TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Adequately Documented and Effectively Implemented

June 12, 2024

Report Number: 2024-200-025

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

HIGHLIGHTS: Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Adequately Documented and Effectively Implemented

Final Audit Report issued on June 12, 2024 **Report Number 2024-200-025**

Why TIGTA Did This Audit

Internal control, which is synonymous with management control, is a major part of managing an organization. It is comprised of the plans, methods, and procedures used to meet an organization's mission, goals, and objectives, and in doing so, supports performance-based management.

This audit was initiated to determine whether corrective actions reported as closed by the Information Technology organization have been fully implemented, adequately documented, properly approved, and effectively corrected the identified deficiencies.

Impact on Tax Administration

Internal control serves as the first line of defense in safeguarding assets as well as preventing and detecting errors and fraud. When previously reported and agreed-to deficiencies are not adequately addressed, the IRS continues to be exposed to security vulnerabilities and exploits. In addition, by not addressing weaknesses and fully implementing corrective actions, realization of program benefits related to the management of taxpayer data and organizational improvements could be negatively affected. Further, without sufficient supporting documentation, there is limited evidence readily available to support that planned corrective actions were fully and effectively implemented.

What TIGTA Found

TIGTA selected a judgmental sample of 20 planned corrective actions (PCAs) from a population of 270 PCAs closed by the Information Technology organization during Fiscal Years 2019 through 2022. TIGTA selected PCAs that were considered higher risk and assessed the closure process and the effectiveness of the corrective actions taken. Reviews of all nine PCAs that were part of the judgmental sample and quality reviewed by the IRS determined that each of the PCAs obtained the required approval signatures and had sufficient documentation to support their closures.

In addition, reviews of the 20 closed PCAs determined that the IRS fully implemented 19 PCAs and did not fully and effectively implement and incorrectly closed one PCA involving high-risk [redacted] that were not remediated timely. Of the PCAs fully implemented, 16 were effective, including implementing alternative site processing. One PCA, involving older software versions running on the IRS network that did not have a Risk-Based Decision (RBD) or a Risk Acceptance Form and Tool (RAFT), was not effective. For the remaining two PCAs, TIGTA was unable to test the effectiveness of the corrective actions because the systems supporting the implementation of the PCAs were undergoing changes. Further, documentation provided for 18 of 20 PCAs supported the closure of the PCA, but the documentation for two PCAs did not.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer or the Chief Risk Officer should ensure that: 1) sufficient management oversight is provided to verify that the use of older software versions has an RBD or RAFT; 2) the Enterprise Standards Profile is updated with fields to track them; 3) [redacted] are remediated by the plan of action and milestones due date; 4) any documentation provided for PCAs that lacked sufficient documentation is uploaded to the Joint Audit Management Enterprise System; and 5) the Enterprise Audit Management organization evaluates sufficient documentation to demonstrate that corrective actions taken are fully implemented and that the documentation is uploaded to the Joint Audit Management Enterprise System prior to closing the PCA.

The IRS agreed with all five recommendations and plans to: 1) create a field to track the use of older software versions, along with their RBD or RAFT; 2) modify the Enterprise Standards Profile database to include RBD or RAFT information; 3) continue to address [redacted] by the plan of action and milestones dates; and 4) upload supporting documentation that was provided to TIGTA. In addition, the Enterprise Audit Management organization stated it has delivered detailed training to business units, created several job aids, and made updates to the closed PCA Quality Review process.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

June 12, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

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

SUBJECT: Final Audit Report – Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Adequately Documented and Effectively Implemented (Audit No.: 202320003)

This report presents the results of our review to determine whether corrective actions reported as closed by the Information Technology organization have been fully implemented, adequately documented, properly approved, and effectively corrected the identified deficiencies. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenge of *Protection of Taxpayer Data and IRS [Internal Revenue Service] Resources*.

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

Table of Contents

Appendices

Background

Internal control, which is synonymous with management control, is a major part of managing an organization.[1] It is comprised of the plans, methods, and procedures used to meet an organization's mission, goals, and objectives, and in doing so, supports performance-based management. Internal control also serves as the first line of defense in safeguarding assets as well as preventing and detecting errors and fraud. It helps Government program managers achieve desired results through effective stewardship of public resources. Systems of internal control provide reasonable assurance that the following objectives are being achieved: 1) effectiveness and efficiency of operations, 2) reliability of financial reporting, and 3) compliance with applicable laws and regulations.

The Joint Audit Management Enterprise System (JAMES) is the Department of the Treasury's web-based management controls database tracking system, and it is used to track audits, findings, and recommendations extracted from Government Accountability Office (GAO), Treasury Office of Inspector General, and Treasury Inspector General for Tax Administration (TIGTA) audit reports. The JAMES is also used to track the status of planned corrective actions (PCA) for material weaknesses, significant deficiencies, existing reportable conditions, remediation plans, and action plans. Tracking issues, findings, recommendations, and the status of PCAs resulting from audits is mandatory to comply with the intent of the GAO's standards for internal control, the Federal Managers Financial Integrity Act of 1982, Office of Management and Budget Circulars, and Department of the Treasury Directives.[2]

Within the Internal Revenue Service's (IRS) Office of the Chief Risk Officer, the Enterprise Audit Management (EAM) organization is responsible for an agency-wide approach to audit management. It provides oversight and policy related to the handling of GAO and TIGTA audits and audit responses as well as the post-audit tracking and monitoring of corrective action implementation. According to the EAM organization, it serves as the single point of contact for GAO and TIGTA audits to promote and support a collaborative, professional, and positive partnership with IRS oversight entities. The EAM organization's primary responsibilities include:

- Acting as the liaison between the IRS and GAO/TIGTA when addressing significant issues that arise during an audit.
- Providing guidance and support to business units on the audit process, including post audit tracking and monitoring of corrective actions.
- Monitoring the timeliness of IRS responses to ensure that due dates are met.
- Reviewing and approving PCAs for closure and business unit requests for extension of PCA due dates.

In addition, the EAM organization performs monthly quality reviews of closed PCAs. Monthly quality reviews validate that supporting documentation provided by the business units meets closure requirements. The quality reviews consist of a statistical sample of closed PCAs provided

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

[2] GAO, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014). 31 U.S.C. §§ 1105, 1113, and 3512 (2018).

by the Statistics of Income division each month. The EAM organization assigns a quality reviewer who performs an in-depth review of the actions taken and the documentation provided to determine whether they are sufficient to support the closure of the PCA. If the quality reviewer determines that the actions taken or the documentation provided for closure is not sufficient, the quality reviewer will request that the business unit take further action(s), which may include providing additional supporting documentation, clarifying the reported actions taken, or requesting additional action(s) to be taken. The quality reviewer records their findings and qualitative improvement comments on Form 14668, *IRS Quality Assurance Review of Closed Planned Corrective Action (PCA) Notification*.

JAMES business unit audit coordinators ensure that the status of action plans addressing material weaknesses and significant deficiencies are posted in the JAMES and PCAs are implemented timely. Their primary responsibilities include:

- Monitoring requests for closure, extensions, and status updates to ensure that the Form 13872, *Planned Corrective Action (PCA) Status Update*, provides appropriate data and comply with reporting requirements.
- Serving as the JAMES expert for their respective business unit.
- Providing additional information or documentation requested by the EAM organization.
- Resolving deficiencies and communicating results of EAM organization reviews with the appropriate business unit management.
- Updating the JAMES routinely on the status of open PCAs.

Results of Review

For our review, we selected a judgmental sample of 20 PCAs from a population of 270 PCAs closed by the Information Technology organization during Fiscal Years 2019 through 2022.[3] For the 20 closed PCAs, we assessed the closure process and the effectiveness of the corrective actions taken.[4] We selected PCAs that we considered of higher risk findings identified in prior TIGTA audit reports.

In addition, to assess the monthly quality review process, we reviewed all nine PCAs that were quality reviewed by the EAM organization and part of our judgmental sample of 20 closed PCAs. The result of our review agreed with the results of the EAM organization's quality review. Specifically, each PCA included a Form 13872 signed by the approving manager responsible for the implementation of the PCA, the JAMES business unit audit coordinator, and the approving executive or official responsible for the PCA as well as sufficient documentation to support the closure of the PCA.

[3] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population. Appendix III provides the report reference, the recommendation, and the PCA for each of the PCAs in the sample.

[4] Appendix III provides the results of our assessment of the PCAs.

The Majority of Closed Planned Corrective Actions Were Fully Implemented But Two Were Not Effective to Address Identified Deficiencies

Our analysis of the 20 closed PCAs determined that the IRS fully implemented 19 PCAs, leaving one PCA not fully and effectively implemented and incorrectly closed. In addition, our analysis determined that of the 19 PCAs fully implemented, 16 were effective and one PCA was not effective in correcting the identified deficiencies. For the remaining two PCAs, we were unable to assess the effectiveness of the corrective actions taken because the systems supporting the implementation of the PCAs were undergoing changes.

Planned Corrective Actions

- ✓ 1 NOT FULLY AND EFFECTIVELY IMPLEMENTED
- ✓ 19 FULLY IMPLEMENTED
  - ➢ 16 EFFECTIVE ◎
  - ➢ 1 INEFFECTIVE ⊗
  - ➢ 2 UNABLE TO TEST ▽

The following provides further details of our analysis related to the two PCAs that were not effective in correcting the identified deficiencies.

- **PCA Sample Number 7:** TIGTA originally found that the IRS was not effectively managing, controlling, and approving the use of older software versions, *i.e.*, sunset and archived/retired. The IRS stated that it will define a process to assess and document the risks, defined at the "major version" level, associated with the continued use of older software versions, and document the risks in a Risk-Based Decision (RBD).

  To support the closure of this PCA in September 2021, the IRS provided policies and guidance for a new Software Version Control SharePoint site used to assess and document the risk of using older software versions. The SharePoint site provides a *Software Version Control List* report that is generated semi-annually by the Strategy and Planning function's Strategic Management Support group. The report reconciles software running on the IRS network to the approved software listed in the Enterprise Standards Profile.

  The Enterprise Standards Profile is the official repository of software that the Enterprise Services function has reviewed and approved for use. The Enterprise Services function sends out a monthly e-mail to product stewards alerting them of software that will be sunset or retired within the next 180 calendar days. Product stewards are required to either accept and document the risk of using the older software version in a Risk Acceptance Form and Tool (RAFT) or ensure that an RBD is in place, or not accept the risk and request that the software be removed from use. The Cybersecurity function's Security Risk Management group is responsible for maintaining the RBDs, while the Office of the Chief Risk Officer's Enterprise Risk Management group is responsible for maintaining the RAFTs.

  The IRS was unable to provide RBDs or RAFTs for most of its older software versions currently running on the network. Based on our review of a March 2024 *Software Version Control List* report, we identified 939 (60 Tier 1 and 879 Tier 2 and 3) software with a "sunset," "beyond sunset," or "remove" status currently running on the IRS network.[5] The IRS was able to provide only three unique RBDs and RAFTs for the Tier 2 and 3 software.[6] For the remaining 936 software, the IRS was unable to provide an RBD or RAFT.

According to the Internal Revenue Manual (IRM), software identified as non-compliant requires product stewards to provide a plan to become compliant via upgrade, replacement, or removal from the IRS network, or request for the continued use of older software version via a RAFT.[7] In addition, the IRM provides that any exception to a system security policy requires that the Authorizing Official make an RBD.[8]

There is insufficient management oversight to ensure that risks associated with the use of older software versions are documented in an RBD or RAFT. In addition, the IRS does not have a centralized database to track and associate an RBD or RAFT with the use of older software versions. If systems are running older software versions and the risks are not properly assessed and documented, the IRS network may be exposed to vulnerabilities. Therefore, while this PCA was fully implemented, it was not effective in correcting the identified deficiency.

The Chief Information Officer (CIO) should ensure that:

Recommendation 1: Sufficient management oversight is provided to verify the use of older software versions is properly documented with an RBD or RAFT.

Management's Response: The IRS agreed with this recommendation. The CIO will create a field to track the use of older software versions, along with their associated RBD or RAFT.

Recommendation 2: The Enterprise Standards Profile is updated with fields to track the use of older software versions, along with their associated RBD or RAFT.

Management's Response: The IRS agreed with this recommendation. The CIO will modify the Enterprise Standards Profile database to include a field for RBD or RAFT information.

- **PCA Sample Number 12:** TIGTA originally found that the IRS did not remediate [redacted] timely based on agency-defined timelines to protect the confidentiality, integrity, and availability of the information system. The IRS stated that the Cybersecurity function has ensured that [redacted] were remediated timely based on agency-defined timelines.

  To support the closure of this PCA in November 2020, the IRS provided an updated [redacted] *Auditing* standard operating procedure (Aug. 2020) and a [redacted]

[5] Software with a "sunset" status is software within the last two years before its sunset end date, "beyond sunset" status is software with no end of life that has passed its sunset end date, and "remove" status is software not authorized for use.

[6] The IRS provided five RBDs and RAFTs. However, two software each had an RBD and RAFT. The IRS also provided an additional 28 RBDs and RAFTs for software not currently running on the IRS network.

[7] IRM 2.17.1 (Oct. 26, 2020).

[8] IRM 10.8.1.2 (1) (Dec. 12, 2023).

[redacted] *Desk Guide for Security Specialists* (Oct. 2020), but no evidence that vulnerabilities were remediated timely. During our current review, the Cybersecurity function provided vulnerability scans from May to September 2023 for the [redacted]. Our review of the vulnerability scans determined that [redacted] that have not been remediated within 60 calendar days. Specifically, we found that 14 (61 percent) of 23 [redacted] for the [redacted] that was not remediated within 60 calendar days.[9]

The [redacted] for the [redacted] are part of the [redacted], which is categorized as a high-risk system based on Federal security categorization standards.[10] The IRM states that high-risk vulnerabilities associated with high value assets should be remediated within 60 calendar days of discovery.[11] Generally, [redacted] are not a vendor supplied solution and may require additional time to create and test prior to deploying it into the production environment. As a result, the IRS created a plan of action and milestones with a completion date of October 2025, to remediate the outstanding high-risk [redacted]. When [redacted] are not remediated timely, the IRS's systems are vulnerable to exploitation by malicious actors. Therefore, this PCA was not fully and effectively implemented to correct the identified deficiency.

When previously reported and agreed-to deficiencies are not adequately addressed, the IRS continues to be exposed to security vulnerabilities and exploits. In addition, by not addressing weaknesses and fully implementing corrective actions, realization of program benefits related to the management of taxpayer data and organizational improvements could be negatively affected.

Recommendation 3: The CIO should ensure that [redacted] are remediated by the plan of action and milestones due date.

Management's Response: The IRS agreed with this recommendation. The CIO will continue to address the [redacted] in alignment with the defined plan of action and milestones dates.

[9] Our review of the vulnerability scans also identified one high-risk [redacted], but an RBD was created. Our review did not identify any high-risk [redacted].

[10] National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

[11] IRM 10.8.1.4.16.4.2 (1) (Dec. 12, 2023).

The Closure of Two Planned Corrective Actions Was Approved Without Sufficient Documentation

Using the same judgmental sample of 20 closed PCAs, our review found that all Forms 13872 were adequately completed; signed by the approving manager, JAMES business unit audit coordinator, and executive or official responsible for the PCA; and uploaded to the JAMES. However, our review also found that the documentation to support the closure of the PCAs was not always sufficient. Specifically, the documentation provided for 18 of 20 PCAs supported the closure of the PCA, but the documentation for two PCAs did not.

Planned Corrective Actions

✓ 18 of 20 Properly Approved

⊗ 2 Approved Without Sufficient Documentation

The following provides further details of our review of the two PCAs that were closed without sufficient documentation.

- **PCA Sample Number 4:** TIGTA originally found that the data at rest being transferred between the IRS and private collection agencies were not encrypted. The IRS stated that it will perform a feasibility study to determine the ability and possible solution to encrypt data files at rest inside the IRS's firewall before transmission and within the private collection agencies' systems. Based on the result of the feasibility study, the IRS will determine and approve the appropriate action needed to encrypt the data files while at rest.

  To support the closure of this PCA, the IRS uploaded the feasibility study that explored the options and solution to encrypt data files while at rest at the IRS and at the private collection agencies. However, the EAM organization prematurely closed this PCA in July 2019, when the encryption solution had not yet been selected and approved until February 2023. The EAM organization omitted that the PCA also included an action to select and approve the encryption solution prior to closing the PCA. Therefore, this PCA was closed without sufficient documentation.

- **PCA Sample Number 12:** TIGTA originally found that the IRS did not remediate [redacted] timely based on agency-defined timelines to protect the confidentiality, integrity, and availability of the information system. The IRS stated that the Cybersecurity function has ensured that the [redacted] were remediated timely based on agency-defined timelines.

  To support the closure of this PCA, the IRS provided an updated [redacted] *Auditing* standard operating procedure and a [redacted] *Desk Guide for Security Specialists*. However, the IRS did not provide any documentation to support that [redacted] were remediated timely based on agency-defined timelines.

  EAM organization management stated that their reviews focus on internal controls, such as policies and procedures. For this PCA, they focused on how the standard operating procedure and desk guide will help to ensure that [redacted] are remediated and not to ensure that vulnerabilities were remediated. However, this is contrary to the PCA. Therefore, this PCA was closed without sufficient documentation.

According to the GAO's standards for internal control, "Documentation is a necessary part of an effective internal control and is required for the effective design, implementation, and operating effectiveness of an entity's internal control system." The IRM requires that the action(s) taken addresses and agrees with the stated PCA, the PCA is fully implemented, and documentation supports the PCA closure and is uploaded to the JAMES.[12]

If the EAM organization does not have, request, and/or evaluate sufficient supporting documentation, there is limited evidence readily available to support that all PCAs were fully and effectively implemented.

The Chief Risk Officer should ensure that:

Recommendation 4: Any appropriate documentation subsequently provided during this review is uploaded to the JAMES for the judgmentally sampled PCAs that lacked sufficient documentation to support their closure.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Risk Officer will upload all supporting documentation provided to TIGTA in July and August 2023, with examples of encrypted data and files at rest and for transmission from the IRS to three private collection agencies.

Recommendation 5: The EAM organization evaluates sufficient testing documentation to demonstrate that corrective actions taken are fully implemented as stated in the PCA and ensures sufficient documentation is uploaded to the JAMES prior to approving PCA closures.

> **Management's Response:** The IRS agreed with this recommendation. Since 2020, the EAM organization has made significant progress in the overall review of PCAs. The EAM organization has delivered detailed training to the business units, created several job aids, and made stringent updates to the closed PCA Quality Review process. These actions have resulted in a reduction of the Quality Review Rework/Fail rate from 38.9 percent in 2020 to 1.67 percent in 2024.

[12] IRM 1.29.1 (July 15, 2022).

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether corrective actions reported as closed by the Information Technology organization have been fully implemented, adequately documented, properly approved, and effectively corrected the identified deficiencies. To accomplish our objective, we:

- Determined the processes used by the Information Technology organization and the Office of the Chief Risk Officer to ensure compliance with the requirements for closing PCAs by identifying and reviewing policies, procedures, and guidelines as well as interviewing EAM organization personnel related to the identification, tracking, and closing of PCAs and the PCA quality review process.
- Determined whether PCAs reported as closed have been fully implemented, adequately documented, properly approved, and effectively corrected the identified deficiencies by selecting a judgmental sample of 20 PCAs for review from a population of 270 PCAs reported as closed by the Information Technology organization during Fiscal Years 2019 through 2022.[1] The sample was selected to focus on those PCAs with a higher risk, emphasizing key controls, *e.g.*, asset management and disaster recovery, and potential risks, *e.g.*, risk management. We used a judgmental sample because we did not plan to project to the population.
- Assessed the EAM organization's quality review process by comparing the results of its quality reviews of nine closed PCAs that were part of our judgmental sample of closed PCAs to the result of our review.

Performance of This Review

This review was performed with information obtained from the Office of the Chief Risk Officer located in Washington, D.C., and the Information Technology organization located at the New Carrollton Federal Building in Lanham, Maryland, during the period May 2023 through March 2024. 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; Kenneth Bensman, Audit Manager; Jason Rosenberg, Acting Audit Manager; Denis Danilin, Lead Auditor; and Benedict Kim, Senior Auditor.

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

Data Validation Methodology

We validated that the JAMES data for our judgmental sample of 20 PCAs was accurate and complete by completing a data reliability assessment. The data reliability assessment included reviews of related supporting documentation, data reports in JAMES, and interviews with knowledgeable agency officials. 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 GAO's standards for internal control and the IRM, as well as various IRS policies, procedures, and guidelines for managing and ensuring the proper closure of PCAs. We evaluated these controls by interviewing Information Technology organization and Office of the Chief Risk Officer personnel, reviewing guidance for managing PCA closures and the quality review process, reviewing documents supporting the closures of the PCAs and the quality reviews of PCAs, and independently assessing the PCA closure process.

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; two closed PCAs that were not effectively implemented and/or fully implemented and did not meet information technology security requirements (see Recommendations 1 through 3).

Methodology Used to Measure the Reported Benefit:

We reviewed a judgmental sample of 20 higher risk closed PCAs and their related supporting documentation.[1] We found that two PCAs were not effectively implemented and/or fully implemented because they did not meet information technology security requirements.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; two PCAs closed as implemented had insufficient documentation recorded in the JAMES to support their closures (see Recommendations 4 and 5).

Methodology Used to Measure the Reported Benefit:

Using the same judgmental sample of 20 higher risk closed PCAs previously mentioned, we found that two of the PCAs had insufficient documentation recorded in the JAMES to support their closures.

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

Appendix III

Assessment of Closed Information Technology Organization Planned Corrective Actions

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
TIGTA, Report No. 2016-20-075, *Information Technology: SharePoint Controls Need Improvement to Mitigate Risks and to Ensure That Possible Duplicate Costs Are Avoided* (Sept. 2016).				
1	PCA 1-1-1	The CIO should ensure that an automated tool is identified, deployed, and routinely executed to identify SharePoint sites containing Personally Identifiable Information and Sensitive But Unclassified data.	The IRS ensured that an automated tool was identified, deployed, and executed to identify SharePoint sites containing Personally Identifiable Information or Sensitive But Unclassified data. PCA closed: October 15, 2019	**Fully Implemented – Effectiveness Not Applicable** The IRS initially closed this PCA in October 2016 with the implementation of a tool to identify SharePoint sites containing Personally Identifiable Information and Sensitive But Unclassified data. However, this tool was found to be ineffective. This PCA was reopened to implement a new tool. We could not test the effectiveness of this PCA because the IRS is performing functional testing and monitoring of the new tool to assess its performance.
TIGTA, Report No. 2018-20-029, *Security Over High Value Assets Should Be Strengthened* (May 2018).				
2	PCA 1-1-1	The CIO should implement the Office of Management and Budget Cybersecurity Strategy and Implementation Plan actions to identify and document current system hardware components for all IRS high value assets.	The Cybersecurity function will continue efforts already underway to identify and document current system hardware for IRS information systems including high value assets. PCA closed: March 4, 2021	**Fully Implemented – Effective** The IRS created a dashboard to provide information on hardware components of high value assets. We reviewed screenshots from a network traffic, database, and analytics tool from September 2023 that documents hardware components for information systems, including high value assets.

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
3	PCA 1-4-1	The CIO should direct the Enterprise Operations function to ensure that patching of security vulnerabilities is completed within the required 30-calendar-day time frame.	The Enterprise Operations function will complete the approved patch management process to ensure patching of security vulnerabilities is completed within the required IRM time frame. PCA closed: December 4, 2018	**Fully Implemented – Effective** TIGTA originally found that vulnerabilities were not patched timely for Integrated Data Retrieval System servers in the Tier 2 environment. The IRS provided evidence that vulnerabilities were patched timely during Fiscal Year 2023 for Integrated Data Retrieval System servers in the Tier 2 environment.
TIGTA, Report No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).				
4	PCA 3-1-1	The CIO should ensure that the data at rest being transferred to the private collection agencies are encrypted at the IRS and at the private collection agency.	The IRS will perform a feasibility study to determine the ability and possible solution to encrypt files at rest inside the firewall before being sent to Secure Data Transfer services for transmission between the IRS and the private collection agencies. Based on those findings, the IRS will determine the appropriate action needed. Any approved actions will also include options for ensuring that the private collection agencies maintain the encrypted data at rest within their systems. PCA closed: July 26, 2019	**Fully Implemented after PCA closure – Effective** The IRS performed a feasibility study to identify a solution to encrypt files at rest inside the firewall before being sent for transmission between the IRS and the private collection agencies. However, this PCA was closed prior to selecting the encryption solution. In August and September 2023, the IRS provided examples of encrypted data and files at rest at the IRS and at three private collection agencies.

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
TIGTA, Report No. 2018-20-045, *Information Technology Investment Management Controls Should Be Better Aligned With the Federal Information Technology Acquisition Reform Act of 2014* (July 2018).[1]				
5	PCA 1-1-1	The CIO should comply with the Department of the Treasury's Federal Information Technology Acquisition Reform Act guidance, which delegates to the IRS CIO responsibility for reviewing the acquisition and contract sections in IRS business cases.	The IRS will establish a process to comply with the Department of the Treasury's Federal Information Technology Acquisition Reform Act assignment guidance. PCA closed: May 23, 2019	**Fully Implemented – Effective** The IRS issued Delegation Order IT [Information Technology]-2-1-2, *Authority to Approve Acquisition Plans* (June 2019), authorizing the CIO to approve acquisition plans between $50 and $68 million and to delegate approval authority for acquisition plans less than $50 million. We reviewed 10 acquisition plans prepared from October 2019 through April 2023 and they were all signed by the appropriate approver.
TIGTA, Report No. 2019-20-008, *The Solaris to Linux Migration Project Was Delayed and Needs Improved Governance* (Dec. 2018).				
6	PCA 2-1-1	The CIO should implement the Linux Migration Project's planned disaster recovery and business continuity strategy utilizing alternate site processing.	The alternate site processing was implemented as of August 2018. In addition, disaster recovery has been successfully tested annually for the last two years. PCA closed: April 15, 2019	**Fully Implemented – Effective** The IRS provided evidence that alternate site processing and disaster recovery testing were performed during Fiscal Years 2022 and 2023.

[1] Pub. L. No. 113-291, Title VIII, Subtitle D.

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
TIGTA, Report No. 2019-20-031, *Software Version Control Management Needs Improvement* (June 2019).				
7	PCA 1-5-1	The CIO should document and approve risk acceptance to continue using older versions of software, *i.e.*, sunset, archived/retired.	The IRS will define a process to assess and document risk(s) associated with the continued use of older versions of software. Risks will be assessed at the "major version" level as identified by a given publisher, and an RBD will be documented. PCA closed: September 21, 2021	**Fully Implemented – Not Effective** The IRS created a new Software Version Control SharePoint site to assess and document the risk of using older software versions. However, the IRS was unable to provide RBDs or RAFTs for most of its older software versions currently running on the network.
TIGTA, Report No. 2019-20-046, *The Bring Your Own Device Program's Security Controls Need Improvement* (Sept. 2019).				
8	PCA 2-1-1	The CIO should ensure that the IRM requirement is met, and vulnerabilities found on Bring Your Own Device servers are timely remediated.	Following the audit, IRS officials completed an analysis on the vulnerability reports and took immediate actions to confirm remediation on several findings. The IRS will continue to monitor vulnerabilities on the Bring Your Own Device system and deploy remediations in accordance with the IRM requirement. PCA closed: November 14, 2019	**Fully Implemented – Effective** In June 2023, the Bring Your Own Device program transitioned from on-premises servers to a Software-as-a-Service through a cloud service provider. We confirmed that the IRS has been performing continuous monitoring security reviews and sending the results of the reviews to the Authorizing Office as required.
TIGTA, Report No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019).				
9	PCA 1-3-1	The CIO and the Chief, Criminal Investigation, should conduct periodic firewall administrator account audits in accordance with agency policies and procedures.	The IRS will conduct periodic audits of firewall administrator accounts in accordance with agency policies and procedures. PCA closed: September 22, 2020	**Fully Implemented – Effective** The IRS provided three reports of firewall administrator account audits performed during Fiscal Year 2023. These audits ensure that firewall administrators are authorized to have access and have matching entitlements in the Business Entitlement Access Request System.

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
TIGTA, Report No. 2020-20-006, *Active Directory Oversight Needs Improvement* (Feb. 2020).				
10	PCA 2-7-1	The CIO should ensure that service account passwords are appropriately configured to expire.	The CIO will ensure that service account passwords are appropriately configured to expire. PCA closed: November 5, 2020	**Fully Implemented – Effective** The IRS provided evidence that the passwords for seven service accounts, active as of August 2023, on a Windows server are appropriately configured to expire.
TIGTA, Report No. 2020-20-036, *Strategies and Protocols to Authenticate Network User Identities Are Effective; However, More Action Is Needed to Verify the Identity of Devices* (Aug. 2020).				
11	PCA 1-2-1	The CIO should ensure that the User and Network Services function configures and implements certificate-based authentication for devices connecting wirelessly to the internal network.	The IRS will complete the work already in progress to implement certificate-based authentication for devices connecting wirelessly to its network. PCA closed: January 28, 2021	**Fully Implemented – Effective** The IRS provided evidence that devices connected wirelessly to its network (as of August 2023) at the enterprise computing centers have certificate-based authentication.
[redacted]				
12	PCA 1-3-1	The CIO should ensure that the [redacted] are timely remediated based on agency-defined timelines to protect the confidentiality, integrity, and availability of the information system.	The Cybersecurity function has ensured that the [redacted], were timely remediated based on agency-defined timelines to protect the confidentiality, integrity, and availability of the information system. PCA closed: November 10, 2020	**Not Fully Implemented – Not Effective** A review of vulnerability scans from May to September 2023 found that 14 of 23 [redacted] not remediated within 60 calendar days.

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
13	PCA 3-1-1	The CIO should develop and approve an RBD for deviating from the IRM, which requires [redacted] computers to automatically update malicious code protection mechanisms and configure these mechanisms to perform weekly scans of the information system.	The Enterprise Operations function will work with Cybersecurity Architecture and Implementation Architect, and Engineering Advisory Security Policy in submitting an RBD with the Authorizing Official. PCA closed: October 21, 2020	**Fully Implemented – Effective** In June 2023, the IRS updated an RBD dated August 2020 to deviate from requirements that [redacted] computers automatically update malicious code protection mechanisms and configure these mechanisms to perform weekly scans of the information system. The IRS stated that [redacted] to provide malicious code protection and reporting.
TIGTA, Report No. 2020-20-063, *Improvements Are Needed to Ensure That Wireless Networks Are Secure* (Sept. 2020).				
14	PCA 2-2-1	The CIO should update the internal procedures to provide detailed requirements for reviews and updates to the wireless access point inventory, including taking photographs of devices during the deployment and replacement stages.	The IRS will update internal procedures for access point deployment and replacement and inventory management, including guidance for taking photographs typical of wireless access point deployments. PCA closed: May 27, 2021	**Fully Implemented – Effective** The IRS provided an updated standard operating procedure detailing requirements for access point deployment and replacement and inventory management, including taking photographs of devices during the deployment and replacement stages. The IRS also provided pictures of the five wireless access points deployed in August and September 2021.

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
TIGTA, Report No. 2021-20-024, *Improvements Are Needed to More Effectively Manage and Secure the Virtual Host Infrastructure Platform* (June 2021).				
15	PCA 3-2-1	The CIO should implement automated audit logging and monitoring and establish a review process for VMware servers in the virtual host infrastructure platform.	The Enterprise Operations function will work with the Cybersecurity function to establish a new real-time monitoring process with data ingestion into the Continuous Diagnostics and Mitigation Program. PCA closed: June 2, 2022	**Fully Implemented – Effective** The IRS provided a September 2023 quarterly server monitoring report identifying potential unauthorized accesses. Our review of the report did not identify any unauthorized accesses.
16	PCA 4-2-1	The CIO should ensure that standard operating procedures are followed to properly decommission virtual host infrastructure platform servers.	The Associate CIO, Enterprise Operations, will ensure that the IRS follows standard operating procedures provided by the Technology Implementation Services Office for properly decommissioning virtual host infrastructure platform servers. PCA closed: August 23, 2022	**Fully Implemented – Effectiveness Not Applicable** The IRS provided two Fiscal Year 2022 change requests to decommission virtual host infrastructure platform servers to close this PCA. We could not test the effectiveness of this PCA because the IRS is in the process of transitioning from the Knowledge Incident/Problem Service Asset Management system to ServiceNow.
TIGTA, Report No. 2021-20-056, *Laptop and Desktop Sanitization Practices Need Improvement* (Sept. 2021).				
17	PCA 2-1-1	The CIO should ensure that steps are taken to degauss or destroy hard disks identified during this review that were not sanitized or had bad sector errors.	The CIO will degauss or destroy hard disks identified during this TIGTA review, which were not sanitized or had bad sector errors. PCA closed: October 28, 2021	**Fully Implemented – Effective** The IRS degaussed seven of nine workstations (two workstations did not have hard drives) and prepared all nine workstations for retirement and disposal via a Form SF-120, *Report of Excess Personal Property*.

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
TIGTA, Report No. 2021-20-063, *Enterprise Linux Platform Management Needs Improvement* (Sept. 2021).				
18	PCA 1-2-1	The CIO should ensure that the Enterprise Linux Platform's servers are effectively defined to improve the accuracy and completeness of the data reported to the official inventory repository.	The Associate CIO, Enterprise Operations, will ensure that the official inventory is accurate and complete and implement inventory verification controls to improve the accuracy and integrity of the data that define the server environment data reported to the official inventory repository. PCA closed: August 19, 2022	**Fully Implemented – Effective** From a January 2024 inventory report of Enterprise Linux Platform servers, the IRS provided evidence that virtual and physical servers not listed on the report have been retired or were not associated with the platform.
TIGTA, Report No. 2021-25-025, *Taxpayer First Act: Data Security in the Identity Theft Tax Refund Fraud Information Sharing And Analysis Center* (May 2021).				
19	PCA 1-1-1	The CIO should ensure that the appropriate updates are installed to timely remediate the critical and high-risk vulnerabilities identified on the servers that temporarily store Federal Tax Information and those that are used as backup servers to transmit Federal Tax Information to the Trusted Third Party.	The Enterprise Operations function will ensure that the critical and high-risk vulnerabilities identified on the servers that store Federal Tax Information and those that are used as backup servers to transmit Federal Tax Information to the Trusted Third Party are updated and remediated by installing the appropriate updates. PCA closed: August 12, 2021	**Fully Implemented – Effective** Our review of a *Patching Automation Log* report of eight servers storing Federal Tax Information from July 2022 through August 2023 determined that all 24 high-risk (no critical) vulnerabilities were remediated timely or accounted for in a plan of action and milestones.

PCA Sample Number	PCA Number	Recommendation	PCA	TIGTA's Assessment of Corrective Action
TIGTA, Report No. 2022-20-006, *Vulnerability Scanning and Remediation Processes Need Improvement* (Dec. 2021).				
20	PCA 3-1-1	The CIO should enforce current guidance to conduct periodic reviews of the scanning exception list to ensure that vulnerability scanning exceptions are properly documented and devices lacking required documentation are added back to the vulnerability scanning footprint as required.	The Information Technology organization will enforce current guidance to conduct periodic reviews of the scanning exception list to ensure that vulnerability scanning exceptions are properly documented and devices lacking the required documentation are added back to the vulnerability scanning footprint. PCA closed: February 25, 2022	**Fully Implemented – Effective** The IRS updated its *Enterprise Vulnerability Scanning Managing Exceptions in Vulnerability Scans Standard Operation Procedure* (Feb. 2022) to include a process for conducting monthly reviews of the scanning exception list. Review meetings are held when vulnerability scanning exceptions are identified. Cybersecurity function management provided evidence that review meetings were scheduled for January through August 2023. However, no new requests were received to be added to the vulnerability scanning exception list and therefore, no review meeting was needed or held.

Appendix IV

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

May 17, 2024

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Rajiv Uppal,
Chief Information Officer

Rajiv K. Uppal

Digitally signed by Rajiv K. Uppal
Date: 2024.05.17 16:57:30 -04'00'

SUBJECT: Draft Audit Report – Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Adequately Documented and Effectively Implemented (Audit #202320003)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. We appreciate the Treasury Inspector General for Tax Administration's (TIGTA's) recognition and validation that Enterprise Audit Management's quality review process is successful in ensuring corrective actions are closed in a timely manner. We also appreciate your recognition that the IRS achieved a 95% implementation rate for tested high-risk corrective actions. We concur with TIGTA's statement in the report that systems of internal control provide reasonable assurance that organizational objectives are achieved while helping government program managers effectively manage public resources.

The IRS is committed to fully and effectively implement and document all agreed upon corrective actions. The IRS's Enterprise Audit Management **organization** has instituted regular process reviews that ensure agreed upon corrective actions are implemented in a timely manner and will continue to conduct rigorous post-implementation reviews to ensure these actions are sustained.

We agree with TIGTA's recommendations and have already begun responding. Our corrective action plan for the five recommendations and two outcome measures identified in the report is attached. Staying on top of potential security threats is of the utmost importance to the IRS, particularly regarding taxpayer data.

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 Russel Rexroat, Director of Business Planning and Risk Management, at (703) 999-7131.

Attachment

Attachment

Audit# 202320003, *Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Adequately Documented and Effectively Implemented*

Recommendations

RECOMMENDATION 1: The Chief Information Officer (CIO) should ensure that sufficient management oversight is provided to verify the use of older software versions is properly documented with a RBD or RAFT.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will create a field to track the use of older software versions, along with their associated RBD or RAFT.

IMPLEMENTATION DATE: October 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Services

RECOMMENDATION 2: The CIO should ensure that the Enterprise Standards Profile is updated with fields to track the use of older software versions, along with their associated RBD or RAFT.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will modify the Enterprise Standards Profile (ESP) database to include a field for RBD or RAFT information.

IMPLEMENTATION DATE: October 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Services

RECOMMENDATION 3: The CIO should ensure that [redacted] are remediated by the plan of action and milestones due date.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will continue to address the [redacted] in alignment with the defined POAM dates.

IMPLEMENTATION DATE: December 15, 2025

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations

Attachment

Audit# 202320003, *Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Adequately Documented and Effectively Implemented*

RECOMMENDATION 4: The Chief Risk Officer should ensure that any appropriate documentation subsequently provided during this review is uploaded to the JAMES for the judgmentally sampled PCAs that lacked sufficient documentation to support their closure.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Risk Officer will upload all supporting documentation provided to TIGTA in July and August 2023, with examples of encrypted data and files at rest and for transmission from the IRS to three private collection agencies.

IMPLEMENTATION DATE: August 15, 2024

RESPONSIBLE OFFICIAL(S): Director, Enterprise Audit Management

RECOMMENDATION 5: The EAM organization evaluates sufficient testing documentation to demonstrate that corrective actions taken are fully implemented as stated in the PCA and ensures sufficient documentation is uploaded to the JAMES prior to approving PCA closures.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. Since 2020, EAM has made significant progress in our overall review of planned corrective actions. We have delivered detailed training to the business units, created several job aids, and made stringent updates to the closed PCA Quality Review process. These actions have resulted in a reduction of the Quality Review Rework/Fail rate from 38.9% in 2020 to 1.67% in 2024. Having a decreasing fail rate has demonstrated that sufficient documentation is being evaluated and uploaded to the JAMES prior to approving the PCA closures.

IMPLEMENTATION DATE: Implemented

RESPONSIBLE OFFICIAL(S): Director, Enterprise Audit Management

Appendix V

Glossary of Terms

Term	Definition
Alternate Site Processing	Involves moving production processing from one Enterprise Computing Center to the other Enterprise Computing Center using replication and gridding (virtual tape) technologies.
Bring Your Own Device	IRS program to allow its employees to access work resources using their personal mobile devices.
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.
Certificate-Based Authentication	An encrypted method that enables devices and people to identify themselves to other devices and systems.
Cloud Service Provider	A third-party company offering a cloud-based platform, infrastructure, application, or storage services.
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.
Cybersecurity Function	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing the confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Enterprise Audit Management Organization	The Office of the Chief Risk Officer oversees the EAM organization. The EAM organization provides an agency-wide approach to audit management, providing oversight and policy related to handling GAO and TIGTA audits and audit responses as well as post-audit tracking and monitoring of corrective action implementation.
Enterprise Standards Profile	The authoritative repository for IRS-approved products and standards. The Enterprise Standards Profile allows project owners and other stakeholders to select preapproved technology products and standards. Development teams should determine which standards and approved products apply to their areas of responsibility. Listings in the Enterprise Standards Profile include guidance for usage that should be reviewed for useful, relevant information.

Term	Definition
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.
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.
High Value Asset	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical Federal operations or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Integrated Data Retrieval System	IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.
Joint Audit Management Enterprise System	The Department of the Treasury 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 PCAs from audit reports issued by oversight agencies, such as TIGTA.
Knowledge Incident/Problem Service Asset Management System	An application that maintains the complete IRS 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.
[redacted]	[redacted].
Partition	A logical portion of a media that functions as though it were physically separate from other logical portions of the media.
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.

Term	Definition
Private Collection Agency	A private company that specializes in collecting overdue (delinquent) debts from individuals and businesses. The Fixing America's Surface Transportation Act, signed into law December 4, 2015, requires the IRS to use private collection agencies for the collection of certain past due modules defined as inactive tax receivables.[1]
Risk Acceptance Form and Tool	Used to support risk response after a risk has been identified by structuring and documenting a formal business decision to accept a significant risk. The tool helps business units analyze and document the decision to accept a risk by capturing options considered, the rationale used and the final decision that is being made and accepted.
Risk-Based Decision	An approved decision for any accepted change to an operating system, database, web technology or application that causes that system to be out of compliance with the established security configuration.
Server	A computer that carries out specific functions, *e.g.*, a file server stores files, a print server manages printers, and a network server stores and manages network traffic.
ServiceNow	A state-of-the-art, cloud-based enterprise service management system that streamlines and automates routine workflows, centralizes data sources, and unites business functions across an agency.
Software	A general term that describes computer programs and consists of lines of code written by computer programmers that have been compiled into a computer program.
Software Version Control List	A report comparing software running on the IRS enterprise network to approved software applications listed on the Enterprise Standards Profile.
Statistics of Income Division	Its mission is to collect, analyze, and disseminate information on Federal taxation for the Department of the Treasury's Office of Tax Analysis, Congressional committees, the IRS in its administration of the tax laws, other organizations engaged in economic and financial analysis, and the general public.
Trusted Third Party	External organizations that work with the IRS, *e.g.*, tax preparers, financial institutions, banks, including providing third parties with access to taxpayer data.
Vulnerability Scanning	The process of proactively identifying vulnerabilities of an information system to determine if and where a system can be exploited or threatened. The process 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.
[redacted]	[redacted]

[1] Pub L. No. 114-94, 129 Stat. 1312.

Term	Definition
[redacted]	[redacted]
[redacted]	[redacted]

Appendix VI

Abbreviations

CIO	Chief Information Officer
EAM	Enterprise Audit Management
GAO	Government Accountability Office
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
JAMES	Joint Audit Management Enterprise System
PCA	Planned Corrective Action
RAFT	Risk Acceptance Form and Tool
RBD	Risk-Based Decision
TIGTA	Treasury Inspector General for Tax Administration

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

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

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