measurable*. Maturity levels range from level 1 for *Ad Hoc* to level 5 for *Optimized*. The IRS needs to take steps to improve its security program deficiencies and fully implement all security program components in compliance with federal requirements.

Problems were also reported in the IRS's handling of the privacy of taxpayer data, access controls, system environment security, roles and responsibilities and separation of duties, security policies, procedures, and documentation. For example, in a previous report, we found that the IRS is not removing user access to taxpayer information once users have separated from the IRS. Specifically, 279 of 91,661 users with sensitive system access were listed as separated but continued to have access to 1 or more sensitive systems. IRS applications with Personally Identifiable Information or Federal Tax Information are not always sending audit trails to the repository as required.

The IRS was unable to locate all cloud services contracts for its cloud applications. The value of all cloud services contracts was also indeterminable. Furthermore, the Cloud Management Office did not provide centralized management and oversight of the Enterprise Cloud Program. The IRS fully implemented some planned corrective actions, but the actions were not always effective.

Because the assessment of IRS information technology in this report was based on Fiscal Year 2024 audit reports, we did not make any further recommendations.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

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

June 23, 2025

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Acting Deputy Inspector General for Audit

SUBJECT: Final Report – Annual Assessment of the IRS’s Information Technology Program for Fiscal Year 2024 (Review No.: 20242S0002)

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 was part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenges of *Information Technology Modernization; Managing IRA [Inflation Reduction Act of 2022] Transformation Efforts; Protection of Taxpayer Data and IRS Resources; Tax Fraud and Improper Payments; and Tax Law Changes.*²

If you have any questions, please contact me or Linna Hung, Acting 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.).

² Pub. L. No. 117-169, 136 Stat. 1818.

Background

The Internal Revenue Service (IRS) Restructuring and Reform Act of 1998 requires TIGTA to annually assess and report on the adequacy and security of the IRS's information technology.¹ TIGTA's Security and Information Technology Services business unit assesses the IRS's information technology by evaluating cybersecurity, systems development, and information technology operations. This report provides our Fiscal Year (FY) 2024 assessment based on audit reports issued by us and the Government Accountability Office (GAO).

The IRS collects taxes, processes tax returns, provides taxpayer services, and enforces federal tax laws. In FY 2024, the IRS collected approximately \$5.1 trillion in federal tax payments and processed 267 million tax returns and forms. In addition, IRS federal tax refund and outlay activities were approximately \$553 billion.² This was a decrease of 16 percent compared to FY 2023.

In FY 2024, the IRS collected approximately \$5.1 trillion in federal tax payments and paid approximately \$553 billion in refund and outlay activities.

The size and complexity of the IRS add unique operational challenges. The IRS employs more than 90,000 people in its Washington, D.C. Headquarters and more than 470 offices in all 50 states and U.S. Territories. 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 operations to collect taxes, process tax returns, provide taxpayer services, 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. However, staffing levels and the number of offices may change due to the implementation of Executive Orders and other directives.

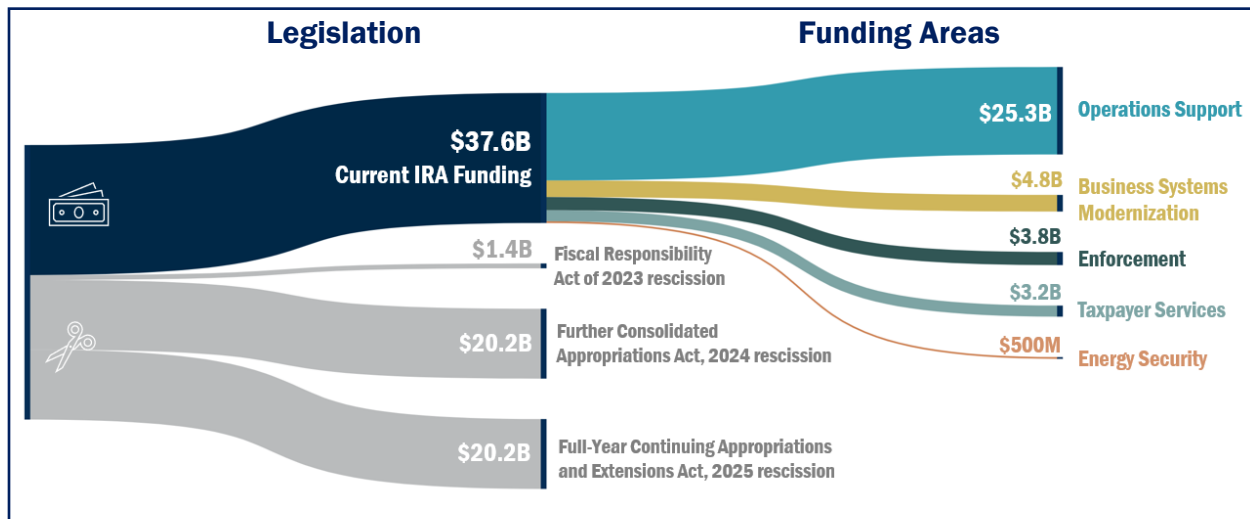
New legislation and guidance affecting modernization

The IRS initially received \$79.4 billion from the Inflation Reduction Act (IRA). However, as of March 2025, Congress subsequently reduced IRA funding to \$37.6 billion.³ IRA funding is designated in the areas of operations support, enforcement, business systems modernization, taxpayer services, and energy security. The Transformation and Strategy Office oversees the IRA modernization efforts of the IRS. However, these modernization efforts are being reassessed since the Transformation and Strategy Office began standing down in March 2025. Figure 1 provides the current IRA funding by area.

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 II 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 The Fiscal Responsibility Act of 2023 (Pub. L. No. 118-5, 137 Stat. 10) rescinded \$1.4 billion; the Further Consolidated Appropriations Act, 2024 (Pub. L. No. 118-47, 138 Stat. 460) rescinded \$20.2 billion; and the Full-Year Continuing Appropriations and Extensions Act, 2025 (Pub. L. No. 119-4) rescinded another \$20.2 billion.

Figure 1: Legislation and IRA Funding by Area

Source: Analysis of related legislation affecting funding areas.

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 and other information technologies to improve customer service; the funding is not to be used for operations and maintenance of legacy systems.

In April 2023, the Department of the Treasury (Treasury Department) and the IRS developed the *Internal Revenue Service Inflation Reduction Act Strategic Operating Plan, FY 2023 – 2031* (the *IRA Strategic Operating Plan*). The plan outlines how the IRS will deploy investments from the IRA to better serve taxpayers, tax professionals, and the broader tax ecosystem. The IRS plans to accomplish this work through a series of initiatives and projects aligned to the following five objectives:

1. Dramatically improve services to help taxpayers.
2. Quickly resolve taxpayer issues when they arise.
3. Focus expanded enforcement on taxpayers with complex tax filings and high-dollar non-compliance to address the Tax Gap.
4. Deliver cutting-edge technology, data, and analytics to operate more effectively.
5. Attract, retain, and empower a highly skilled, diverse workforce and develop a culture that is better equipped to deliver results for taxpayers.

However, in January 2025, a Presidential Memorandum implemented a hiring freeze and subsequently commenced early retirement initiatives for federal employees.⁴ In February 2025, the IRS began reductions in force and reorganization plans as part of a federal-wide effort to shrink government.⁵ The IRS also began employment actions to terminate probationary employees. In May 2025, we reported that the IRS placed 48 senior Information Technology

⁴ *Hiring Freeze*, 90 Fed. Reg. 8247 (January 2025).

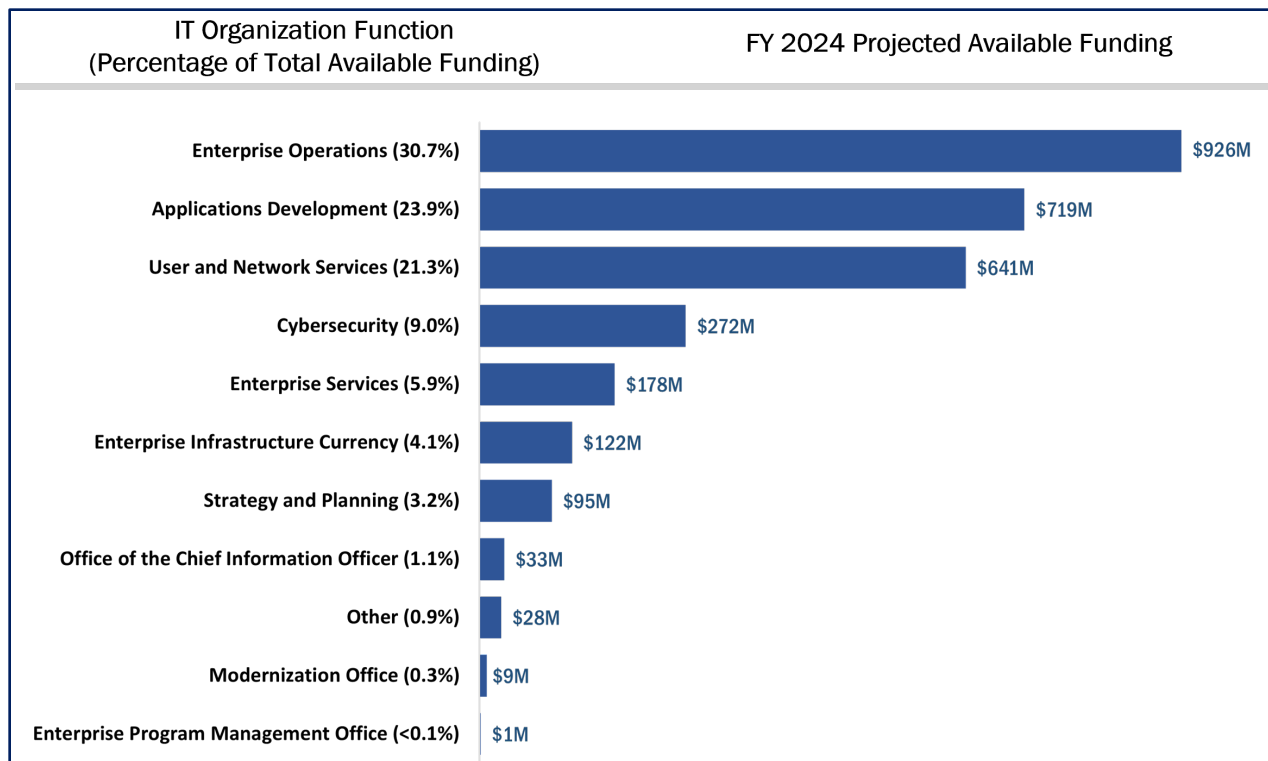
⁵ Memorandum to Heads of Executive Departments and Agencies, *Guidance on Agency RIF and Reorganization Plans Requested by Implementing the President's "Department of Government Efficiency" Workforce Optimization Initiative* (February 2025).

employees on administrative leave.⁶ Treasury and IRS leadership determined that “the best way to improve the performance of the IRS was to place approximately 50 personnel, primarily non-technical, who were in technical decision-making roles on temporary paid administrative leave while information technology reform efforts were underway.” Of the 48 employees placed on leave, 27 were either in key management positions or were individuals recruited for their expertise related to the IRS’s restructuring efforts. The IRS’s ability to move forward with its modernization efforts is uncertain considering the recent federal-wide and cost-cutting initiatives.

The IRS’s information technology budget remained the same as last year

In FY 2024, the IRS’s appropriations remained at \$12.3 billion, designated for operations support, enforcement, business systems modernization, and taxpayer services. The Information Technology (IT) organization comprises a significant portion of the IRS’s budget and plays a critical role that enables the IRS to carry out its mission and responsibilities. The IRS’s FY 2024 projected available funds included approximately \$5.7 billion for information technology investments, of which \$4.4 billion was received to fund recent legislative requirements. Figure 2 illustrates the IRS’s FY 2024 information technology projected available funding by IT organization function and major program.

Figure 2: FY 2024 Information Technology Projected Available Funding by IT Organization Function and Major Program

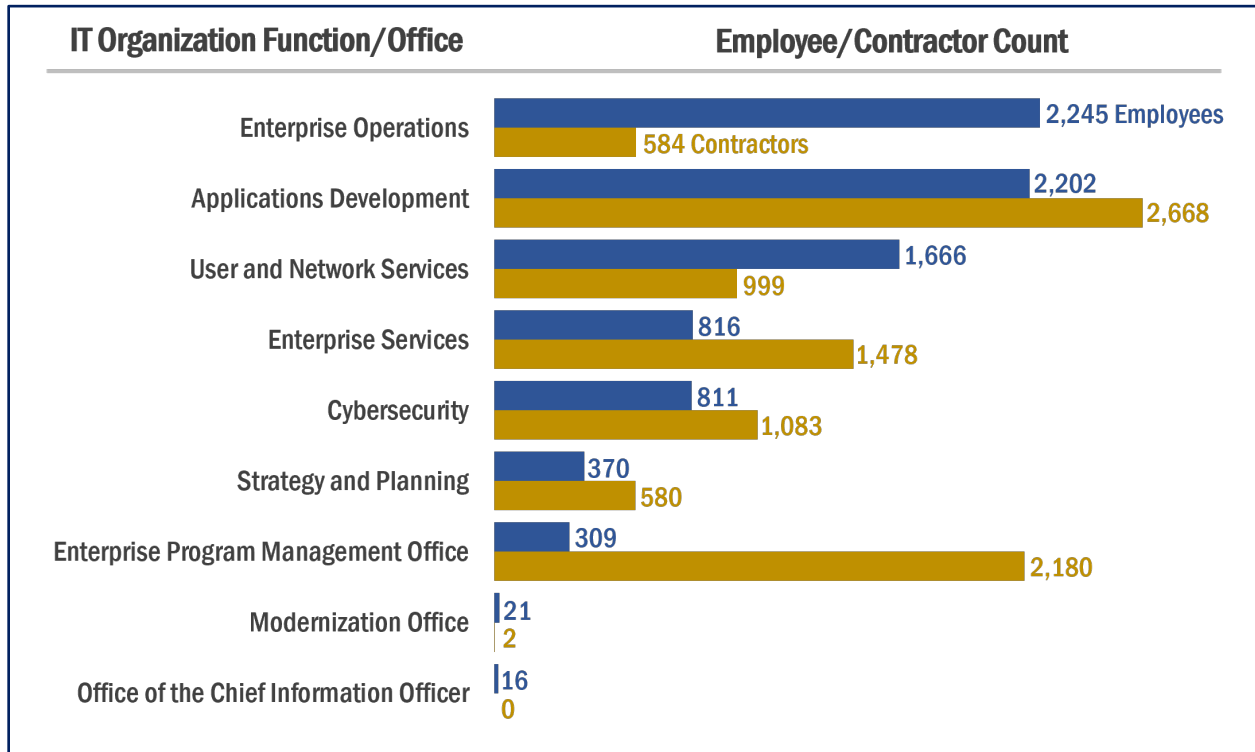


Source: IT organization budget data as of June 2024, based on information provided by the Strategy and Planning function’s Office of Financial Management Services. The Other category includes Shared Support and other funds not yet distributed. The percentages do not add up to 100 percent due to rounding.

⁶ TIGTA, Report No. 2025-IE-R017, [Snapshot Report: IRS Workforce Reductions as of March 2025](#), (May 2025).

Figure 3 illustrates that, as of June 2024, the IRS had a total of 8,456 employees and 9,574 contractors working across 9 different IT organization functions and offices – 1,287 more employees and 1,267 more contractors than reported in FY 2023.

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



Source: IRS Human Resources Reporting Center as of June 2024.

Objective

The overall objective of this review was to assess the adequacy and security of the IRS's information technology.

Results of Review

During this annual review, we summarized information from program efforts in cybersecurity, systems development, and information technology operations. We compiled the summaries from 24 audit reports (19 by TIGTA and 5 by the GAO) that were issued during FY 2024.⁷ This report does not reflect any additional audit work or corrective actions that the IRS may have taken since the initial reporting of the audit results.

⁷ See Appendix I for a complete list of audit reports.

Secure Information Systems Help Protect 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 also 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 must secure its computer systems against the growing threat of cyberattacks. In addition to TIGTA's annual Federal Information Security Modernization Act (FISMA) report that provides an overall assessment of the information security program, we issued several reports assessing the IRS's efforts to protect its information and taxpayer data.⁸ We feature findings from some of those reports below.

Cybersecurity program rated not fully effective















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 FISMA and is supported by the Office of Management and Budget (OMB), the Department of Homeland Security, agency security policy, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST) related to information security practices. Figure 4 presents the five NIST Cybersecurity Framework function areas and aligns each with the associated security program components of the FISMA Reporting Metric Domains.⁹

⁸ Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551-3558 (2018).

TIGTA, Report No. 2024-200-039, [Fiscal Year 2024 IRS Federal Information Security Modernization Act Evaluation](#) (July 2024).

⁹ OMB, *Fiscal Year 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (February 2023); NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 2018).

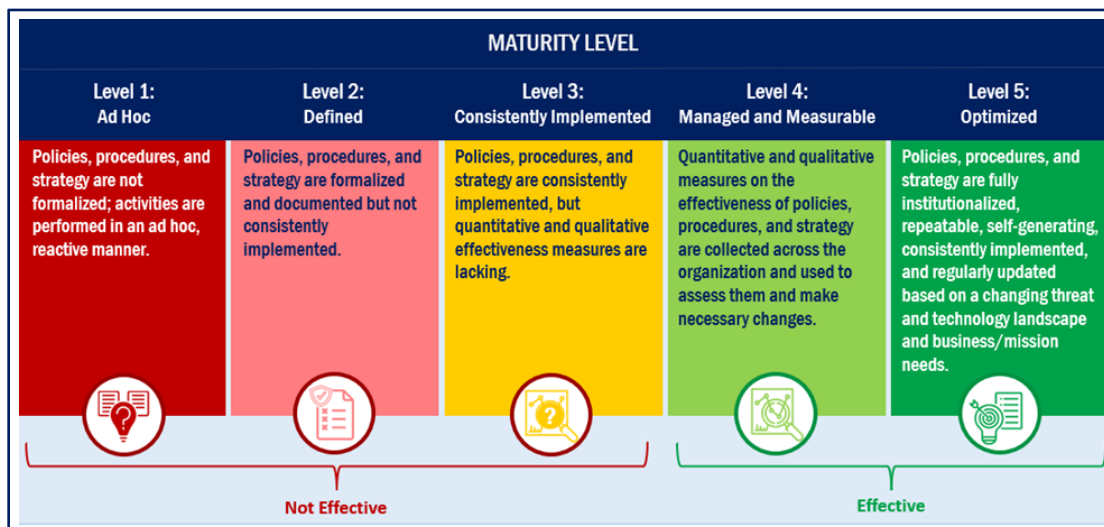
Figure 4: Alignment of the Cybersecurity Framework Function Areas to the FISMA Reporting Metric Domains

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: FISMA Reporting Metrics and the 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. There are five maturity levels, ranging from *Ad Hoc* for not having formalized policies, procedures, and strategies to *Optimized* for fully institutionalizing sound policies, procedures, and strategies across the agency. The scoring methodology defines “effective” as being at a maturity level 4, *Managed and Measurable*, or above.

Figure 5: Inspector General’s Assessment Maturity Levels



Source: FISMA Reporting Metrics.

We rated the Cybersecurity program as “not fully effective”, based upon the program not being effective in the IDENTIFY, PROTECT, and DETECT capabilities (*i.e.*, three of the five capabilities) of the Cybersecurity Framework. We found 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; implementing flaw remediation on a timely basis; encrypting to protect data at rest; and implementing multifactor authentication on its systems and facilities. We rated the RESPOND and RECOVER capabilities as effective.

Taxpayer data privacy risks continue

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 2024, TIGTA performed four audits involving privacy of taxpayer data. We initiated one audit to assess the effectiveness of the development and security of the IRS Direct File pilot.¹⁰ The IRA required the IRS to establish a task force to design and report to Congress on an IRS-run free, direct electronic filing tax return system. The Direct File pilot team selected the use of a memorandum of understanding to document the information exchanges between the IRS and each participating state. We reviewed the memorandum of understanding between the IRS and five participating states: Arizona, California, Massachusetts, New York, and Washington. We did not find the relevant security or technical details, as defined by the NIST, required for managing the exchange of taxpayer data during our review of the memorandums of understanding with the participating states. The memorandums of understanding only contained high-level detail on how the states would work with the Direct File pilot. Therefore, without the appropriate agreements in place with participating states, there is a risk that the information exchange may not adequately protect sensitive data during transmission.

We initiated another audit to assess the IRS's actions to timely address the 30-day requirements from OMB guidance that did not allow TikTok on government devices.¹¹ TikTok is a software application owned and operated by a privately held company headquartered in Beijing, China. The No TikTok on Government Devices Act requires agencies to remove the social networking service TikTok from government devices.¹² On February 27, 2023, the OMB issued implementation guidance for the removal of TikTok from government devices.¹³ Our review identified more than 2,800 mobile devices used by Criminal Investigation that could access TikTok's website and approximately 900 employees who could use assigned computers to get access to TikTok using a third-party software accessed through the computer's internet browser.

¹⁰ TIGTA, Report No. 2024-200-050, [The Direct File Pilot Deployed Successfully: However, Security and Testing Improvements Are Needed](#) (September 2024).

¹¹ TIGTA, Report No. 2024-IE-R003, [The Internal Revenue Service Is Not Fully Complying With the No TikTok on Government Devices Implementation Guidance](#) (December 2023).

¹² Pub. L. No. 117-328, div. R, §§ 101-102.

¹³ OMB Memorandum M-23-13, “No TikTok on Government Devices” Implementation Guidance (February 2023).

Criminal Investigation did not request the required exemption from the Treasury Department to continue using TikTok nor has it taken steps to block access to TikTok on computers and mobile devices assigned to its personnel.

Access controls should ensure resource protection

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, and other computing resources. Access controls involve 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. System security access controls include authentication and identity proofing, authorization, and access management.

Authentication and identity proofing efforts were sufficient

In our audit of the IRS Direct File pilot, we reviewed the Digital Identity Risk Assessment and associated documents and found that the Direct File pilot sufficiently assessed and implemented assurance levels. The NIST provides requirements for agencies to address authentication and identity proofing risks related to digital transactions.¹⁴ Agencies must perform risk assessments; select individual assurance levels for identity proofing, authentication, and federation; determine which processes and technologies they will employ to meet each assurance level; and document these decisions. The Direct File pilot uses the Secure Access Digital Identity solution for identity proofing and authentication. All taxpayers are required to create a Secure Access Digital Identity account to access the Direct File pilot. By complying with NIST and IRS requirements for assessing risks associated with Direct File pilot identity proofing and authentication, the IRS has taken steps to mitigate potential unauthorized disclosure of taxpayer data.

Authorizations were not always justified

Authorization is the process of granting access rights and privileges to a system or file. 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. In FY 2024, TIGTA initiated an audit to determine whether the IRS effectively implemented the Next Generation Enterprise Security Audit Trails program to meet federal and IRS authorization requirements.¹⁵ The data repository that the program uses contains two modules with audit trail information. These had 74 and 29 authorized users, respectively, in the Business Entitlement Access Request System as of February 2023. We found 18 users without a valid business justification for access.

Management Action: As of May 2023, each of the 18 users without a valid business justification had their access removed.

¹⁴ NIST, Special Publication 800-63-3, *Digital Identity Guidelines* (June 2017).

¹⁵ 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](#) (October 2023).

Control weaknesses identified in access management

Access management helps to protect the confidentiality, integrity, and availability of the services, data, and assets by ensuring that only authorized users can access or modify them. During FY 2024, TIGTA performed three reviews involving access management. We initiated a review to assess user access to taxpayer information maintained by the IRS and identify the number of IRS systems that contain taxpayer information.¹⁶ Our evaluation identified that not all user accesses are timely removed once they separated from the IRS. Specifically, we identified that 279 of the 91,661 users with sensitive system access were listed in the Business Entitlement Access Request System as separated and continued to have access to 1 or more sensitive systems as of July 2023. For 276 of these users, they had been separated from the IRS between 6 and 502 days without their systems' access being removed.

In our audit of the Next Generation Enterprise Security Audit Trails program, we found that the IRS is not removing inactive user accounts timely. The data repository where audit trail information is stored had 1,383 users as of March 2023. The IRS identified 486 (35 percent) of the 1,383 users with access to its data repository who had not logged into the system in the 90 days prior to its March 2023 review.

By not monitoring the activity of user accounts, the IRS is unaware of when inactive accounts reach a threshold that requires action, such as disabling an account or removing access. Failure to properly monitor and deactivate user accounts increases the risk of unauthorized access to sensitive audit trail data.

Management Action: As of June 2023, the IRS implemented an automated process to disable user accounts with 120 days of inactivity. In addition, it began removing access authorizations to the data repository for user accounts with 120 days of inactivity. While an improvement, the IRS's *Cloud Computing Security Policy* requires inactive user accounts be automatically disabled after 90 days.

Network vulnerabilities were not timely identified or resolved

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. In FY 2024, TIGTA performed four audits involving system scanning, vulnerability remediation, and patching. We initiated an audit to evaluate the effectiveness and security of the Login.gov deployment.¹⁷ In early February 2023, we found that the Security Risk Management organization had not yet obtained access to the Federal Risk and Authorization Management Program (FedRAMP) repository for Login.gov so that the [REDACTED] could begin continuous monitoring security reviews. After we brought this matter to the IRS's attention, management from the Security Risk Management organization stated that they would obtain access to the FedRAMP repository, and the [REDACTED] would start retroactively completing the



¹⁶ TIGTA, Report No. 2024-IE-R008, [Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information](#) (February 2024).

¹⁷ TIGTA, Report No. 2024-200-032, [Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed](#) (July 2024).

continuous monitoring security reviews and documenting the results for each of the months missed. For the months when continuous monitoring security reviews were not completed timely, *i.e.*, November 2022 through May 2023, our review identified a critical vulnerability. Personally Identifiable Information was sent to unauthorized locations outside of the United States by a Login.gov vendor's fraud prevention solution. As a result, user data associated with 613,407 IRS user authentications for Login.gov were potentially placed at risk.

We also initiated an audit to determine whether sufficient security safeguards over the Compliance Data Warehouse (CDW) exist to protect taxpayer data against unauthorized access.¹⁸

According to the IRS, the timely identification and resolution of information security weaknesses are the primary cornerstones of a sound information security program. The Internal Revenue Manual (IRM) requires system owners to employ vulnerability scanning tools that look for software flaws and improper configuration settings and measure vulnerability impacts.

From December 2022 to October 2023, nine plans of action and milestones were created to implement corrective action plans for untimely unremediated vulnerabilities within the CDW. However, none of these nine plans were created within agency-defined timelines. Research, Applied Analytics, and Statistics management officials acknowledged

In addition, we initiated an audit to review the vulnerability and configuration compliance of a General Support System, Mainframe Platform Environment, and a Major Application, Security Application Environment.¹⁹ In January 2024, the Mainframe Platform Environment had 80 open and unresolved vulnerabilities. Of these vulnerabilities, 67 were overdue: 15 had a Critical Risk, 30 had a High Risk, and 22 had a Medium Risk. The remaining 13 vulnerabilities were open but not overdue. The Security Application Environment had 56,537 open and unresolved vulnerabilities. Of these vulnerabilities, 33,366 were overdue: 2,048 had a Critical Risk, 13,558 had a High Risk, 15,452 had a Medium Risk, and 2,308 had a Low Risk. The remaining 23,171 vulnerabilities were open but not overdue.

Cybersecurity function personnel confirmed that the unresolved vulnerabilities are the result of a transition from one vulnerability scanning tool to another. The transition to the new tool resulted in more robust scanning and an overall increase in the volume of identified vulnerabilities that they have not yet addressed. Enterprise Operations and Cybersecurity functions' personnel agreed that vulnerabilities persist. The existence of unresolved vulnerabilities increases the risk to the overall security of IRS assets.

System assets were not in compliance with configuration requirements

Configuration management administers security features for hardware, software, and firmware components of an information system throughout its life cycle. Effective configuration

¹⁸ TIGTA, Report No. 2024-200-042, [Compliance Data Warehouse Security Needs Improvement](#) (September 2024).

¹⁹ TIGTA, Report No. 2024-200-057, [Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement](#) (September 2024).

management provides reasonable assurance that systems are operating securely and as intended. In FY 2024, TIGTA performed two audits involving system configuration management.

In July 2024, we assessed the Mainframe Platform Environment and the Security Application Environment configuration compliance reports and found 48 and 695 noncompliant asset configurations, respectively. Overall, a total of 743 assets used noncompliant configurations across both environments. The existence of noncompliant configurations increases the risk to the overall security of IRS assets.

In our audit of the security safeguards over the CDW, we found that multiple servers were not in compliance with configuration requirements. We reviewed a configuration compliance scan report dated September 5, 2023, and found that it included [REDACTED] CDW servers. [REDACTED]

The remaining 13 servers were compliant with agency security policies.

Management Actions: In response to this finding, from September to November 2023, Research, Applied Analytics, and Statistics officials successfully remediated [REDACTED] and created an active plan of action and milestone for the remaining [REDACTED]

Network monitoring and audit logs facilitate security assessments

Audit and monitoring involve the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity. Audit and monitoring controls help information systems security professionals routinely assess computer security, recognize ongoing attacks, and perform investigations during and after an attack.

In FY 2024, TIGTA performed two audits involving network monitoring and audit logs. In our audit of the security safeguards over the CDW, we analyzed the source system audit trail files, the agency's audit trail repository, and other pertinent system security documents to evaluate compliance with auditing requirements. We found that while audit trail data are sent to the repository, accurate login information is not always accessible. Since August 2022, the CDW's audit trails have been sent to the agency's audit trail repository. However, the tools used to visualize the audit trails failed to accurately display login data fields, resulting in incomplete and unreliable login data.

In our audit of the Next Generation Enterprise Security Audit Trails program, we found that all applications with Personally Identifiable Information or Federal Tax Information are not sending audit trails to the repository. The IRM requires audit trails for systems containing Personally Identifiable Information and Federal Tax Information. The IRS states it identified 814 systems requiring an assessment of audit trails requirements. The IRS determined that 356 (44 percent) of the 814 systems required application-level audit trails for the detection and investigation of unauthorized accesses of Personally Identifiable Information and Federal Tax Information. Our analysis of the 356 systems as of June 2023 showed that:

- 231 (65 percent) systems are sending their event log data to the data repository.
- 125 (35 percent) systems are not sending their event log data to the data repository.

In addition, as of June 2023, several system owners have not engaged the Next Generation Enterprise Security Audit Trails program's application audit process to have their event log data collected. Failure to collect event log data limits audit capability to determine access to Personally Identifiable Information and Federal Tax Information data and the ability to identify root causes of information system problems.

Insider threat vulnerabilities remain a concern

An insider threat is current or former personnel, *e.g.*, employees and contractors, or other business partners who have or had authorized access to an organization's network, systems, or data and could intentionally misuse that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. For example, in February 2024, Charles Edward Littlejohn, a former IRS contractor, was sentenced to five years in prison for disclosing thousands of tax returns without authorization.²⁰ While working at the IRS, Littlejohn accessed and stole tax returns and return information for a high-ranking government official and related entities and individuals. He disclosed the tax return information to two different news organizations that published more than 50 articles using the information.

In FY 2024, TIGTA performed an audit involving insider threats.²¹ As of January 2024, the IRS had [REDACTED] active users with approval to [REDACTED]. We determined that all users had the required Business Entitlement Access Request System approval. We also tested the effectiveness of this control [REDACTED] the computer of an IRS user who did not have the [REDACTED] approval. The user was able to [REDACTED] but was unable to [REDACTED] which demonstrated that the control was working properly.

The IRS is effectively preventing users from [REDACTED]. The IRS [REDACTED]. The IRS uses a [REDACTED] lookup tool that categorizes [REDACTED] and determines if a [REDACTED] is properly categorized and if not, requests the vendor to categorize the [REDACTED]. We selected a judgmental sample of 50 [REDACTED] that were [REDACTED] by the IRS and tested our access to them. We determined that the IRS properly [REDACTED] all 50 [REDACTED].

However, during this audit, we found that while controls are in place to detect, monitor, and sever external connections, [REDACTED]. The IRS implemented a network visibility tool to identify and track unauthorized access attempts to [REDACTED]. We reviewed the tool and determined it has capabilities such as real-time monitoring, detecting malicious activities, and blocking unauthorized access, but the controls to [REDACTED] external connections [REDACTED] mock taxpayer data [REDACTED]. The NIST requires organizations to detect and deny outgoing communications traffic posing a threat to systems and audit the identity of internal users associated with denied communications.²² [REDACTED] access to [REDACTED] accessible on [REDACTED] users can exfiltrate taxpayer data.

²⁰ TIGTA, Announcement, [Former IRS Contractor Sentenced for Disclosing Tax Return Information](#) (February 2024).

²¹ TIGTA, Report No. 2024-200-048, [Actions Need to Be Taken to Improve the Data Loss Prevention Solution and Reduce the Risk of Data Exfiltration](#) (September 2024).

²² NIST, Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020).

[REDACTED] to an [REDACTED], and [REDACTED] that [REDACTED] to a [REDACTED]. Once [REDACTED] was transmitted, we were able to [REDACTED] open it on a personal device, and read the data. In addition, following IRS-approved methods for external [REDACTED], we were able to [REDACTED] and [REDACTED]. We then were able to [REDACTED]. These [REDACTED] that there are [REDACTED] within the data loss prevention solution that could allow a user to intentionally circumvent the controls and exfiltrate sensitive taxpayer data for inappropriate use.

Separation of duties for cloud systems were not always adequate

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

During FY 2024, we initiated an audit to determine whether the FedRAMP Security Threat Analysis Reports were prepared and if continuous monitoring efforts were adequate to ensure the security of IRS cloud systems.²³ The IRS was not maintaining appropriate separation of duties for certain roles related to cloud systems. We determined that 35 (70 percent) of the 50 cloud systems reviewed had the same individuals assigned as either the Authorizing Official or the Authorizing Official Designated Representative and System Owner. Insufficient separation of duties elevates the risk of both erroneous and inappropriate actions whether deliberate or unintentional.

Effective security policies, procedures, and documentation enable governance

The documentation of system security is an important element of information management for an organization. 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, define a sequence of steps to be followed in a consistent manner.

In FY 2024, TIGTA performed eight audits involving security policies, procedures, and documentation. We initiated an audit to assess the IRS's efforts to provide effective management and oversight of cloud services contracts.²⁴ The Cybersecurity function was unable to provide documentation that it completed any FY 2022 FedRAMP continuous monitoring security reviews for 67 cloud applications listed on the November 2022 *Cloud Inventory Report*. Cybersecurity function management explained that they performed the FedRAMP continuous

²³ TIGTA, Report No. 2024-200-047, [Improvements Are Needed in the Cloud Security Assessment, Approval, and Monitoring Processes](#) (September 2024).

²⁴ TIGTA, Report No. 2024-200-009, [Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements](#) (January 2024).

monitoring security reviews but did not document them. Because the IRS did not document its FedRAMP continuous monitoring security reviews, it is unable to support that the cloud service providers are maintaining an appropriate risk posture of its cloud applications.

In the Login.gov audit, we found that the requirements for credential service providers to capture and provide sufficient audit log content need improvement. The IRS does not have consolidated guidance, but rather various policies and related documents requiring credential service providers to capture audit trail requirements. In addition, the policies and related documents do not include all audit trail data, including investigative data elements. It is also important to have consolidated guidance to ensure the efficient and effective identification and implementation of credential service provider requirements. This will reduce the risk of Login.gov and future credential service providers omitting critical investigative audit trail data elements and potentially jeopardize investigations.

Systems Development and Information Technology Operations Are Critical to Administering Tax Laws

In carrying out its responsibilities for administering the tax laws, the IRS relies extensively on information technology investments to support its mission-related operations. TIGTA and GAO performed several audits that assessed systems development and information technology operations at the IRS. These audits covered information technology acquisitions; information technology asset management; project management; implementation of corrective actions; and updating and modernizing operations/information technology investments.

Information technology acquisition procedures were not always followed

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. 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 2024, TIGTA performed two audits involving information technology acquisitions. We initiated an audit to determine the IRS's effectiveness to convert its information systems and services to Internet Protocol version 6 (IPv6) to comply with OMB requirements.²⁵ We found that IRS contracting officers either did not accurately complete or submit documentation to show if internet protocol would be used for communication for 8 (67 percent) of 12 acquisitions sampled. However, the 4 (33 percent) remaining acquisitions were properly completed and submitted, or internet protocol was not applicable. Also, the IRS did not ensure that IPv6 compliance is fully addressed with IPv6 language in requirement documents for the eight acquisitions. Without evaluating acquisitions for IPv6 compliance, the IRS may buy products that eventually may be unable to communicate with the network.

²⁵ TIGTA, Report No. 2024-200-049, [The IRS Is Not Meeting Key Federal Requirements in Its Transition to Internet Protocol Version 6](#) (September 2024).

In the cloud services contracts audit, we found that the IRS was unable to locate all cloud services contracts. After searching for nearly three months from January through March 2023, the Office of the Chief Procurement Officer, Strategic Supplier Management, and the Authorizing Officials collectively identified and provided the cloud services contracts for 65 (97 percent) of 67 cloud applications. The cloud services contracts for the remaining 2 (3 percent) cloud applications were not found. Not being able to readily identify cloud services contracts increases the risk of potential lost cost savings and duplication of cloud services and the inefficient use of resources searching for information in response to stakeholder requests. In addition, despite locating the cloud services contracts for 65 of 67 cloud applications listed on the November 2022 *Cloud Inventory Report*, the IRS was able to determine the value of the contracts for only 37 (55 percent) cloud applications of approximately \$105 million. The IRS was unable to determine the value of the cloud services contracts for the remaining 30 (45 percent) cloud applications. Therefore, the IRS's inability to identify specific cloud services contract values by cloud application increases the risk for making uninformed financial decisions.

Information technology asset management is crucial for optimizing resources

Information technology asset management refers to a set of policies and procedures that an organization uses to track, audit, and monitor the state of its information technology assets, and maintain system configurations. In FY 2024, TIGTA performed two audits involving information technology asset management. In our audit of the IPv6, we found that the IRS did not transition 20 percent of its assets requiring an internet protocol address to an IPv6-only environment within the time required by OMB and IRM guidance.²⁶ Without timely transitioning to IPv6-only communication, IRS systems will be vulnerable targets for common attacks prevalent in Internet Protocol version 4 networks such as distributed denial of service, port scanning, and spoofing. We also found that the IRS overstated the number of assets that needed to transition to IPv6. Specifically, we counted 165,251 assets that needed to be transitioned to IPv6, but the IRS reported 186,675 in the March 2024 IPv6 Chief Information Officer metrics. Therefore, the IRS incorrectly reported that 21,424 assets needed to transition to an IPv6-only environment.

In the vulnerability and configuration compliance audit of a General Support System and Major Application, we reviewed the internet protocol addresses assigned to these environments and verified that the IRS inventory system has limitations to the identification of its assets based on the discrepancies we identified. When an asset cannot be reconciled due to this limitation, it will be placed into temporary or unknown repositories. The IRS is in the process of migrating to a new system that will have more robust capabilities and resolve the issue of items being incorrectly assigned to temporary and unknown repositories.

Project management ensures organizational goals and outcomes are met

Project management is the discipline of using established principles, procedures, and policies to manage a project from conception through completion. In FY 2024, TIGTA and GAO provided coverage of information technology project management in seven audits. We initiated an audit

²⁶ OMB Memorandum, M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)* (August 2005); OMB Memorandum, *Transition to IPv6* (September 2010); and OMB Memorandum, M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)* (November 2020). This most recent OMB Memorandum partially rescinded the requirements from the 2010 guidance but directs agencies to further enhance security by completing the transition to IPv6-enabled systems and services through a series of outlined milestones.

to determine whether the IRS effectively managed the testing and defect remediation process for the Individual Tax Processing Engine project.²⁷ The Individual Tax Processing Engine project team's monitoring and measuring activities enabled them to realize that the project was at risk of not timely completing the work required to begin parallel operations in April 2024 and go-live in January 2025. Identifying these problems in advance allowed the IRS time to develop options for starting parallel operations.

In our audit of cloud services contracts, we found that the IT organization instructs stakeholders to use the Cloud Front Door and complete its four-step process for all applications migrating to the cloud. The Cloud Management Office migrates cloud-based projects, such as applications, to the cloud through its Cloud Front Door process. However, we determined that none of the 34 cloud applications listed on the November 2022 *Cloud Inventory Report* fully completed the Cloud Front Door process as part of the IRS's Enterprise Cloud Program.²⁸ The Cloud Management Office did not provide centralized management and oversight of the Enterprise Cloud Program. As a result, the Cloud Front Door process is routinely bypassed, creating confusion and leading to inefficiencies for applications migrating to the cloud. In August 2023, the Chief Information Officer announced that the Cloud Management Office was officially phased out and would be transitioning to the Enterprise Cloud Architecture and Design office to better align with the IRS's enterprise goals and modernization efforts.

GAO initiated an audit to report on the IRS's estimates of the costs and benefits of the Direct File pilot.²⁹ GAO reported the Direct File cost estimates that the IRS provided in its May 2023 report to Congress did not fully align with best practices for cost estimation. The IRS's report stated its estimates included the cost of developing and maintaining a secure, multilingual, mobile-friendly tax filing tool and its underlying technology to keep pace with changes to tax law as well as the cost of providing customer support. However, the IRS's cost estimates did not address other recommended practices, such as ensuring that all costs were included and documented. IRS officials also told GAO that the Direct File cost estimates did not include start-up costs, such as technology for a novel system, which could be substantial. Without a comprehensive accounting for costs, estimates could understate the full amount of resources required for the IRS to develop and maintain the Direct File program.

Implemented corrective actions were not always effective

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 audit 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 2024, TIGTA and GAO performed five audits with coverage on the status of implementing corrective actions. We initiated an audit to assess the efforts to identify, replace, and

²⁷ TIGTA, Report No. 2024-208-052, [*The Individual Tax Processing Engine Project Is Progressing, but Risks Remain*](#) (September 2024).

²⁸ Because the Cloud Management Office was established in February 2020, only 34 of the 67 cloud applications on the *Cloud Inventory Report* were required to complete the Cloud Front Door process.

²⁹ GAO, GAO-24-107236, *IRS Direct File: Actions Needed during Pilot to Improve Information on Costs and Benefits* (April 2024).

decommission legacy systems and follow up on prior audit recommendations.³⁰ The IRS fully and effectively implemented the planned corrective actions for two of the four recommendations from the prior report. For example, we previously reported that there were no requirements for system owners to provide and periodically update system information in the As-Built Architecture. The IRS agreed to implement a policy requiring system owners to provide and update system information. Our review also determined that, as of February 2024, information for 732 of the 733 systems had been updated within a year of our review, and the remaining system was updated just over 1 year after our review. As a result, we determined that this planned corrective action was fully and effectively implemented.

While the IRS fully and effectively implemented the planned corrective actions for two of four recommendations from the prior report, two planned corrective actions fully implemented were not effective. For example, we previously reported that the IRS did not have specific or long-term plans to address the updating, replacing, or retiring of most legacy systems. The IRS stated that it will implement a strategy to include the current scope of IT organization-managed and business-managed systems for an enterprise-wide strategic approach to identify, prioritize, and recommend the updating, replacing, or retiring of current and future legacy systems. The IRS established the Technology Retirement Office within the Enterprise Services function in August 2021 to strategically reduce the information technology footprint across the enterprise. As of December 2023, the IRS had identified only 107 (32 percent) of 334 legacy systems in the As-Built Architecture as candidates for retirement, while the remaining 227 legacy systems had not been identified for retirement. Of the 107 legacy systems, only 2 systems have specific decommissioning plans. As a result, we determined that while this planned corrective action was fully implemented, it was not effective in correcting the identified deficiency.

During its audit of the IRS's FY 2023 and FY 2022 financial statements, GAO determined that unresolved information system control deficiencies from prior audits along with new control deficiencies collectively represent a significant deficiency in the IRS's internal control over financial reporting.³¹ These control deficiencies relate to information system general controls in the areas of security management, access controls, and configuration management. The new and continuing control deficiencies include the timely creation of plans of action and milestones to address identified vulnerabilities or weaknesses, use of multifactor authentication, encryption of sensitive data, logging and monitoring of audit records, and management of configuration settings for certain platforms.

The IRS mitigated the potential effect of these control deficiencies primarily through compensating controls that management has designed to detect potential misstatements on the financial statements. In addition, over the past several years, IRS management has increased its focus on completing the corrective actions necessary to address many of the information system control deficiencies that make up the significant deficiency. This has resulted in the closure of numerous system-specific recommendations. However, while IRS management has demonstrated its commitment to addressing the significant deficiency in information system controls, additional efforts are needed to fully address the remaining unresolved control deficiencies that constitute the significant deficiency. It will be important for IRS management to

³⁰ TIGTA, Report No. 2024-200-038, [The IRS Does Not Have Specific Plans to Replace and Decommission Legacy Systems](#) (August 2024).

³¹ GAO, GAO-24-106472, *Financial Audit: IRS's FY 2023 and FY 2022 Financial Statements* (November 2023).

build on the progress made and to sustain focus on improving the agency's information system controls.

Progress continues in modernizing operations

Successful modernization of systems and the development and implementation of new information technology applications are critical to meet the IRS's evolving business needs and enhance services provided to taxpayers.

In FY 2024, TIGTA and GAO performed six audits with coverage on updating and modernizing operations. We initiated a review to evaluate the progress of the IRS's information technology modernization, including transforming core account data and processing efforts funded by the IRA.³² The IRS identified 58 milestones in its *IRA Strategic Operating Plan* that were to be delivered in FY 2023. We found that the IRS is making progress in its modernization efforts while adhering to its strategic goals. Specifically, the IT organization is making significant technical advancements in the areas of Artificial Intelligence, automation, cloud capabilities, data access, data quality, and data standards. The IRS is undergoing multiple new processes, and once fully operational, they will pave the way for a new technology era across the enterprise. However, the *IRA Strategic Operating Plan* does not identify specific projects. Therefore, we could not determine the project interdependencies. Current, complete, and accurate information is necessary for management to make informed decisions and to achieve objectives and evaluate risks.

In its audit of the IRS's modernization efforts, GAO determined that the IRS defined a new vision for information technology modernization, but implementation plans were not completed.³³ Although the IRS issued its agencywide *IRA Strategic Operating Plan* outlining its vision to use billions of dollars contained in the IRA appropriation to transform the administration of the tax system and services provided to taxpayers, plans showing changes to the scope of future work, milestones, and efforts to retire legacy systems, however, had not yet been updated. Completing the roadmap and then updating ongoing information technology modernization plans to reflect revisions driven by the strategic plan are essential to the transformation's success.

Conclusion

The security of systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. The IRS needs to ensure that it continues to leverage viable technological advances as it modernizes its 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 such as addressing weaknesses within the IRS's computer operations. In addition, staffing levels within the Information Technology organization may change due to the implementation of Executive Orders and other directives. Reduced staffing could adversely affect the IRS's ability to meet its mission of helping taxpayers comply with their tax responsibilities and enforcing the tax laws with integrity and fairness to all.

³² TIGTA, Memorandum No. 2024-2S8-055, [Progress of Information Technology Modernization Efforts](#) (September 2024).

³³ GAO, GAO-24-106566, *Information Technology: IRS Needs to Complete Planning and Improve Reporting for Its Modernization Programs* (March 2024).

Performance of This Review

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Federal Offices of Inspector General*. Those standards require that the work adheres to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on the objective of our review.

Appendix I

List of Treasury Inspector General for Tax Administration and Government Accountability Office Reports Reviewed (in month issuance order)

1. 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* (October 2023).
2. TIGTA, Report No. 2024-408-004, *Inflation Reduction Act: Assessment of Implementation of Processing Year 2023 Tax Provisions* (October 2023).
3. GAO, GAO-24-106472, *Financial Audit: IRS's FY 2023 and FY 2022 Financial Statements* (November 2023).
4. TIGTA, Report No. 2024-400-012, *Administration of the Individual Taxpayer Identification Number Program* (December 2023).
5. TIGTA, Report No. 2024-IE-R003, *The Internal Revenue Service Is Not Fully Complying With the No TikTok on Government Devices Implementation Guidance* (December 2023).
6. TIGTA, Report No. 2024-200-009, *Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements* (January 2024).
7. GAO, GAO-24-106091, *IRS Reform: Following Leading Practices and Improving Cost Estimation Policies Could Benefit Agency Efforts* (February 2024).
8. TIGTA, Report No. 2024-IE-R008, *Assessment of Processes to Grant Access to Sensitive Systems and to Safeguard Federal Tax Information* (February 2024).
9. GAO, GAO-24-106566, *Information Technology: IRS Needs to Complete Planning and Improve Reporting for Its Modernization Programs* (March 2024).
10. GAO, GAO-24-107236, *IRS Direct File: Actions Needed During Pilot to Improve Information on Costs and Benefits* (April 2024).
11. GAO, GAO-24-107356, *Priority Open Recommendations: Internal Revenue Service* (June 2024).
12. TIGTA, Report No. 2024-200-025, *Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Adequately Documented and Effectively Implemented* (June 2024).
13. TIGTA, Report No. 2024-200-032, *Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed* (July 2024).
14. TIGTA, Report No. 2024-200-039, *Fiscal Year 2024 IRS Federal Information Security Modernization Act Evaluation* (July 2024).
15. TIGTA, Report No. 2024-200-038, *The IRS Does Not Have Specific Plans to Replace and Decommission Legacy Systems* (August 2024).

16. TIGTA, Report No. 2024-200-042, *Compliance Data Warehouse Security Needs Improvement* (September 2024).
17. TIGTA, Report No. 2024-200-046, *The Vulnerability Disclosure Policy Has Been Implemented; However, Actions Are Needed to Improve the Program* (September 2024).
18. TIGTA, Report No. 2024-200-047, *Improvements Are Needed in the Cloud Security Assessment, Approval, and Monitoring Processes* (September 2024).
19. TIGTA, Report No. 2024-200-048, *Actions Need to Be Taken to Improve the Data Loss Prevention Solution and Reduce the Risk of Data Exfiltration* (September 2024).
20. TIGTA, Report No. 2024-200-049, *The IRS Is Not Meeting Key Federal Requirements in Its Transition to Internet Protocol Version 6* (September 2024).
21. TIGTA, Report No. 2024-200-050, *The Direct File Pilot Deployed Successfully; However, Security and Testing Improvements Are Needed* (September 2024).
22. TIGTA, Report No. 2024-200-057, *Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement* (September 2024).
23. TIGTA, Report No. 2024-208-052, *The Individual Tax Processing Engine Project Is Progressing, but Risks Remain* (September 2024).
24. TIGTA, Report No. 2024-2S8-055, *Progress of Information Technology Modernization Efforts* (September 2024).

Appendix II

Glossary of Terms

Term	Definition
Acquisition	The acquiring, by contract with appropriated funds, of supplies or services (including construction) by and for the use of the federal government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated.
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.
Artificial Intelligence	The ability of a digital computer to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.
As-Built Architecture	The authoritative source of the IRS's information technology and business environments. It documents the production environment of IRS systems, infrastructure, technology platforms, <i>etc.</i>
Asset	A major application, General Support System, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Trail	A chronological record of information system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorizing Official	An official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Business Entitlement Access Request System	A system that manages identity access management. It is used to request, modify, and remove access for active users to IRS systems by managing the digital identity of individuals, roles, resources, and entitlements granted or removed.
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.
Cloud	The use of computing resources, <i>e.g.</i> , hardware and software, which are delivered as a service over a network (typically the internet).

Term	Definition
Cloud Service Provider	A third-party company offering a cloud-based platform, infrastructure, application, or storage services.
Configuration	The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged.
Configuration Management	Establishes proper control over approved project documentation, hardware, and software, and assures changes are authorized, controlled, and tracked.
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Control/Internal Control	A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. It comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. It also serves as the first line of defense in safeguarding assets. In short, controls help managers achieve desired results through effective stewardship of public resources.
Credential	An object or data structure that authoritatively binds an identity – via an identifier or identifiers and (optionally) additional attributes – to at least one authenticator possessed and controlled by a subscriber.
Credential Service Provider	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A credential service provider may be an independent third party or may issue credentials for its own use.
Criminal Investigation	An IRS business unit that serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.
Data Loss Prevention	The practice of detecting and preventing confidential data, such as Personally Identifiable Information, from being "leaked" out of an organization's boundaries, either intentionally or unintentionally.
Data Repository	A database and analytics tool used to analyze the streams of machine data generated by information technology systems and technology infrastructure.
Decommission	The removal of information technology assets from the production environment. Decommissioning legacy systems includes hardware, software, licenses, and the closeout of support contracts.
Decrypt	The process of converting encrypted data into recognizable information.
Defect	An error in coding or logic that causes a program to malfunction or to produce incorrect/unexpected results.
Department of the Treasury	The federal agency that manages federal finances by collecting taxes and paying bills and by managing currency, government accounts, and public debt. The Treasury Department also enforces finance and tax laws.

Term	Definition
Digital Identity Risk Assessment	This process identifies the risks to system security and determines the probability of occurrence, the resulting impact, and the additional safeguards that would mitigate the impact. It is a redesign of the IRS's previous Electronic Authentication Risk Assessment process.
Distributed Denial of Service	A malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.
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.
Encrypt	The process of converting plain text to cipher text by means of a cryptographic system.
Entitlement	Rights granted to the user of licensed software that are defined within the license agreement.
Event	Any action that happens on a computer system. Examples include logging in to a system, executing a program, and opening a file.
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 Information Security Modernization Act of 2014	An amendment to the Federal Information Security Management Act of 2002 that allows for further reform to federal information security. This bill amends Chapter 35 of Title 44 of the United States Code. The original statute (Federal Information Security Management Act of 2002) requires agencies to assess risks to information systems and provide information security protections commensurate with the risks, integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to the OMB.
Federal Risk and Authorization Management Program	A governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Federal Risk and Authorization Management Program Security Threat Analysis Report	Provides the Authorizing Official with a systematic analysis of which controls failed, given the nature of the system, the probable threat characteristics, and the most likely attack vectors. A threat analysis answers questions like, "Where am I most vulnerable for attack?," "What are the most relevant threats?," and "What do I need to do to safeguard against these threats?," thus enabling informed risk management decisions.
Federal Tax Information	Consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code and subject to the § 6103(p)(4) safeguarding requirements including IRS oversight.

Term	Definition
Federation	A collection of realms (domains) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.
Filing Season	The period from Jan. 1 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.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Identity Proofing	Verifying the claimed identity of an applicant by collecting and validating sufficient information, <i>e.g.</i> , identity history, credentials, and documents, about a person.
Implementation Plan	A written document that outlines a team's steps to accomplish a goal or project. This document enables team members and key stakeholders to understand all aspects of a project before executing it.
Individual Tax Processing Engine	A modernization effort to convert two Individual Master File programs written in an old programming language into a modern programming language with the intent of maintaining all current functionality and capabilities.
Information System Security Officer	An individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or system owner for maintaining the appropriate operational security posture for a system or program.
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.
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 and is usually internal to an organization and deployed within owned facilities.

Term	Definition
Internal Revenue Manual	The IRS's primary source of instructions to its employees related to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Internet Protocol	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Internet Protocol Version 4	The version of the internet protocol which specifies a 32-bit address field that will run out of available address space in the near future.
Internet Protocol Version 6	The next generation internet protocol that allows a 128-bit address field in the form of 8 16-bit integers represented as 4 hexadecimal digits separated by colons.
Joint Audit Management Enterprise System	The Treasury Department system for use by all bureaus to track, monitor, and report the status of internal control audit results. The system tracks specific information on issues, findings, recommendations, and planned corrective actions from audit reports issued by oversight agencies, such as TIGTA.
Legacy System	An information system that may be based on outdated technologies but is critical to day-to-day operations. In the context of computing, it refers to outdated computer systems, programming languages, or application software that are used instead of more modern alternatives.
Log	A file containing data about an event that occurred in an application or operating system.
Login.gov	A service that offers secure and private online access to federal government programs, such as federal benefits, services, and applications. With a Login.gov account, users can sign into multiple federal government websites with the same email address and password.
Mainframe	A powerful, multiuser computer capable of simultaneously supporting many hundreds of thousands of users.
Memorandum of Understanding	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.
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, <i>e.g.</i> , password/Personal Identification Number; 2) something you have, <i>e.g.</i> , cryptographic identification device, token; or 3) something you are, <i>e.g.</i> , 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.

Term	Definition
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Office of Management and Budget	Federal agency that oversees the preparation and administration of the federal budget and coordinates federal procurement, financial management, information, and regulatory policies.
Parallel Operations	Compares legacy Individual Master File output with the output generated by the Java code for two Individual Master File programs and will occur prior to the Individual Tax Processing Engine project moving into production.
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.
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.
Pilot	A limited version (limited functionality or limited number of users) of a system being deployed to discover as well as resolve problems before full implementation.
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.
Planned Corrective Action	A process to address IRS material weaknesses, significant deficiencies, and existing reportable conditions through remediation and action plans.
Platform	A computer or hardware device, associated operating system, or virtual environment on which software can be installed or run.
Policy	A guiding principle, typically established by senior management, which is adopted by an organization to influence and determine decisions.
Port Scanning	A method of determining which ports on a network are open and could be receiving or sending data.
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.
Proxy Server	A server that filters and evaluates each internet address and request when a user accesses a file or opens a web page.
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.

Term	Definition
Requirement	Describes a condition or capability to which a system must conform, either derived directly from user needs, or stated in a contract, standard, specification, or other formally imposed document. A desired feature, property, or behavior of a system.
Retire	The act of taking a system or product out of service. The system may still be running but is no longer used by the business except for legacy or legal queries.
Risk	A potential event or condition that could have an impact or opportunity on the cost, schedule, business, or technical performance of an information technology investment, program, project, or organization.
Secure Access Digital Identity	Uses authentication when an individual attempting to access a protected resource has control of the specified authenticators/credentials. Security Access Digital Identity is a major system that provides a modern digital identity technology platform and capabilities to protect IRS public-facing applications.
Security Control	A safeguard or countermeasure prescribed for an information system, or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Risk Management Organization	An office within the Cybersecurity function that provides guidance and direction to the IRS enterprise-wide disaster recovery efforts as well as a comprehensive, business-centric information technology service continuity management program designed to protect IRS operations, assets, and information.
Server	A computer that carries out specific functions, <i>e.g.</i> , a file server stores files, a print server manages printers, and a network server stores and manages network traffic.
Software	A general term that consists of lines of code written by computer programmers that have been compiled into a computer program.
Solution	An implementation of people, processes, information, and technologies in a distinct system to support a set of business or technical capabilities that solve one or more business problems.
Spoofing	Packets which have a modified source address to either hide the identity of the sender, to impersonate another computer system, or both.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people.
System Owner	The agency official responsible for the overall development, integration, modification, and operation and maintenance of an information system.
Tax Ecosystem	A holistic look at the entire tax system, from the end-user workstation to filing the tax return and beyond.

Term	Definition
Unauthorized Access	The willful unauthorized access and inspection of taxpayer returns or return information.
Vulnerability	Weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten the network's security.
Website	A collection of web pages grouped together using the same domain name and operated by the same person or organization.
Zip File	A file that contains one or more compressed files.

Appendix III

Abbreviations

CDW	Compliance Data Warehouse
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
IPv6	Internet Protocol version 6
IRA	Inflation Reduction Act
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TIGTA	Treasury Inspector General for Tax Administration



**To report fraud, waste, or abuse,
contact our hotline on the web
at <https://www.tigta.gov/reportcrime-misconduct>.**

**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.