TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

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

June 1, 2020

Reference Number: 2020-20-022

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

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

Final Audit Report issued on June 1, 2020
Reference Number 2020-20-022

Why TIGTA Did This Audit

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

Impact on Taxpayers

Internal controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are being achieved. Internal controls protect assets, detect errors, and prevent fraud. The IRS continues to be exposed to security vulnerabilities by not adequately addressing previously reported and agreed-to deficiencies in its internal control environment. 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.

What TIGTA Found

TIGTA selected a judgmental sample of 24 planned corrective actions (PCA) from a population of 83 PCAs closed as implemented or canceled by the Information Technology organization during Fiscal Years 2017 and 2018. Of the 24 PCAs, TIGTA selected 15 higher risk PCAs closed as implemented to assess the closure process and the effectiveness of the corrective actions taken. TIGTA also selected all nine PCAs closed as canceled during this time frame to assess the closure process for canceling these PCAs.

Our review of the nine PCAs closed as canceled determined that they were properly approved and adequately documented as required. In addition, our review determined that the IRS fully implemented 11 of the 15 PCAs reported as closed. Of these 11 PCAs, seven were effective in correcting their identified deficiencies. TIGTA was unable to test for effectiveness for the remaining four PCAs due to the nature of the corrective actions, such as conducting a feasibility analysis, updating the methodology section of a document, *etc.*

However, TIGTA also determined that the IRS did not fully implement four of the 15 closed PCAs (*e.g.*, implement mitigating controls for **********2********** and apply timely patches to some file transfer servers), resulting in the corrective actions taken not being fully effective. In addition, the IRS did not upload sufficient documentation (*e.g.*, authorization and annual validation of ***2*** ****2**** and audit trails capturing necessary security information) to the Joint Audit Management Enterprise System (JAMES) to fully support the proper closure for eight of the judgmentally sampled PCAs.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer implement mitigating controls for the **********2**********, ensure that patches are applied to file transfer servers, and verify through testing that the IRS Information Technology organization is able to recover mission essential functions within the maximum tolerable downtimes or recovery time objectives to address the prematurely closed PCAs identified during this review. In addition, 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.

The IRS agreed with all of our recommendations. The Information Technology organization laid out a plan to implement mitigating controls for the **********2**********, is on target to complete the remaining actions to close the prematurely closed PCAs [related to patching], and began work on a plan to verify through testing that the IRS is able to recover mission essential functions within the maximum downtimes or recovery time objectives. In addition, the Chief Risk Officer has begun to put in place procedures to ensure that any appropriate documentation is uploaded to the JAMES.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

June 1, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Fully and Effectively Implemented and Documented (Audit # 201920017)

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, and properly approved and whether those actions effectively corrected the identified deficiencies. This review is part of our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Achieving Operational Efficiencies*.

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

Copies of this report are also being sent to the IRS managers affected by the report recommendations. 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

Internal controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are being achieved. Internal controls protect assets, detect errors, and prevent fraud. Internal controls help Government program managers achieve desired results through effective stewardship of public resources. Systems of internal control provide reasonable assurance that the following objectives are being met: 1) effectiveness and efficiency of operations, 2) reliability of financial reporting, and 3) compliance with applicable laws and regulations.

Internal controls protect assets, detect errors, and prevent fraud as well as provide reasonable assurance that organizational objectives are being achieved.

The Joint Audit Management Enterprise System (JAMES) is the Department of the Treasury's (hereafter referred to as the Treasury Department) web-based management controls database tracking system. It is used to track issues, findings, and recommendations extracted from Government Accountability Office[1] (GAO), Treasury Office of Inspector General, and Treasury Inspector General for Tax Administration (TIGTA) audit reports. It 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 is mandatory to comply with the intent of the GAO's *Standards for Internal Control in the Federal Government*,[2] the Federal Managers Financial Integrity Act of 1982,[3] Office of Management and Budget Circulars, and Treasury Department Directives. In addition, the Treasury Department and its bureaus use the information contained in the JAMES to assess the effectiveness and progress in correcting internal control deficiencies and implementing audit recommendations.

Within the Office of the Chief Risk Officer, the Enterprise Audit Management (EAM) organization, formerly the Office of Audit Coordination, is responsible for carrying out the day-to-day internal control program, including audit follow-up activities.[4] The EAM organization is the single point-of-contact for all open audits and is responsible for managing deficiencies in the JAMES. The EAM organization's primary responsibilities include:

- Monitoring and tracking material weaknesses and significant deficiencies as well as GAO and TIGTA report findings, recommendations, and PCAs in the JAMES.

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

[2] GAO, GAO-14-704G, dated September 10, 2014.

[3] 31 U.S.C. §§ 1105, 1113, and 3512 (2013).

[4] Prior to July 8, 2019, the EAM organization was known as the Office of Audit Coordination and was located within the Office of the Chief Financial Officer's Associate Chief Financial Officer for Internal Controls Division. Our use of 'the EAM organization' throughout the remainder of this report includes the Office of Audit Coordination when referring to work done during the applicable time period that it existed.

- Reviewing and validating all status updates via Forms 13872, *Planned Corrective Action (PCA) Status Update for TIGTA/GAO/MW/SD/TAS/REM Reports*,[5] entered into the JAMES by the JAMES audit coordinators.
- Maintaining complete and accurate records of management updates and responses to the Federal Managers Financial Integrity Act of 1982 as well as PCA remediation.
- Providing direction and assistance to the JAMES audit coordinators and their managers, as needed.

In addition, JAMES audit coordinators are embedded in the various business units and are responsible for ensuring that the PCA statuses are correctly posted in the JAMES and that the PCAs are timely implemented for material weaknesses and significant deficiencies as well as GAO and TIGTA report findings and recommendations. Their primary responsibilities include:

- Assisting management with the internal control program and serving as their business unit's primary liaison with the EAM organization.
- Preparing and submitting verification of the PCA completions to the EAM organization.
- Monitoring and updating the status of the PCAs in the JAMES.
- Maintaining complete audit files, including documentation of corrective actions taken, executive certification of status updates, and concurrence memoranda.
- Uploading and entering all implemented status updates in the JAMES within five workdays of the due date.
- Ensuring that sufficient documentation supporting the closed PCA is available for five years after the fiscal year in which the PCA was closed.

Results of Review

For our review, we selected a judgmental sample[6] of 24 PCAs from a population of 83 PCAs closed as implemented or canceled by the Information Technology (IT) organization during Fiscal Years 2017 and 2018. Of the 24 PCAs, we selected 15 PCAs closed as implemented to assess the closure process and the effectiveness of the corrective actions taken.[7] We selected PCAs that we considered higher risk findings identified in prior TIGTA reports. In addition, we selected all nine PCAs closed as canceled during this time frame to assess the closure process for canceling these PCAs.

Our review of the nine PCAs closed as canceled determined that they were properly approved and adequately documented via the required Form 13872. Specifically, both an Internal Revenue Service (IRS) and TIGTA executive approved the cancellation of these PCAs.[8] However,

[5] All business units also use this form to record specific actions taken to implement and to update the status of their PCAs, *e.g.*, adding the PCA implementation date or extending the due date. MW is Material Weakness, SD is Significant Deficiency, TAS is Taxpayer Advocate Service, and REM is Remediation Plan.

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

[7] Appendix III provides the results of our judgmental sample review.

[8] The JAMES audit coordinator and an IRS approving official did not sign two of the nine Forms 13872. TIGTA did not consider this material because of subsequent documentation provided showing that an IRS and TIGTA executive approved the cancellation of both PCAs.

our review also found that the closure process for PCAs closed as implemented needs to be strengthened to ensure that PCAs are fully implemented and effectively corrected the identified deficiencies, and that sufficient supporting documentation of corrective actions taken is properly maintained.

Some Closed Planned Corrective Actions Were Not Fully and Effectively Implemented to Address Identified Deficiencies

The IRS continues to be exposed to security vulnerabilities by not adequately addressing previously reported and agreed-to deficiencies in its internal control environment.

The IRS continues to be exposed to security vulnerabilities by not adequately addressing previously reported and agreed-to deficiencies in its internal control environment. 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. Our analysis of the 15 judgmentally sampled PCAs reported as closed determined that the IRS fully implemented 11 of them.[9] Of these 11 PCAs, seven were effective in correcting the identified deficiencies. For the remaining four PCAs, we were unable to test for effectiveness due to the nature of the corrective actions, such as conducting a feasibility analysis, updating the methodology section of a document, *etc.*

However, our analysis also determined that the IRS did not fully implement four (27 percent) of the 15 closed PCAs reviewed. All four PCAs were partially implemented to address portions of the identified deficiencies. The Internal Revenue Manual[10] provides that the heads of all business units are required to certify that corrective actions are met. The following provides further details of our analysis related to the four closed PCAs that were partially implemented.

- **PCA Sample Number 2:** TIGTA originally found deficiencies on **********2********** ***2*** related to ***********2*********** for *******2*******. The IRS agreed to implement mitigating controls for ***********2*********** that are ********2********* and stated that it has controls in place to include the annual recertification process.

  Enterprise Operations function management provided two standard operating procedures, ************2*********** Management Certification Process Standard Operating Procedures* and *Requesting *******2******** Standard Operating Procedures*,[11] documenting the annual ****2**** process and the creation of ****2**** ****2****. They also provided examples of two revalidation ****2**** reports detailing the status of the annual recertification of *******2******* for May and June 2019.

[9] Two of the 11 PCAs were fully implemented after their PCA closure dates. For one PCA, Enterprise Services function management stated that, while one of a three-part corrective action was completed and the other two components were started, they did not realize that all three components must be completed fully prior to the closure of the PCA. All components of the PCA were subsequently completed after the closure date. For the second PCA, Applications Development function management stated that, while they updated documents with the validation of ******2****** information, they did not realize until after closing the PCA that the updated documents were not the appropriate place to add that information. The appropriate documents were subsequently updated after the PCA closure date.

[10] Internal Revenue Manual 1.4.30, *Resource Guide for Managers, Monitoring Internal Control Planned Corrective Actions* (Oct. 2015).

[11] Dated March and June 2019, respectively.

Due to the large number of ********2********, the Enterprise Operations function allocates a proportionate number of ********2******** each month to be revalidated for the annual recertification process. Our analysis of the June 2019 report determined that there were gaps in the revalidation. Of the 144 ********2******** listed in the June 2019 report, only ********2******** was revalidated. In addition, of the 16 ********2******** ***2*** after the December 21, 2016, PCA closure date, 10 were never revalidated during the annual recertification process.[12] As a result, we determined that this PCA was partially implemented; however, the corrective actions taken were not fully effective.

Enterprise Operations function management stated that the gaps in the revalidation of ********2******** were caused by a misunderstanding of which function was responsible for their revalidation. As a result, the revalidation of ********2******** did not occur for a period of time. Enterprise Operations function management also stated that they have initiated a project that will review all **********2********** to ensure that the *******2******* meet the annual recertification requirements and that ********2********.

- **PCA Sample Number 8:** TIGTA originally found that reported vulnerabilities were not timely remediated on file transfer servers. The IRS stated it has an enterprise-wide process in place to continuously and timely implement patches to the information technology infrastructure and will follow this process to ensure that patches are applied to file transfer servers, including those located in the Demilitarized Zone, within established time frames. The IRS stated it would also verify that patching for file transfer servers has been applied.

  Enterprise Operations function management provided two documents, *Server Patch Management Standard* and *Patch Implementation Standard Operating Procedures*,[13] that provide the procedures to continuously and timely implement patches to the information technology infrastructure. In addition, they provided customized patch reports, as of October 2019, to support that patches were installed to file transfer servers, including those located in the Demilitarized Zone, within established time frames. However, the patch reports also showed that some patches were not timely installed to some file transfer servers in the Demilitarized Zone. For example, the IRS did not install all seven critical vulnerability patches within 30 calendar days as required (averaging 216 calendar days). The IRS also did not install 20 (10 percent) of the 199 important/high vulnerability patches within 90 calendar days as required (averaging 157 calendar days). According to Enterprise Operations function management, patching servers in the Demilitarized Zone requires a manual process to complete the scanning and remediation, which contributed to the delays. As a result, we determined that this PCA was partially implemented; however, the corrective actions taken were not fully effective.

- **PCA Sample Number 10:** TIGTA originally found that the IRS could not identify actual recovery times for all systems supporting its mission-essential functions and, therefore, did not have sufficient information to verify its ability to recover mission-essential functions within the time frames defined by the business units. The IRS stated that the Enterprise Operations function will verify, through its current documented process, that it is able to recover mission-essential functions within the maximum tolerable

[12] The remaining six ********2******** were not applicable because they were recently ****2**** in June 2019 and a revalidation was not yet required.
[13] Both documents are dated May 2019.

downtimes for only those systems the Cybersecurity function identified as needing disaster recovery or alternate site processing.

The Cybersecurity function identified 39 systems supporting its mission-essential functions that need disaster recovery or alternate site processing. The IRS uploaded to the JAMES a spreadsheet that provides the testing schedules and recovery time objectives[14] for 22 critical infrastructure protection program systems,[15] which included 13 of the 39 systems that support mission-essential functions.

Based on the initial documentation provided, we found that the testing results for six of the 13 systems were able to recover mission-essential functions within the maximum tolerable downtimes. Cybersecurity function management subsequently provided documentation supporting that three additional systems (totaling nine systems) were able and one system was unable to recover mission-essential functions within the maximum tolerable downtime.[16] Testing results were not provided for the remaining three systems.

Cybersecurity function management stated that the IRS received an extension until July 2020 to identify the recovery time objective for the remaining 29 systems supporting its mission-essential functions. The Enterprise Operations function would need this information before being able to determine whether the systems are able to recover mission-essential functions within the maximum tolerable downtimes. As a result, we determined that this PCA was partially implemented; however, the corrective actions taken were not fully effective.

- **PCA Sample Number 14:** TIGTA originally identified incident tickets from the Knowledge Incident/Problem Service Asset Management (KISAM) system that had negative resolve times (*i.e.*, the resolve time was recorded prior to the incident ticket being reported). The IRS agreed to implement systemic controls to prevent erroneous incident ticket time entries for which the incident stop time is earlier than the incident start time.

  Our review determined that the IRS did not implement effective systemic controls to fully prevent erroneous incident ticket time entries. Specifically, we analyzed a KISAM data extract containing 281,102 incident tickets closed during Fiscal Year 2018 and identified three incident tickets that were closed with an incident stop time that was earlier than the incident start time. On October 15, 2019, we met with Enterprise Operations function personnel and an IRS contractor regarding this issue, and they subsequently determined that there was a defect in the vendor's code and the chronological order of the ruleset for these three incident tickets. Although the number of problematic incident tickets appear to be relatively few, we determined that the initial corrective actions taken were not fully effective. On November 7, 2019, the IRS contractor subsequently updated the chronological order of the ruleset to resolve this issue. The PCA is now effectively implemented.

[14] The recovery time objective is needed before being able to determine whether a system is able to recover mission-essential functions within the maximum tolerable downtime.

[15] Critical infrastructure protection program system testing of disaster recovery or alternative site processing can be used for the testing of systems supporting mission-essential functions.

[16] One system was unable to recover mission-essential functions within the maximum tolerable downtime due to its reliance on and the failure of a general support system.

Our results on this review are similar to the results of two prior TIGTA reviews[17] of PCAs closed by the IT organization. In these two reviews combined, we selected a judgmental sample of 43 PCAs from a total population of 279 PCAs the IT organization closed as implemented.[18] We reported that 14 (33 percent) of the 43 judgmentally sampled PCAs were not fully implemented.[19] Of the 14 PCAs, 12 PCAs were partially implemented and two PCAs were not implemented at all.

For our current review, the supporting documentation did not support a conclusion that the corrective actions taken for four PCAs have been fully and effectively implemented. As a result, the IRS may have a false sense that it has effectively corrected identified internal control deficiencies when in reality it has not.

For the prematurely closed PCAs identified during this review, the Chief Information Officer (CIO) should:

Recommendation 1: Implement mitigating controls for the **********2********** that are ********2********.

> **Management's Response:** The IRS agreed with this recommendation. The IT organization has laid out a plan to implement mitigating controls for the ***2*** **********2**********. The implementation date reflects time for the IT organization to close the actions needed as well as collect and submit one quarter of evidence that the recommendation has been met.

Recommendation 2: Ensure that patches are applied to file transfer servers, including those located in the Demilitarized Zone, within established time frames.

> **Management's Response:** The IRS agreed with this recommendation. This recommendation had been partially completed. The IT organization is on target to complete the remaining actions needed to close the PCAs [related to patching] and produce the necessary evidence required by TIGTA on that closure.

Recommendation 3: Verify through testing that the IRS IT organization is able to recover mission-essential functions identified by the Cybersecurity function within the maximum tolerable downtimes or recovery time objectives.

> **Management's Response:** The IRS agreed with this recommendation. The IT organization has begun work on a plan to verify through testing, where possible, that it is able to recover mission-essential functions identified by the Cybersecurity function within the maximum downtimes or recovery time objectives.

[17] TIGTA, Ref. No. 2018-20-063, *Improved Controls Are Needed to Ensure That Corrective Actions for Reported Information Technology Weaknesses Are Documented and Fully Implemented Prior to Closure* p. 7 (Sept. 2018), and TIGTA, Ref. No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* p. 5 (Sept. 2018).

[18] The judgmental sample from each review included 20 of 203 PCAs that were closed as implemented between Fiscal Years 2013 and 2017, and 23 of 76 PCAs that were closed as implemented between Fiscal Years 2012 and 2017.

[19] These two prior reviews did not test for the effectiveness of the corrective actions.

The Planned Corrective Action Closure Process Continues to Need Improvement

Generally, our review of the 15 judgmentally sampled PCAs closed as implemented found that an IRS approving official and JAMES audit coordinator approved each of the PCA closures as required. However, the closure process of uploading supporting documentation to the JAMES continues to be problematic.

Documentation supporting information technology PCA closures was not always uploaded to the JAMES

Without sufficient supporting documentation, there is limited evidence readily available to support that all PCAs were fully implemented.

Prior to April 1, 2017, the EAM organization did not require the IRS to upload supporting documentation to the JAMES if corrective action was taken to address the identified deficiency prior to signing the management's response to the TIGTA draft report. One of the 15 judgmentally sampled PCAs met this criterion; therefore, documentation for it was not required to be uploaded to the JAMES. Of the remaining 14 judgmentally sampled PCAs, our analysis determined that eight (57 percent) PCAs had insufficient documentation in the JAMES to fully support their closures. The following provides further details of our analysis related to the insufficient documentation uploaded to the JAMES.

- **PCA Sample Number 2:** TIGTA originally found deficiencies related to *******2******* ****2**** for ******2******. The IRS agreed to implement mitigating controls for **********2********** that are **********2**********.

  The IRS uploaded Form 3.3, *Request for Non-SEID SEID **********2**********;*[20] a template for creating nonstandard **********2**********, and *Non-SEID **********2********** Standard Operating Procedures*,[21] which defines the types of and requirements for nonstandard **********2********** in the **********2**********. However, the standard operating procedure does not document mitigating controls to include the annual recertification process for ***2*** ********2******** that are *********2*********. Enterprise Operations function management subsequently provided two standard operating procedures, *****2***** *********2********* Management Certification Process Standard Operating Procedures* and *Requesting *********2********* Standard Operating Procedures*, documenting the annual recertification process and the **********2**********. They also provided two revalidation ****2**** reports as examples supporting that mitigating controls were implemented to annually recertify some *******2*******.

- **PCA Sample Number 3:** TIGTA originally found that the IRS did not follow established processes for authorizing and documenting access controls. Specifically, the IRS could not provide documentation to support that the Integrated Production Model service accounts were authorized and approved to access the data for 27 source systems. The IRS agreed that the Integrated Production Model application will establish an annual

[20] SEID is Standard Employee Identifier, **********2**********.
[21] The standard operating procedures is not dated.

validation of service accounts as part of its filing season update process and will document service account information in the interface control documents for source systems.

The IRS uploaded an e-mail and an architecture document that explain and support that an interface control document for one source system was not needed because the source system and the Integrated Production Model application are within the boundary of a larger system and data is not transmitted into or out of the larger system. In addition, the IRS uploaded the Online 5081 forms documenting the authorization for four of seven service accounts used in accessing the Integrated Production Model application by the remaining 26 source systems.[22] However, the authorization for the remaining three service accounts and all interface control documents were not uploaded. Applications Development function management subsequently provided supporting documentation for the authorization of the remaining service accounts as well as the annual validation for all seven service accounts. They also provided the interface control documents for 16 source systems still in use[23] that document the service account information.

- **PCA Sample Number 6:** TIGTA originally found that, while the Cybersecurity function's Security Operations organization began producing reports from the electronic Authentication (eAuthentication) audit logs, the reports provided a list of only suspicious transactions. It did not contain summary information on the number of events that would be necessary to investigate the transactions and determine whether any action needs to be taken in response to those events. The IRS agreed to ensure that the eAuthentication audit trail includes information indicating which target application the user intended to access after authenticating. The IRS stated it would ensure that Security Audit and Analysis System events are captured for: 1) identification proofing to provide target application information, 2) activation and security codes, and 3) SiteMinder target application information.

  The IRS uploaded some documentation to support that the eAuthentication audit trail includes information indicating the target application the user intended to access after authenticating. Specifically, the IRS uploaded documentation that Security Audit and Analysis System events captured identification proofing that provides target application and SiteMinder target application information. However, documentation that supports activation and security codes are being captured was not uploaded. Applications Development function management subsequently provided us the supporting documentation.

- **PCA Sample Number 7:** TIGTA originally found that the IRS did not ensure that only secure protocols (rather than nonsecure protocols such as File Transfer Protocol and Telnet) are being used to fully protect information during transmission. The IRS agreed and stated that it would continue to review its external file transfer firewall rulesets, remove those that are no longer needed, and ensure that only transmissions approved in a current Interconnection Security Agreement are allowed through the firewalls.

  The IRS stated it completed a full cycle review of the external file transfer firewall rulesets and related Interconnection Security Agreements. The IRS also uploaded a change

[22] One service account can access more than one source system.

[23] Ten of the remaining 26 source systems were retired subsequent to TIGTA's prior audit.

request to remove a firewall rule that was no longer needed. However, a change request alone is not sufficient evidence that the firewall rule was actually deleted. User and Network Services function management subsequently provided documentation that the firewall rule was deleted. In addition, they also provided documentation of detailed communications between firewall administrators to remove rules that are no longer needed, supporting the continual review of firewall rulesets.

- **PCA Sample Number 8:** TIGTA originally found that reported vulnerabilities were not timely remediated on file transfer servers in the Demilitarized Zone. The IRS stated it has a process in place to continuously and timely implement patches and would verify that patches were applied to the file transfer servers.

  The IRS uploaded an undated and unsigned half-page document listing seven procedures that briefly describe patching responsibilities. This document is not official and does not provide sufficient support as an enterprise-wide process to continuously and timely implement patches to file transfer servers, including those located in the Demilitarized Zone. The IRS also did not upload documentation that supports verification of timely patching the file transfer servers. Enterprise Operations function management subsequently provided documents on the standards for server patch management and standard operating procedures to continuously and timely implement patches to the information technology infrastructure. In addition, they provided customized patch reports to support that some patches were installed to file transfer servers, including those located in the Demilitarized Zone, within established time frames.

- **PCA Sample Number 10:** TIGTA originally found that the IRS could not identify actual recovery times for all systems supporting its mission-essential functions. The IRS stated it would verify that it is able to recover mission-essential functions within the maximum tolerable downtimes for only those systems the Cybersecurity function identified as needing disaster recovery or alternate site processing.

  The IRS uploaded and provided subsequent documentation supporting that nine systems were able and one system was unable to recover mission-essential functions within the maximum tolerable downtimes of 39 systems that the Cybersecurity function identified as needing disaster recovery or alternate site processing. However, the IRS received an extension on a related PCA to identify the recovery time objective, which is needed in determining whether systems are able to recover mission-essential functions within the maximum tolerable downtimes, for the remaining 29 systems.

- **PCA Sample Number 11:** TIGTA originally found that the IRS did not follow the existing policy regarding systems access and approval. The IRS agreed that the Enterprise Services function would ensure that all existing Big Data Analytics service accounts are compliant with the Online 5081 application requirements and access is still required. In addition, the Enterprise Services function will modify the approval path for Big Data Analytics database administrator account requests to ensure that the established Online 5081 application process is followed before accounts are created.

  The IRS uploaded the *Big Data Analytics (BDA), Release 1.0, Design Specification Report (DSR), Logical/Physical Design*,[24] which provides a comprehensive design overview of the

[24] Version 1.8, dated June 18, 2014.

Big Data Analytics infrastructure, the original and modified approval paths for database administrator account requests, an e-mail listing tasks and their statuses related to updating and cleaning up service accounts, and a listing of service accounts for potential deletion. However, the e-mail listing still contained tasks with "pending" statuses, incomplete tasks, and the listing of service accounts that identifies accounts still waiting for a decision on whether they should be deleted. Enterprise Services function management subsequently provided documentation supporting that the tasks were completed and the service accounts were deleted when no longer needed.

- **PCA Sample Number 13:** TIGTA originally found that Computer Security Incident Response Center (CSIRC) contractors did not always meet Federal Information Security Modernization Act of 2014[25] specialized security training requirements. The IRS stated that it implemented new technology, policy, and process changes to deprovision noncompliant contractors from accessing the IRS network instead of relying on individual system owners to remove access privileges.

  The IRS only uploaded a desk guide, *Specialized Information Technology (IT) Security Training for Contractor Employees*.[26] The desk guide provides that IRS contractors not in compliance with specialized security training requirements will have their system accesses suspended. Information on the new technology or process changes was not uploaded.

  Cybersecurity function management subsequently provided documentation that the Archer system and the Enterprise Learning Management System are used to track and report training compliance, including the number of training hours assigned and completed. They also provided us documentation supporting that all CSIRC contractors completed the specialized security training requirements for the last three years since TIGTA's prior audit. As a result, the IRS has not had to deprovision any CSIRC contractor's system access. Cybersecurity function management explained that they implemented an annual process that would deprovision CSIRC contractor access when contractors are noncompliant with specialized security training requirements by changing their employment status from "Active" to "Suspended" in the Human Resources Connect system. This action notifies downstream applications to reflect the contractor's employment status as "Inactive" and deprovisions contractor access to the local area network, e-mail, and the Internet.

Internal Revenue Manual 1.4.30 requires JAMES audit coordinators to upload supporting documentation to the JAMES and to maintain complete audit files to ensure that sufficient documentation supporting the PCA closure is available for five years after the fiscal year in which the PCA was closed.[27] It also provides that the EAM organization should ensure that supporting documentation is uploaded to the JAMES. In addition, the heads of all business units are required to adhere to the requirements governing the internal control process for the

[25] Pub. L. No. 113-283. This bill amends chapter 35 of title 44 of the U.S.C. to provide for reform to Federal information security.

[26] Version 3, dated March 6, 2017.

[27] In September 2010, the Treasury Department updated the retention period for source documentation in the JAMES from five to nine years. We reported that the IRS did not update this requirement in its Internal Revenue Manual in TIGTA, Ref. No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* p. 10 (Sept. 2018). The IRS plans to update the manual with the Treasury Department's revised retention period requirement in Calendar Year 2020.

JAMES by emphasizing the importance of maintaining supporting documentation. Further, the EAM organization issued guidance, *JAMES Closure Guidance*, requiring supporting documentation to be uploaded to the JAMES if the IRS took corrective action prior to signing the management's response to a TIGTA draft report, effective April 1, 2017.

In the same two prior TIGTA reviews of PCAs, we reported that the IRS did not always upload to the JAMES documentation supporting the PCA closures. For this test, we selected a judgmental sample of 79 PCAs from the total population of 279 PCAs closed by the IT organization and determined that the documentation uploaded to the JAMES for 57 (72 percent) of them did not support their closures.[28] In one of the reports, we recommended that EAM reviewers (known as PCA closure analysts) improve their skillsets on obtaining sufficient and appropriate PCA closure evidence to support their review findings and conclusions. The IRS agreed and developed a training plan that emphasized critical thinking and analytical review skills for internal controls and closed recommendations. The IRS subsequently had the PCA closure analysts attend a training class on documentary evidence identification and analysis (classes were held on January 15 and 16, 2020). Because the IRS had not implemented this corrective action prior to our current review of closed PCAs, we are not making a recommendation on the overall PCA closure documentation process in this report.

Generally, Forms 13872 were adequately completed and uploaded to the JAMES

Our review of 14 of the 15 judgmentally sampled PCAs found that Forms 13872 were adequately completed and uploaded to the JAMES. The Form 13872 for the remaining PCA was not uploaded to the JAMES, but the assigned JAMES audit coordinator for this PCA was able to provide a copy. Our subsequent review of the remaining PCA determined that the Form 13872 had the following issues:

- The JAMES audit coordinator did not sign the form.
- The IRS approving official did not sign the form with either a handwritten or an electronic signature, but rather typed his/her name on the form.
- The IRS approving official typed his/her name on the form on November 15, 2018, which is approximately 25 months after the PCA due date of October 2, 2016.

Internal Revenue Manual 1.4.30 requires the JAMES audit coordinators to upload the approved Form 13872 to the JAMES and for the EAM organization to ensure that it occurs. As of October 1, 2014, all approving officials must also sign and date the form via a handwritten or electronic signature. In addition, the approving official must sign the form within five workdays of the PCA due date.

Based on the 15 judgmentally sampled PCAs reviewed, we determined that the JAMES audit coordinators and EAM organization did not always ensure that adequate documentation was uploaded to the JAMES to support the PCA closures. Without sufficient supporting documentation in the JAMES, there is limited evidence readily available to support that all of the judgmentally sampled PCAs were fully implemented.

[28] In one of the two prior reviews, the audit team reviewed an additional 40 PCAs closed as implemented to determine whether the documentation uploaded to the JAMES supported the PCA closures. In addition, our judgmental samples from the two prior TIGTA reviews included 17 PCAs for which the IRS took corrective action prior to signing the management's response to TIGTA's draft reports. Because this occurred prior to April 1, 2017, for these 17 PCAs, there was no requirement that supporting documentation be uploaded to the JAMES.

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.

Management's Response: The IRS agreed with this recommendation. The Chief Risk Officer has begun to put in place procedures to ensure that any appropriate documentation subsequently provided during this review is uploaded to the JAMES for the judgmentally scripted PCAs that lacked sufficient documentation to support the closure.

Appendix I

Detailed Objective, Scope, and Methodology

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

- Determined the processes used by the CIO and the Office of the Chief Risk Officer to ensure compliance with the requirements for closing implemented IT organization PCAs by reviewing policies and procedures as well as interviewing EAM and IT organization personnel.
- Obtained information from the JAMES of all 83 PCAs closed as implemented or canceled during Fiscal Years 2017 and 2018. We selected a judgmental sample[1] of 15 higher risk and all nine canceled PCAs for a detailed review. We used a judgmental sample because we did not plan to project to the population.

  Reviewed Forms 13872 and associated supporting documentation to determine whether the PCAs that were closed as implemented were adequately documented, properly approved, and fully implemented and whether they effectively corrected the reported deficiencies.
- Determined whether IT organization PCAs reported as canceled were adequately documented and properly approved by reviewing supporting documentation for all nine canceled PCAs.

Performance of This Review

This review was performed at the New Carrollton Federal Building in Lanham, Maryland, in the IT organization during the period June 2019 through January 2020. 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 R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Bryce Kisler, Director; Louis Lee, Audit Manager; David Allen, Lead Auditor; Paula Benjamin-Grant, 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 KISAM system. We evaluated the data to ensure that the data were reasonably complete and accurate and that the incident tickets were closed in Fiscal Year 2018. We obtained the data extract from another audit team and relied on their data validation that previously verified the criteria, that all fields requested

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

were received, that the record counts were as expected, *etc*. We determined that the data were sufficiently reliable for the 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 in the Federal Government* and the Internal Revenue Manual as well as various IRS policies, procedures, and processes for managing and ensuring the proper closure of PCAs. We evaluated these controls by interviewing JAMES audit coordinators and EAM and IT organization personnel, identifying guidance for managing and ensuring PCA closure and implementation, reviewing documents supporting the closure of the 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:

- Reliability of Information – Potential; four closed PCAs that were not fully and effectively implemented and were prematurely closed, which resulted in incorrect information being recorded in the JAMES (see page 3).

Methodology Used to Measure the Reported Benefit:

We reviewed a judgmental[1] sample of 15 PCAs closed as implemented and their related supporting documentation. We found that four of the sampled PCAs were not fully and effectively implemented, which resulted in incorrect information being recorded in the JAMES.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; three KISAM incident tickets closed in Fiscal Year 2018 that had inaccurate date information (see page 3).

Methodology Used to Measure the Reported Benefit:

We reviewed all 281,102 incident tickets closed in Fiscal Year 2018 from the KISAM system. Our analysis of the KISAM data identified three incident tickets that were closed with an incident stop time that was earlier than the incident start time.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; five PCAs closed as implemented had insufficient documentation in the JAMES to support their closure (see page 7).

Methodology Used to Measure the Reported Benefit:

Using the same judgmental sample of 15 closed PCAs previously mentioned, we found that eight sampled PCAs had insufficient documentation in the JAMES to support their closure. However, three of these PCAs were also prematurely closed without being fully and effectively implemented as well as having insufficient documentation to support their closure. These three PCAs were included in the count total of the first outcome measure and thus were not included here.

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

Appendix III

Assessment of the Information Technology Organization's Planned Corrective Actions

PCA Sample Number	TIGTA Reported Deficiency	Recommendation	PCA	TIGTA's Assessment of Corrective Actions
TIGTA, Ref. No. 2014-20-083, *The Internal Revenue Service Should Implement an Efficient Internal Information Security Continuous Monitoring Program That Meets Its Security Needs* (Sept. 2014).				
1	PCA 1-1-1 The IRS should continue to move forward in implementing a stronger information security continuous monitoring program.	The Chief Technology Officer should select and implement an integrated dashboard of the security scanning tools to allow stakeholders and decision makers to make well informed risk-based decisions.	The Chief Technology Officer will select and implement an integrated dashboard of the security scanning tools to allow stakeholders and decision makers to make well informed risk-based decisions by establishing an enterprise-wide integrated project team to direct their Information Security Continuous Monitoring initiative. Based on the future direction of the integrated project team, the IRS will select and implement an integrated local dashboard of its security scanning tools.	**Effective – Fully Implemented**
TIGTA, Ref. No. 2016-20-012, ***********2********** Need Improvement to Mitigate Insider Threats* (Feb. 2016).				
2	PCA 2-2-1 **********2******** **********2******** *****2****.	The Chief Technology Officer should implement mitigating controls for the *******2******* *********2******* that are **2** *********2*******.	The IRS will implement mitigating controls for the **************2************** that are *********2********.	**Not Fully Effective – Partially Implemented**
TIGTA, Ref. No. 2016-20-058, *The Integrated Production Model Increases Data Access Efficiency; However, Access Controls and Data Validation Could Be Improved* (July 2016).				
3	PCA 1-2-1 The IRS did not follow established processes for authorizing and documenting access controls.	The Chief Technology Officer should conduct a periodic review of access control lists to verify that all systems are current, authorized, and documented.	The Integrated Production Model will establish an annual validation of service accounts as part of its filing season update process and will document service account information in the interface control documents for source systems.	**Effective – Fully Implemented After PCA Closure Date**

PCA Sample Number	TIGTA Reported Deficiency	Recommendation	PCA	TIGTA's Assessment of Corrective Actions
TIGTA, Ref. No. 2016-20-075, *Information Technology: SharePoint Controls Need Improvement to Mitigate Risks and to Ensure That Possible Duplicate Costs Are Avoided* (Sept. 2016).				
4	PCA 2-1-1 The SharePoint approach should be evaluated and justified as a long-term solution within the Treasury Department's shared services strategy.	The CIO should ensure that a feasibility analysis is conducted regarding use of the Treasury Enterprise Content Management environment, including an assessment of functionality, security, risks, costs, and benefits.	A feasibility analysis will be conducted regarding utilizing the Treasury Enterprise Content Management environment, including an assessment of functionality, security, risks, costs, and benefits.	**Effectiveness Not Applicable – Fully Implemented**
TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016).				
5	PCA 1-2-1 Network monitoring tools were not sufficient to detect automated attacks.	The CIO should establish a process to monitor the results and effectiveness of controls to prevent/detect automated attacks.	The IRS established a new organization within the Cybersecurity function's Security Operations organization with responsibility for monitoring protected applications to prevent and detect against automated attacks. The organization has established processes to monitor the results and effectiveness of the layered protections in place.	**Effective – Fully Implemented**
6	PCA 4-2-1 Additional information would improve the usefulness of audit log reports.	The CIO should ensure that the eAuthentication audit trail includes an EventID that indicates which target application the user intended to access after authenticating.	The IRS will ensure that Security Audit and Analysis System events are captured for: 1) identity proofing to provide target application information; 2) activation and security codes; and 3) SiteMinder target application information.	**Effective – Fully Implemented**
TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).				
7	PCA 1-2-1 Encryption was not fully implemented for all data transfers.	The CIO should continue to work on reviewing the firewall rulesets to remove those that are no longer needed and ensure that only transmissions approved in a current Interconnection Security Agreement are allowed through the firewalls.	The IT organization's User and Network Services and Cybersecurity functions will continue to review the external file transfer firewall rulesets and remove those that are no longer needed. The IRS will ensure that only transmissions approved in a current Interconnection Security Agreement are allowed through the firewalls.	**Effective – Fully Implemented**

PCA Sample Number	TIGTA Reported Deficiency	Recommendation	PCA	TIGTA's Assessment of Corrective Actions
8	PCA 2-2-1 File transfer servers were not always securely configured, and reported vulnerabilities were not timely remediated.	The CIO should ensure that patches are applied to file transfer servers, including those located in the Demilitarized Zone, within established time frames.	The IRS has an enterprise-wide process in place to continuously and timely implement patches to the information technology infrastructure. The IRS will follow this process to ensure that patches are applied to file transfer servers, including those located in the Demilitarized Zone, within established time frames. The IRS will verify that patching for file transfer servers has been applied.	**Not Fully Effective – Partially Implemented**
TIGTA, Ref. No. 2017-20-024, *Information Technology: Improvements Are Needed in Enterprise-Wide Disaster Recovery Planning and Testing* (June 2017).				
9	PCA 1-1-1 An enterprise-wide business impact analysis is needed to identify disaster recovery priorities for the orderly recovery of systems and applications supporting mission-essential functions.	The CIO should complete the enterprise-wide business impact analysis in accordance with the IRS business impact analysis methodology.	The IRS stated that, although its business impact analysis processes are current, the documentation is outdated. The IRS will document the methodology appropriately.	**Effectiveness Not Applicable – Fully Implemented**
10	PCA 2-2-1 Maximum tolerable downtimes for mission-essential functions have not been identified or verified to ensure that business needs can be met.	The CIO should verify through testing that the IRS IT organization is able to recover mission-essential functions within the maximum tolerable downtimes or recovery time objectives for mission-essential functions established by the business units.	The Enterprise Operations function will verify, through its current documented testing process, that the organization is able to recover mission-essential functions within the maximum tolerable downtimes for only the systems that are identified by the Cybersecurity function as needing disaster recovery or alternate site processing and to the extent that funding is available.	**Not Fully Effective – Partially Implemented**

PCA Sample Number	TIGTA Reported Deficiency	Recommendation	PCA	TIGTA's Assessment of Corrective Actions
TIGTA, Ref. No. 2017-20-029, *The Big Data Analytics General Support System Security Controls Need Improvement* (June 2017).				
11	PCA 3-1-1 Unauthorized accounts are operating within the Big Data Analytics General Support System.	The CIO should enforce current request and approval policy for all the Big Data Analytics General Support System database administrator accounts and service accounts to ensure that these accounts are compliant with the Online 5081 application requirements and that access is still required.	The Enterprise Services function will ensure that all existing Big Data Analytics database administrator accounts and service accounts are compliant with the Online 5081 application requirements and that access is still required. Additionally, the Enterprise Services function will collaborate with the Enterprise Operations Online 5081 group to modify the approval path for Big Data Analytics General Support System account requests to ensure that they follow the established Online 5081 process before accounts are created.	**Effective – Fully Implemented After PCA Closure Date**
TIGTA, Ref. No. 2017-20-050, *The Computer Security Incident Response Center Is Preventing, Detecting, Reporting, and Responding to Incidents, but Improvements Are Needed* (Aug. 2017).				
12	PCA 1-1-1 Incident handling and reporting could be enhanced.	The CIO should ensure that the CSIRC corrects the reporting inconsistency by reporting the remaining cell phones that contained Personally Identifiable Information to the Incident Management and Employee Protection office, and correct the missing or incomplete documentation indicating the actions to halt the spread of and limit the damage caused by the incident, and, when applicable, document the effectiveness of the containment actions for the eight incidents.	The CSIRC has ensured that each of the remaining incidents involving lost/stolen cell phones are properly reflected as containing Personally Identifiable Information within its incident tracking system, along with reporting to the Treasury CSIRC, and the Privacy, Governmental Liaison and Disclosure office.	**Effectiveness Not Applicable – Fully Implemented**

PCA Sample Number	TIGTA Reported Deficiency	Recommendation	PCA	TIGTA's Assessment of Corrective Actions
13	PCA 2-2-1 Employees and contractors did not always meet training guidelines, and skill assessments demonstrate a need for more training.	The CIO should ensure that system owners remove CSIRC contractors' access privileges to IRS systems when they are noncompliant with Federal Information Security Modernization Act of 2014 training requirements.	The IRS implemented systemic deprovisioning at the network access point to ensure that all access would be eliminated instead of relying on individual system owners to remove access privileges. On March 6, 2017, the IRS had already fully implemented new technology, policy and process changes to deprovision Federal Information Security Modernization Act of 2014 noncompliant contractors from accessing the IRS network. This deprovisioning process is executed weekly for Information Systems Security training and for annual Specialized Information Technology Security training prior to June 30, 2017.	**Effectiveness Not Applicable – Fully Implemented**
TIGTA, Ref. No. 2017-20-051, *Sixty-Four Percent of the Internal Revenue Service's Information Technology Hardware Infrastructure Is Beyond Its Useful Life* (Sept. 2017).				
14	PCA 1-2-1 Additional coordination with business units is needed to improve replacement of aged information technology hardware.	The CIO should implement systemic controls to prevent erroneous incident ticket time entries to the KISAM system for which the incident stop time is earlier than the incident start time.	The IRS will implement systemic controls to prevent erroneous incident ticket time entries to the KISAM system for which the incident stop time is earlier than the incident start time.	**Not Fully Effective – Partially Implemented**
TIGTA, Ref. No. 2018-20-030, *The Cybersecurity Data Warehouse Needs Improved Security Controls* (June 2018).				
15	PCA 3-1-1 An inventory of systems that transfer taxpayer data to the Cybersecurity Data Warehouse was not maintained.	The CIO should ensure that a complete and accurate inventory of systems that transfer transactional audit logs containing taxpayer data to the Cybersecurity Data Warehouse is maintained.	The IRS provided a comprehensive list and additional evidence that identified systems that transfer data to the Cybersecurity Data Warehouse. The IRS will ensure this list is maintained.	**Effective – Fully Implemented**

Appendix IV

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 15, 2020

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Acting Chief Information Officer

Thomas A. Brandt
Chief Risk Officer
Digitally signed by Thomas A. Brandt
Date: 2020.05.15 08:29:02 -04'00'

SUBJECT: Response to Draft Audit Report – Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Fully and Effectively Implemented and Documented - (audit #201920017) (e-trak # 2020-22303)

Thank you for the opportunity to review your draft audit report and address the report observations with the audit team. We appreciate TIGTA's recognition that nearly 75% of the high risk Planned Corrective Actions that TIGTA reviewed were fully implemented. We concur with TIGTA's statement in the report that internal controls are a major part of managing an organization and providing reasonable assurance that organizational objectives are being achieved.

The IRS is committed to fully and effectively implementing and documenting all agreed upon corrective actions. IRS's Enterprise Audit Management is instituting regular reviews of our processes to ensure agreed upon corrective actions are implemented and will be conducting rigorous post-implementation reviews on a periodic basis to ensure that those actions are working effectively.

We agree with TIGTA's recommendations and have already begun taking actions to address them. Our corrective action plan for the recommendations identified in the report is attached and will strengthen our security against threats. Staying on top of

potential security threats are of the utmost importance to IRS, particularly regarding taxpayer data.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact LaTonya Gutrick, Acting Director, Business Planning and Risk Management, at (240) 613- 3923.

Attachment

Attachment

Draft Audit Report – Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Fully and Effectively Implemented and Documented (audit #201920017) (e-trak # 2020-22303)

RECOMMENDATION #1: For the prematurely closed PCAs identified during the review, the Chief Information Officer (CIO) should implement mitigating controls for the ****2**** **********2**********.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The Information Technology (IT) organization has laid out a plan to implement mitigating controls for the **********2**********. The implementation date reflects time for IT to close the actions needed as well as collect and submit one quarter of evidence that the recommendation has been met.

IMPLEMENTATION DATE: September 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: For the prematurely closed PCAs identified during the review, the Chief Information Officer (CIO) should ensure that patches are applied to file transfer servers, including those located in the Demilitarized Zone, within established time frames.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. This recommendation has been partially completed. IT is on target to complete the remaining actions needed to close the PCAs and produce the necessary evidence required by TIGTA on that closure.

IMPLEMENTATION DATE: November 15, 2020

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations.

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #3: For the prematurely closed PCAs identified during the review, the Chief Information Officer (CIO) should verify through testing that the IRS IT organization is able to recover mission essential functions identified by the Cybersecurity function within the maximum tolerable downtimes or recovery time objectives.

Attachment

Draft Audit Report - Some Corrective Actions to Address Reported Information Technology Weaknesses Were Not Fully and Effectively Implemented and Documented (audit #201920017) (e-trak # 2020-22303)

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. IT has begun work on a plan to verify through testing, where possible, that we are able to recover mission essential functions identified by the Cybersecurity function within the maximum downtimes or recovery time objectives.

IMPLEMENTATION DATE: June 15, 2022

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations working with the Associate Chief Information Officers, Cybersecurity and User and Network Services.

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

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

CORRECTIVE ACTION #4: IRS agrees with this recommendation. The Chief Risk Officer has begun to put in place procedures to ensure that any appropriate documentation subsequently provided during this review is uploaded to the JAMES for the judgmentally scripted PCAs that lacked sufficient documentation to support the closure.

IMPLEMENTATION DATE: June 15, 2021

RESPONSIBLE OFFICIALS: Director, Enterprise Audit Management

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

Appendix V

Glossary of Terms

Term	Definition
Active Directory	A Microsoft Corporation software system for administering and securing computer networks. It manages the identities and relationships of computing resources that comprise a network. It also enables administrators to assign enterprise-wide policies, deploys programs to many computers, and applies critical updates to an entire organization simultaneously from a central, organized, accessible database. It simplifies system administration and provides methods to strengthen and consistently secure computer systems.
Application	An information technology component of a system that uses information technology resources to store, process, retrieve, or transmit data or information using information technology hardware and software.
Archer	A commercial off-the-shelf software product that assists IT organization executive leadership in improving its current capabilities to assess compliance with IRS policy and other Federal guidance.
Audit Trail	A record of system activity, both by system and application processes and by user activity, on systems and applications. In conjunction with the appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.
Big Data Analytics	The strategy of analyzing large volumes of data, or big data, to uncover patterns, connections, and valuable insights that might otherwise be invisible.
Business Impact Analysis	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Business Unit	A title for major IRS organizations, such as Appeals, the Wage and Investment Division, the IT organization, *etc.*
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the requirements for the system.
Computer Security Incident Response Center	Part of the IRS IT organization's Cybersecurity function. The CSIRC's mission is to ensure that the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify and eradicate cyber threats or cyberattacks. One of the primary duties of the CSIRC is to provide 24-hour monitoring and support to IRS operations seven days a week, 365 days a year.

Contractor	An organization or individual external to the IRS that supplies goods and services according to a formal contract and task order.
Corrective Action	Identification and elimination of the causes of a problem and preventing their recurrence.
Critical Infrastructure Protection Program	Addresses the security, protection, and resiliency of any asset that the failure or destruction of would have a severe impact on security, national economic security, or national public health and safety.
Cybersecurity Data Warehouse	Collects and stores security logs from dedicated devices used to protect the IRS network, and allows the IRS to retain log file output data for seven years in accordance with the data retention schedule approved by the National Archives and Records Administration.
Cybersecurity Function	Within the IRS IT organization, it is responsible for ensuring IRS compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Database	A computer system with a means of storing information in such a way that information can be retrieved.
Database Administrator	An individual that performs all activities related to maintaining a correctly performing and secure database environment. Responsibilities include design, implementation, and maintenance of the database system.
Deficiency	An instance of weak or missing controls.
Demilitarized Zone	A network segment inserted as a "neutral zone" between an organization's private network and the Internet.
Deprovision	The process in which access rights to software and network services are taken away; typically occurs when an employee leaves a company or changes roles within the organization.
eAuthentication	The process of establishing confidence in user identities electronically presented to an information system.
Encryption	The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge (referred to as a key).
Enterprise Content Management	The Treasury Department's preferred platform for new web application development and intranet content. An architectural framework and a set of tools and technologies that help improve the management of unstructured content.
Enterprise Learning Management System	An application that provides training, administration, and training resource management (instructors, classroom, and all web resources for learning).
Enterprise Operations Function	Within the IRS IT organization, it is responsible for providing efficient, cost-effective, and highly reliable computing (server and mainframe) services for all IRS business entities and taxpayers.
Enterprise Services Function	Within the IRS IT organization, it designs and tests enterprise solutions.
Feasibility Analysis	An analysis that establishes whether conditions are right to implement a particular project.

File Transfer	The process of copying or moving a file from one computer to another over a network or Internet connection. It enables sharing, transferring, or transmitting a file or a logical data object between different users and computers both locally and remotely.
File Transfer Protocol	A standard Internet protocol for transmitting files between computers on the Internet. It was originally defined in 1971 without much concern for security.
Firewall	Software used to maintain the security of the IRS's network by blocking unauthorized network traffic to or from IRS systems. It is employed to prevent unauthorized web users or illicit software from gaining access to the IRS network that is connected to the Internet. It is the first line of defense in securing sensitive information. The IRS has installed firewalls at its connections with the Internet, its business partners, and its internal network.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Government Accountability Office	An independent, nonpartisan agency that works for Congress. It reports to Congress on how well Government programs and policies are meeting their objectives. It advises Congress and the heads of executive agencies about ways to make the Government more efficient, effective, ethical, equitable, and responsive.
Human Resources Connect	The Treasury Department's primary human resources system that provides a broad range of applications, services, and information to human resources offices, employees, and managers. Managers are able to initiate paperless personnel actions and electronically route those actions for approval, reducing the time it takes to process a personnel action.
Identification Proofing	Verifying the claimed identity of an applicant by collecting and validating sufficient information, *e.g.*, identity history, credentials, and documents, about a person.
Incident Ticket	Incident tickets are created as part of the IRS's Information Technology Incident Management process and define the process and procedures for recording, categorizing, prioritizing, investigating, diagnosing, resolving, dispatching, monitoring, and closing out the incidents.
Infrastructure	The hardware, software, and network resources and services required for the existence, operation, and management of an enterprise information technology environment. It allows an organization to deliver information technology solutions and services to its employees, partners, and customers and is usually internal to an organization and deployed within owned facilities.

Integrated Production Model	A data warehouse that consolidates information from a variety of internal and some external sources, which is made available to a variety of downstream security-certified systems for use in conducting analysis, case selection, and report preparation.
Interconnection Security Agreement	An agreement established between the organizations that own and operate connected information technology systems to document the technical requirements of the interconnection.
Interface Control Document	Technical document describing interface controls and identifying the authorities and responsibilities for ensuring the operation of such controls. This document is baselined during the preliminary design review and is maintained throughout the information system life cycle.
Internal Revenue Manual	The IRS's primary source of instructions to its employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
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.
Maximum Tolerable Downtime	The maximum amount of time a business can tolerate the outage of a critical business function. It consists of two elements, the system's recovery time objective and the work recovery time.
Mission-Essential Function	An activity, directly related to accomplishing an organization's goal or objective, that must be continued throughout, or resumed rapidly after, a disruption of normal operations, such as in a disaster event.
Online 5081 Application	The IRS's web-based application that is used to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems.
Patch	Update to an operating system, application, or other software issued specifically to correct particular problems with the software.
Personally Identifiable Information	Any information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, and mother's maiden name.
Recovery Time Objective	The period of time within which data, system, and application functionality must be restored after an outage (*e.g.*, one business day) to resume processing transactions.
Risk-Based Decision	A decision made when meeting a requirement is technically or operationally not possible or is not cost effective. It is required for any situation in which the system will be operating outside of IRS information technology security policy or National Institute of Standards and Technology guidelines, whether related to a technical, operational, or management control.
Ruleset	A rule that defines and compares the parameters against each connection. It specifies what services to let through a firewall.

Security Audit and Analysis System	A system that collects security audit information. It assists the IRS and TIGTA in the detection of unauthorized intrusions and privileged access abuse.
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.
Service Account	Represents a process or a set of processes to manage authentication service operations with the operating system and network resources.
SharePoint	A web-based repository that the IRS uses to store and control organizational products and documentation.
SiteMinder	A user authentication and authorization component of an access management suite. It provides policy-based authentication as well as single sign-on for all web-based applications.
Standard Employee Identifier	The standard identifier for any user of an IRS system. A randomly generated five-character designation.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people.
Telnet	A telecommunications protocol providing specifications for emulating a remote computer terminal so that one can access a distant computer and function online using an interface that appears to be part of the user's local system.
User and Network Services Function	Within the IRS IT organization, it supplies and maintains all desk-side (including telephone) technology, provides workstation software standardization and security management, inventories data processing equipment, conducts annual certification of assets, and other services.
Vulnerability	A flaw or weakness in an information system's design, implementation, or operation and management that could potentially be exploited by a threat to gain unauthorized access to information, disrupt critical processing, or otherwise violate the system's security policy.

Appendix VI

Abbreviations

CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Center
EAM	Enterprise Audit Management
GAO	Government Accountability Office
IRS	Internal Revenue Service
IT	Information Technology
JAMES	Joint Audit Management Enterprise System
KISAM	Knowledge Incident/Problem Service Asset Management
PCA	Planned Corrective Action
TIGTA	Treasury Inspector General for Tax Administration