TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement

April 19, 2023

Report Number: 2023-25-017

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

HIGHLIGHTS: Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement

Final Audit Report issued on April 19, 2023 **Report Number 2023-25-017**

Why TIGTA Did This Audit

At the IRS, information technology resources outside of the Information Technology (IT) organization include hardware, software, information systems, and staff.

The Taxpayer First Act requires the Chief Information Officer (CIO) to oversee the development, implementation, and maintenance of information technology throughout the IRS; ensure that the information technology is secure and integrated; maintain operational control over the information technology; and act as the principal advocate for the IRS's information technology needs.

This audit was initiated to assess the efforts to manage hardware, software, information systems, and associated staff outside of the IT organization.

Impact on Tax Administration

Without effective controls and management oversight of all information technology resources, the IRS risks unnecessarily increasing the exposure of its information systems to potential malware and viruses; making less informed program decisions; using information technology resources inefficiently; and not complying with requirements. In addition, as stewards of taxpayer dollars, the IRS must ensure that it only pays for procured information technology products as authorized.

What TIGTA Found

The purchase of approximately $1.2 million in information technology products initiated by business units outside of the IT organization were not properly approved by IT organization management as required. Approximately $1 million in information technology product purchases were properly approved.

While the IT organization has procedures for hiring information technology staff outside of the IT organization, it does not have a process to ensure that inherently information technology-related work is not being performed. The IT organization is also unable to provide evidence of its oversight of 95 information systems managed by business units outside of the IT organization.

Although the IRS has written policy and procedures to mitigate unauthorized hardware, the detection and oversight of unauthorized hardware are not defined and documented. In addition, the IRS has procedures to manage unauthorized software, but the methodology used to manage unauthorized software needs improvement. The IRS excludes software executed fewer times than an established threshold from review. Applying this same criteria, a review of a March 2022 report 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. Software with low execution totals may pose a higher security risk because the software is less commonly known and used. Finally, performance metrics have not been developed to assess the team's effectiveness in managing unauthorized software.

What TIGTA Recommended

TIGTA made eight recommendations to the CIO. They include ensuring that: 1) the appropriate management official approves the purchase of information technology products; 2) inherently information technology-related work is clarified; 3) inherently information technology-related work is not performed by non-IT organization staff; 4) oversight of information systems not managed by the IT organization is documented; 5) procedures are updated to include and clarify stakeholders' defined roles and responsibilities in detecting, overseeing, and reviewing unauthorized hardware; 6) all unauthorized software are disabled; 7) unauthorized software standard operating procedures are updated; and 8) unauthorized software performance metrics are developed.

The IRS agreed with all eight recommendations. The Chief Procurement Officer plans to ensure that all information technology purchases are approved by the proper management official. The CIO plans to clarify inherently information technology-related work and develop controls to sanction use of information technology staff outside of the IT organization to not perform that work; establish a process to provide oversight of information systems managed by business units outside of the IT organization; and update the unauthorized hardware and software standard operating procedures.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

April 19, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement (Audit # 202220012)

This report presents the results of our review to assess the efforts to manage hardware, software, information systems, and associated staff outside of the Information Technology organization. This review is part of our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS [Internal Revenue Service] Resources*.

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

Table of Contents

Background

Information technology is constantly changing to meet new business requirements and evolving demands.[1] It often requires additional resources, including upgrades to, or new, hardware or software for applications and systems (hereafter collectively referred to as information systems) and additional staff. Tracking and monitoring changes to the information technology infrastructure are critical to effectively managing information systems and its supporting infrastructure as well as information technology staff who support the daily operations of the organization.

In July 2019, Congress enacted the Taxpayer First Act (TFA) to amend the Internal Revenue Code of 1986 to modernize and improve the Internal Revenue Service (IRS).[2] Specifically, the TFA aims to improve IRS operations and the administration of the tax laws by strengthening taxpayer rights, enhancing customer service, restructuring the organization, and advancing information technology. TFA § 2101, *Management of Internal Revenue Service Information Technology*, specifies that the IRS Commissioner and the Secretary of the Treasury will act through the Chief Information Officer (CIO) with respect to the development, implementation, and maintenance of the IRS's information technology. TFA § 2101 defines the CIO's roles and responsibilities and requires the CIO to:

1) Oversee the development, implementation, and maintenance of information technology throughout the IRS, including the Taxpayer Advocate Service, Criminal Investigation, and the Office of Chief Counsel.
2) Ensure that the information technology is secure and integrated.
3) Maintain operational control over the information technology.
4) Act as the principal advocate for the IRS's information technology needs.
5) Be aware of all information technology acquisitions throughout the IRS enterprise.

At the IRS, information technology resources managed outside of the Information Technology (IT) organization include hardware, software, information systems, and staff. The IRS maintains a list of all information systems in the As-Built Architecture. It is the authoritative source for the IRS's systems architecture and captures data attributes of each information system, including the business unit responsible for managing the system. The IRS also has a process in place in which the IT organization must approve the hiring of information technology staff outside of the IT organization and the staff only perform specific information technology-related work based on approved business needs. However, the IRS does not distinguish the program management between information technology resources, *e.g.*, hardware and software, managed directly by the IT organization or by business units outside of the IT organization.

In addition, two IRS organizations are primarily involved in the procurement of information technology products and services. Within the IT organization's Strategy and Planning function, Strategic Supplier Management manages information technology acquisitions and vendors.

[1] See Appendix IV for a glossary of terms.

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

According to the IRS, the primary goal of Strategic Supplier Management is to identify opportunities to improve information technology procurements. Within the Office of the Chief Procurement Officer, the Office of Information Technology Acquisitions plans, negotiates, executes, and manages the procurement of information technology products and services. It is also responsible for ensuring that the information technology procurement process is properly and efficiently managed, and is conducted with integrity, fairness, and openness.

Results of Review

Not All Information Technology Purchases Were Properly Approved

The procurement process includes acquisition planning to research whether the procurement meets the IRS's needs, 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.[3] 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 carts, totaling approximately $1.2 million, were not properly approved. None of the individuals who approved the 10 shopping carts were on the signature authority list.

* Dollar amounts are rounded.

The shopping cart approval chains were obtained from the Procurement for Public Sector application and signed between October 2020 and December 2021. All 17 shopping carts each had a total purchase of $500,000 and below and were requested by Criminal Investigation. 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*.

Internal Revenue Manual 2.21.1, *Shopping Cart Processing for Information Technology (IT) Products and Services, Introduction to Shopping Cart Processing for IT* (Feb. 2021), states that the appropriate Associate CIO must receive, review, and approve shopping carts containing information technology purchases initiated by a business unit outside of the IT organization. The signature authority cannot be re-delegated or assigned to acting managers. In addition, Delegation Order IT [Information Technology]-2-1-1, Revision 3, effective October 2018, states that the CIO has unlimited signature authority and can approve all shopping carts regardless of dollar value. The CIO can delegate the authority to the Deputy CIOs, Associate CIOs, and Deputy Associate CIOs. The delegation order also states that direct report executives and

[3] Each contract contained one shopping cart each for the purchase of hardware or software.

executive officers of the Associate CIOs and Deputy Associate CIOs have signature authority to approve shopping carts valued up to $500,000. Further, the *Shopping Cart Signature Authority List* outlines each level of funding authority (including delegations); it is updated monthly or whenever an IT organization management official change occurs.

Strategy and Planning function management stated that the 10 shopping carts were approved using a new approval process that was not yet finalized, specifically for Criminal Investigation. This new approval process requires the Criminal Investigation Director, instead of IT organization management, to approve the shopping carts. However, the Criminal Investigation Director did not approve the 10 shopping carts. In addition, while the individuals who approved the 10 shopping carts were IT organization personnel, they were not listed as approvers on the *Shopping Cart Signature Authority List;* and therefore, not authorized to approve them. We believe that this situation occurred because the shopping cart approval process did not include comparing the management official who signed and approved the shopping cart to the *Shopping Cart Signature Authority List* before the Office of the Chief Procurement Officer purchased the requested information technology products. As stewards of taxpayer dollars, the IRS must ensure that it only pays for procured information technology products as authorized.

Recommendation 1: The CIO should coordinate with the Chief Procurement Officer to ensure that the approval process includes a review that the appropriate management official approved the shopping cart prior to the purchase of information technology products.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Procurement Officer will ensure the authorized IT organization management official has reviewed and approved all shopping carts related to the acquisition of information technology goods and/or services. The CIO will provide an authorized signature list to the Office of the Chief Procurement Officer for this purpose and establish a process to maintain its currency.

Information Technology Resources Are Not Being Effectively Managed

The IT organization cannot ensure that information technology staff outside the IT organization are not performing inherently information technology-related work

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 Fiscal Years 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] 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. This is because IT organization 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.

In September 2020, the IRS's then Acting CIO issued CIO Memorandum, CIO-09200-0001, to all IRS heads of office outlining the procedures for filling positions in 10 information technology job series outside of the IT organization.[4] The procedures require business units outside of the IT organization to submit annual staff requests for approval. In addition to requesting the number of new information technology positions to be filled, the number of current information technology staff on-rolls must also be provided. Once the business unit head of office and the CIO have approved the staff request, the business unit shares the approved request with the Human Capital Office. Staffing specialists from the Human Capital Office work to ensure that the approved request is implemented as planned.

Besides outlining the procedures for hiring information technology staff outside of the IT organization, the CIO memorandum provides general areas of information technology-related work that should not be performed. The CIO memorandum states that:

> *It is imperative that no organization is perceived as trying to create a duplicative IT organization. Work related to the determination of information technology solutions, IT [information technology] investments, Cyber Security (protection of our systems), and technology products used in the IT organization is inherently IT and should not be staffed from within OUs outside of the IT organization.*

According to the Government Accountability Office's *Standards for Internal Control in the Federal Government* (Sept. 2014), management should design control activities, preventative or detective, in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, *i.e.*, CIO Memorandum, CIO-09200-0001. Management evaluates the purpose of the control activities and the effect a deficiency would have on the entity in achieving its objectives.

IT organization management does not have a control in place to ensure that information technology staff outside the IT organization are not performing inherently information technology-related work to meet the intent of 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 a proper control in place to monitor 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.

[4] The 10 information technology positions include the following General Schedule job series: 1) 0080 – Security Administration Series, 2) 0332 – Computer Operation Series, 3) 0335 – Computer Clerk and Assistant Series, 4) 0390 – Telecommunications Processing Series, 5) 0391 – Telecommunications Series, 6) 0392 – General Telecommunications Series, 7) 0394 – Communications Clerical Series, 8) 0854 – Computer Engineering Series, 9) 1550 – Computer Science Series, and 10) 2210 – Information Technology Management Series.

The CIO should:

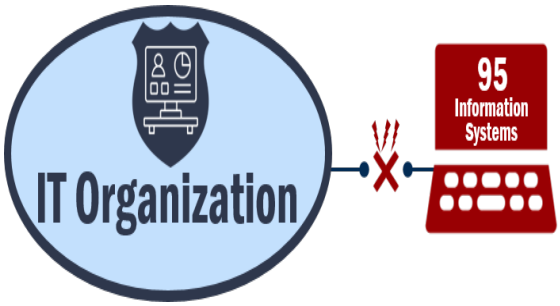
Recommendation 2: Provide clarification on the inherently information technology-related work that should not be performed by the information technology staff outside of the IT organization to the heads of the business units to ensure compliance with the CIO's memorandum.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will update or amend the current CIO Memorandum, CIO-09200-0001 in collaboration with internal stakeholders to clarify what inherently technology-related work should not be performed by information technology staff outside the IT organization.

Recommendation 3: Develop a control to ensure that the information technology staff outside of the IT organization are not performing inherently information technology-related work in accordance the CIO's memorandum.

> **Management's Response:** The IRS agreed with this recommendation. The CIO in collaboration with internal stakeholders will develop control measures to appropriately sanction use of information technology staff outside of the IT organization to not perform inherently technology-related work in accordance with the CIO Memorandum, CIO-09200-0001.

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.[5] 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 the 103 information systems and was unable to provide evidence of any oversight for the remaining 95 (92 percent) systems.

Internal Revenue Manual 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities* (Sept. 2022), states that the CIO shall provide executive leadership in information technology strategic and operational planning to achieve business goals by fostering innovation, prioritizing complex information technology initiatives, and directing the evaluation, deployment, and management of current and future information systems across the organization. The manual also states that the CIO shall provide leadership and high-level direction in the management of projects and plans involving highly complex, mission-critical

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

information systems, and business systems modernization projects in support of modernizing the Nation's tax system.

IT organization management does not have a process in place to ensure that their oversight of information systems managed by a business unit outside of the IT organization is documented. Without documented oversight of all information systems, the IRS is unable to demonstrate that it is complying with the TFA provision requiring the CIO to oversee the development, implementation, maintenance, and security as well as maintain operational control of information technology throughout the IRS.

Recommendation 4: The CIO should establish a process to ensure that oversight of information systems managed by business units outside of the IT organization is documented to support complying with the TFA.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will engage stakeholders to establish a process to provide oversight of information systems managed by business units outside the IT organization and ensure it is documented to comply with TFA.

Procedures for the detection and oversight of unauthorized hardware are not clearly defined and documented

The IRS has a written policy and standard operating procedures to mitigate unauthorized hardware on its network. However, the standard operating procedures do not document the procedures or define the stakeholders' roles and responsibilities for the detection and oversight of unauthorized hardware.

Internal Revenue Manual 10.8.55, *Information Technology (IT) Security, Network Security Policy* (May 2022) and the *Network Security Management Standard, Standard Operating Procedures* (Jan. 2020) create "…a network security standard that mandates all IRS asset stakeholders to be responsible and communicative when their assets are determined to be in violation, unidentified, or indicative of a threat to the IRS enterprise." The policy and standard operating procedures collectively provide for the mitigation of unauthorized hardware as a shared responsibility between the IT organization's User and Network Services and Cybersecurity functions. They also provide that the User and Network Services function's Network Monitoring Control Center (NMCC) oversees the monitoring of the IRS network for assessing all network risks, vulnerabilities, and violations.

The policy and standard operating procedures are initiated when unauthorized hardware is detected on the IRS network. Accordingly, the business unit that detects the unauthorized hardware completes a *Network Security Investigation* request form and submits it to the NMCC or the Cybersecurity function's Computer Security Incident Response Center (CSIRC) for review. However, the IRS did not document how a business unit becomes aware of unauthorized hardware. Ultimately, the NMCC or the CSIRC reviews the submitted evidence and assesses whether the unauthorized hardware should be approved or disapproved, or take additional action.

While the IRS did not document detailed procedures for business unit submissions received by the CSIRC, when the NMCC receives a submission, procedures show the NMCC opens a ticket in the Knowledge Incident/Problem Service Asset Management system to track the incident.

A NMCC analyst then reviews the investigation request form for completeness, verifies the information, and advises of any changes. Upon the NMCC's completion of the review, the investigation request form is e-mailed to the business unit requestor and the CSIRC for review.

The business unit requestor must provide evidence and current authorizations supporting that the hardware is allowed access to the IRS network. After approval or action taken, a summary and root cause analysis are conducted to complete the investigation request form. The NMCC opens another ticket in the Knowledge Incident/Problem Service Asset Management system to update the hardware information for asset management and the Internet Protocol address for network security tools. Finally, the completed investigation request form is documented and uploaded to the NMCC Security Management Standards SharePoint site.

Contrary to the policy and standard operating procedures that we identified, NMCC management stated that they provide only investigative assistance and that the CSIRC has the primary responsibility to identify, prevent, and assist in the resolution of cyber incidents and vulnerabilities, *e.g.*, unauthorized hardware. However, CSIRC management stated that they do not approve network connections for unauthorized hardware; they only assist the NMCC in the analysis and determination of whether an identified unauthorized hardware is compliant with IRS requirements.

Cybersecurity function personnel stated that they use a variety of security tools and data sources to determine whether a device is unauthorized to be on the IRS network. For example, they use an agentless security tool that continuously scans the network and dynamically identifies and evaluates hardware endpoints as they connect to the network. In addition, they collect data from the Knowledge Incident/Problem Service Asset Management system and a variety of other data sources. The collected data, along with the data collected from the security tool, are reported into a network, database, and analytics tool to determine whether hardware on the IRS network is unauthorized.

According to the *Standards for Internal Control in the Federal Government*, documentation is a necessary part of an effective internal control system and is required for the effective design, implementation, and operating effectiveness of an organization's internal control system. Management should also evaluate and document internal control issues and determine appropriate corrective actions for internal control deficiencies on a timely basis.

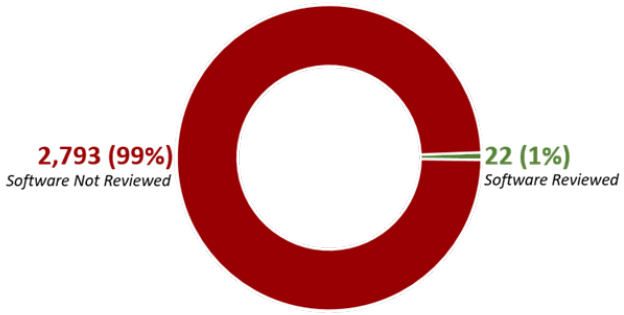
We attribute the IRS not having written procedures and defined roles and responsibilities for the detection of unauthorized hardware to a lack of management oversight, in which functional roles and responsibilities are decentralized and have not been adequately defined. Without written procedures, the IRS risks knowledge loss when skilled employees retire or leave the organization, and potential inefficiencies or ineffectiveness, *e.g.*, processing delays, when resolving unauthorized hardware issues because employees are not clear on their responsibilities.

Recommendation 5: The CIO should ensure that the *Network Security Management Standard, Standard Operating Procedures* are updated to include the procedures for stakeholders' defined roles and responsibilities in detecting and overseeing as well as to clarify the CSIRC's and NMCC's roles and responsibilities in reviewing unauthorized hardware.

Management's Response: The IRS agreed with this recommendation. The CIO will ensure that updates to the *Network Security Management Standard, Standard Operating Procedures* are made to enhance the descriptions on the roles and responsibilities for the User and Network Services process for detecting and overseeing unauthorized hardware.

Unauthorized software is not being effectively managed

Although the User and Network Services function's Application Control Solution (ACS) team has procedures to manage unauthorized software, the methodology used to manage unauthorized software needs improvement. The ACS team excludes software executed fewer times than an established threshold from review. We analyzed a March 2022 unauthorized software list by applying the same criteria used by the ACS team to sample and review unauthorized software that have been executed equal to or more times than an established threshold. We estimate that the ACS team would have reviewed a maximum of only 22 (1 percent) of 2,815 unauthorized software on the list. The remaining 2,793 (99 percent) unauthorized software would not have been reviewed. ACS team personnel acknowledged that software with low execution totals is not likely to be reviewed. The ACS team is staffed with three employees and they stated that it is impossible for them to review, research, and process all software shown on the unauthorized list. However, 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 ACS 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. If the software is on the approved list, the software has been previously reviewed and approved for use. If the software is on the blocked list, the software has been previously reviewed, not approved for use, and is disabled and blocked from further being used. 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). The unauthorized list is updated daily and maintains a running list of software for 30 calendar days from the date when the software was first executed. At the end of the 30 calendar days, the software is automatically deleted from the unauthorized list if the software is not executed again. The ACS team does not save the daily unauthorized list or maintain historical copies of it.

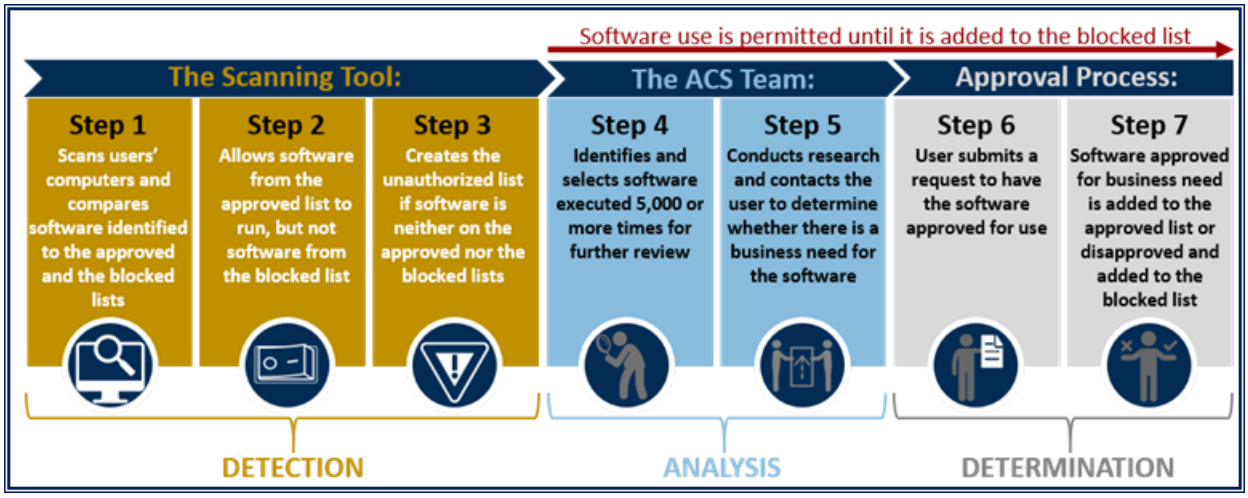
For software on the unauthorized list, the ACS team judgmentally selects software that has been executed equal to or more times than an established threshold for further review.[6] The ACS team reviews and compares the records created by the scanning tool to the:

- Enterprise Standards Profile database – It is the authoritative repository for IRS approved products and standards. It allows project owners and other stakeholders to select pre-approved information technology products and standards.
- Common Operating Environment database – It is a standardized, configured computer image on IRS computers integrated with a set of standard software to support the needs of all IRS employees.

Specifically, the ACS team reviews the software for information and use, such as software version; whether the software is vendor supported or unsupported, or retired; related software executable files; and whether the software is used by others users.[7]

The ACS team also contacts the user to determine whether there is a business need for the software. The user is allowed up to two weeks to respond, during which time the user is permitted to continue using the software. If the user does not respond or indicates there is not a business need, the software is added to the blocked list. If the user indicates there is a business need, the user then works with their business unit's Business Systems Planning office to submit a request for approval to use the software. 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. Figure 1 provides the process from identifying software being executed on users' computers, to reviewing the software, to approving or disapproving use of the software.

Figure 1: Software Identification, Review, and Approval Process



Source: Treasury Inspector General for Tax Administration's analysis of the software identification, review, and approval process.

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

[7] Executable files commonly have an EXE file extension. Software may have more than one executable file in its software package.

Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Sept. 2021), states that the IRS shall prohibit or restrict the use of any software that does not have a business need. It also requires that the IRS identify, disable, and remove software deemed unnecessary, unauthorized, or nonsecure. In addition, the manual requires that the IRS employ a deny-all, permit-by-exception policy for the use of software on information systems.

We attribute the issue of unauthorized software not being effectively managed to insufficient management oversight. In addition, the scanning tool has a capability limitation, *i.e.*, unauthorized software is deleted from the unauthorized list if not executed again after 30 calendar days, and its review process is manual and labor intensive. User and Network Services function management stated that they implemented the scanning tool as an interim tool until an enterprise-wide solution to software asset management is found. Cybersecurity function management stated that they plan to replace the software scanning tool with an application control product in Fiscal Year 2023. The application control product is expected to continuously monitor and record all endpoint and server activity to prevent, detect, and respond to cyberthreats that evade traditional security defenses.

We believe that the ACS team's procedures and methodology used to manage software from the unauthorized list is primarily focused on a business need rather than an information technology security perspective. 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.

The CIO should:

Recommendation 6: Disable all software on the unauthorized list and add them to the blocked list until the user can demonstrate a business need and has obtained approval for software use in accordance with requirements.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will disable the unauthorized software list policy after developing and enforcing a policy and process to move all software to either the blocked or the approved list in accordance with demonstrated business need and software approval requirements.

Recommendation 7: Update the *Application Control Solution Standard Operating Procedures* to reflect the deny-all, permit-by-exception policy for the use of software on information systems in alignment with requirements.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will update its *Application Control Solution Standard Operating Procedures* to reflect the implementation of the deny-all, allow-by-exception policy.

Performance metrics have not been developed

Performance metrics need to be developed to assess the ACS team's effectiveness to manage unauthorized software. The ACS team was unable to provide any measures of their performance because no performance metrics have been developed. As previously discussed, we estimate that the ACS team would have reviewed a maximum of only 22 (1 percent) of

2,815 unauthorized software on the list. The remaining 2,793 (99 percent) unauthorized software would not have been reviewed.

According to the *Standards for Internal Control in the Federal Government*, a performance metric is a means of evaluating an entity's performance in achieving objectives. The guidance states that management should establish activities to monitor the performance metrics. Activities may include comparisons and assessments relating different data sets to one another so that analyses of the relationships can be made and appropriate actions taken. In addition, Internal Revenue Manual 2.109.1, *Risk, Issue, and Action Item Management Practices – Risk, Issue, and Action Item Management Policy* (Apr. 2020), states that each program management office or equivalent function shall ensure that all program and project metrics for its organization are collected to determine the effectiveness of the items and contingency management activities. Internal Revenue Manual 2.109.2, *Risk, Issue, and Action Item Management Practices – Risk, Issue, and Action Item Management Process* (Apr. 2020), further states that the process will be reviewed regularly to ensure that it continues to support the business requirements of the enterprise. Performance metrics will be focused on providing relevant information as opposed to merely presenting raw data.

We attribute the issue of performance metrics not being developed to insufficient management oversight. Without established performance metrics, IRS management is unable to assess the ACS team's effectiveness to manage unauthorized software or make more informed program decisions.

Recommendation 8: The CIO should develop performance metrics to assess the ACS team's effectiveness in managing unauthorized software.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will develop and implement periodic performance metrics to assess its effectiveness in managing unauthorized software.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to assess the efforts to manage hardware, software, information systems, and associated staff outside of the IT organization. To accomplish our objective, we:

- Reviewed Federal and IRS policies, procedures, and guidance for managing the purchase and use of hardware and software, information systems, and associated staff outside of the IT organization.
- Determined whether the IT organization properly approved the purchase of information technology products initiated by business units outside of the IT organization by reviewing the approval chain for all 17 shopping carts from 17 contracts. The shopping carts were approved between October 2020 and December 2021 and obtained from the Procurement for Public Sector application. We also interviewed Strategy and Planning function management.
- Determined whether business units outside of the IT organization complied with the IT organization's staff request process by interviewing IT organization management and Human Capital Office personnel and reviewing all 20 staff requests submitted by business units for Fiscal Years 2021 and 2022.
- Determined whether the IT organization provided oversight of information systems managed by business units outside of the IT organization by obtaining a list of 103 active information systems not managed by the IT organization as of April 2022, interviewing IT organization management, and reviewing documentation.
- Determined whether appropriate steps were taken to approve, disable, or remove unauthorized hardware and software, and whether steps taken complied with Federal and IRS requirements by interviewing Cybersecurity and User and Network Services function personnel and reviewing documentation.

Performance of This Review

This review was performed with information obtained from the IT organization's Cybersecurity, Strategy and Planning, and User and Network Services functions located at the New Carrollton Federal Building in Lanham, Maryland, and the Office of the Chief Procurement Officer and the Human Capital Office located at IRS Headquarters in Washington, D.C., during the period January through November 2022. We conducted this performance audit 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 Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Louis Lee, Director; Catherine Sykes, Audit

Manager; Cindy Harris, Acting Audit Manager; Nicholas Reyes, Acting Audit Manager; Jason Rosenberg, Lead Auditor; and Kamelia Phillips, Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from the Procurement for Public Sector application. We evaluated the data by 1) reviewing existing information about the data and the systems that produced them; 2) performing electronic testing of required data elements, including that all fields requested were received and record counts equaled to what was expected; and 3) reviewing the data to detect obvious errors, duplicate values, and unexpected missing data. We determined that the data were sufficiently reliable for purposes of this report.

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. We determined that the following internal controls were relevant to our audit objective: the TFA; the Government Accountability Office's *Standards for Internal Control in the Federal Government*; and various Federal and IRS policies, procedures, and guidance related to the purchase of information technology products and the management of hardware, software, information systems, and associated staff outside of the IT organization. We evaluated these controls by interviewing Cybersecurity, Strategy and Planning, and User and Network Services function personnel as well as Human Capital Office personnel, and information technology personnel outside of the IT organization concerning the management over the purchase and use of hardware and software and information systems. We also reviewed relevant documentation.

Appendix II

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective action will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Protection of Resources – Potential; 10 purchases totaling $1,212,183 did not receive proper IT organization approval (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

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.[1] The shopping cart approval chains were obtained from the Procurement for Public Sector application and signed between October 2020 and December 2021. The appropriate IT organization management official, *e.g.*, Associate CIO, Deputy Associate CIO, authorized to approve a shopping cart is determined based upon the dollar value of the shopping cart and is listed in the *Shopping Cart Signature Authority List*. We determined that the appropriate IT organization management official did not properly approve 10 (59 percent) of 17 shopping carts, totaling $1,212,183.

[1] Each contract contained one shopping cart each for the purchase of hardware or software.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

March 20, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer
Tommy A. Smith
Digitally signed by Tommy A. Smith
Date: 2023.03.20 06:25:22 -04'00'

Todd A. Anthony
Chief Procurement Officer
Digitally signed by Todd A. Anthony
Date: 2023.03.17 10:53:51 -04'00'

SUBJECT: Draft Audit Report – Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement (Audit #202220012)

Thank you for the opportunity to review and comment on the subject draft audit report. At the IRS, the Chief Information Officer (CIO) oversees the development, implementation, and maintenance of information technology (IT) throughout the IRS, including offices outside the IT organization such as the Taxpayer Advocate Service, Criminal Investigation and the Office of Chief Counsel. The Chief Procurement Officer is responsible for planning, directing, coordinating and controlling the Procurement Program and maintaining the integrity of the procurement process for the IRS and other supported customer organizations.

The IRS has implemented internal controls and taken steps to strengthen the management and security of IT resources. For example, the CIO meets monthly with the leaders of IRS operating divisions and support functions to focus on the technology services and solutions needed to fulfill mission requirements. Furthermore, in compliance with the CIO's responsibilities under the Taxpayer First Act, at least once a year the IRS IT organization conducts a comprehensive review of IT activities conducted outside the IT organization to ensure proper oversight and management. We are also taking steps to ensure that the proper IT approval is documented for the purchase of IT resources and look forward to making further improvements in this area.

With regard to unauthorized software and hardware, the IRS has multi-layered controls in place to protect IRS assets and taxpayer data. This report presents opportunities to improve our documentation and standard operating procedures. However, we emphasize that the Treasury Inspector General for Tax Administration found no

evidence of unauthorized devices being able to successfully get on the IRS network as part of this audit.

As noted in this report, we have internal controls in place to ensure adherence to Federal and IRS policies, procedures and guidance related to the purchase of IT products and the management of hardware, software, information systems and associated staff outside of the IT organization. Although the results of this audit report have findings limited to a small portion of the technology portfolio and should not be used to project to the overall management of IRS IT resources, we will take action to further strengthen our internal controls. We agree with the audit team's recommendations and have enclosed a corrective action plan which will also address the related outcome measure.

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

Attachment

Attachment

Audit# 202220012, Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement

Recommendations

RECOMMENDATION 1: The Chief Information Officer should coordinate with the Chief Procurement Officer to ensure that the approval process includes a review that the appropriate management official approved the shopping cart prior to the purchase of information technology products.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Procurement Officer will ensure the authorized IT management official has reviewed and approved all shopping carts related to the acquisition of IT goods and/or services. The Chief Information Officer will provide an authorized signature list to the OCPO for this purpose and establish a process to maintain its currency.

IMPLEMENTATION DATE: March 15, 2024

RESPONSIBLE OFFICIAL(S): Chief Procurement Officer

RECOMMENDATION 2: The Chief Information Officer should provide clarification on the inherently information technology-related work that should not be performed by the information technology staff outside of the IT organization to the heads of the business units to ensure compliance with the CIO's memorandum.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will update or amend the current CIO Memorandum, CIO-09200-0001 in collaboration with internal stakeholders to clarify what inherently technology-related work should not be performed by information technology staff outside the IT organization.

IMPLEMENTATION DATE: February 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Strategy and Planning

Attachment

Audit# 202220012, Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement

RECOMMENDATION 3: The Chief Information Officer should develop a control to ensure that the information technology staff outside of the IT organization are not performing inherently information technology-related work in accordance the CIO's memorandum.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer in collaboration with internal stakeholders will develop control measures to appropriately sanction use of information technology staff outside of the IT organization to not perform inherently technology-related work in accordance with the CIO Memorandum, CIO-09200-0001.

IMPLEMENTATION DATE: February 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Strategy and Planning

RECOMMENDATION 4: The Chief Information Officer should establish a process to ensure that oversight of information systems managed by business units outside of the IT organization is documented to support complying with the TFA.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will engage stakeholders to establish a process to provide oversight of information systems managed by business units outside the IT organization and ensure it is documented to comply with TFA.

IMPLEMENTATION DATE: February 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Strategy and Planning

Attachment

Audit# 202220012, Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement

RECOMMENDATION 5: The Chief Information Officer should ensure that the *Network Security Management Standard, Standard Operating Procedures* are updated to include procedures for stakeholders' defined roles and responsibilities in detecting and overseeing as well as to clarify the CSIRC and NMCC's roles and responsibilities in reviewing unauthorized hardware.

CORRECTIVE ACTION 5: The IRS agrees with the recommendation. The Chief Information Officer will ensure that updates to the Network Security Management Standard, Standard Operating Procedures (SOP) are made to enhance the descriptions on the roles and responsibilities for the UNS process for detecting and overseeing unauthorized hardware.

IMPLEMENTATION DATE: October 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 6: The Chief Information Officer should disable all software on the unauthorized list and add them to the blocked list until the user can demonstrate a business need and has obtained approval for software use in accordance with requirements.

CORRECTIVE ACTION 6: The IRS agrees with this recommendation. The Chief Information Officer will disable the software Greylist policy after developing and enforcing a policy and process to move all software to either the Blacklist or Whitelist in accordance with demonstrated business need and software approval requirements..

IMPLEMENTATION DATE: April 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

Attachment

Audit# 202220012, Implementation of the Taxpayer First Act Provision Regarding the Management and Purchase of Information Technology Resources Needs Improvement

RECOMMENDATION 7: The Chief Information Officer should update the *Application Control Solution Standard Operating Procedures* to reflect the deny-all, permit-by-exception policy for the use of software on information systems in alignment with requirements.

CORRECTIVE ACTION 7: The IRS agrees with this recommendation. The Chief Information Officer will update its Application Control Solution (ACS) SOP to reflect the implementation of the deny-all, allow-by-exception policy.

IMPLEMENTATION DATE: December 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 8: The Chief Information Officer should develop performance metrics to assess the ACS team's effectiveness in managing unauthorized software.

CORRECTIVE ACTION 8: The IRS agrees with this recommendation. The Chief Information Officer will develop and implement periodic performance metrics to assess its effectiveness in managing unauthorized software.

IMPLEMENTATION DATE: December 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

Appendix IV

Glossary of Terms

Term	Definition
Business Unit	A title for IRS offices and organizations such as the IRS Independent Office of Appeals, Criminal Investigation, and Information Technology.
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.
Endpoint	A remote computing device that communicates back and forth with a network to which it is connected.
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.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency. The term information technology includes computers, ancillary equipment, software, firmware, services (including support services), and related resources.
Knowledge Incident/Problem Service Asset Management System	Maintains the complete inventory of information technology and non-information technology assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications and shares information with the Enterprise Service Desk.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the computer's data, applications, or operating system.
Metric	A standard of measurement.
Procurement for Public Sector Application	An application used by the IRS to request, fund, and award contracts; execute deliver orders; and verify receipt and acceptance of products and services as well as accrue procurement-related liabilities and process payments.
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.
Virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

Appendix V

Abbreviations

ACS	Application Control Solution
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Center
IRS	Internal Revenue Service
IT	Information Technology
NMCC	Network Monitoring Control Center
TFA	Taxpayer First Act

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

(800) 366-4484

By Web:

www.tigta.gov

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 23291

Washington, D.C. 20026

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