TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented

September 20, 2018

Reference Number: 2018-20-066

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

Redaction Legend:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

HIGHLIGHTS

CONTROLS CONTINUE TO NEED IMPROVEMENT TO ENSURE THAT ALL PLANNED CORRECTIVE ACTIONS FOR SECURITY WEAKNESSES ARE FULLY IMPLEMENTED AND DOCUMENTED

Highlights

Final Report issued on September 20, 2018

Highlights of Reference Number: 2018-20-066 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The IRS relies extensively on its computer systems to support both its financial and mission-related operations. Recent cyber events against the IRS have illustrated that the bad actors are continually seeking new ways to attack and exploit IRS systems and processes in order to access tax information for the purpose of identity theft and filing fraudulent tax refunds. To strengthen its security posture and protect taxpayer data, the IRS should fully implement audit recommendations related to cybersecurity.

WHY TIGTA DID THE AUDIT

This audit addresses language in the Consolidated Appropriations Act, 2017, that directed TIGTA to submit a report to the Committees on Appropriations of the House and Senate on updates to cybersecurity recommendations at the IRS. Therefore, this audit was initiated to determine whether prior TIGTA cybersecurity audit recommendations have been appropriately addressed, documented, and closed.

WHAT TIGTA FOUND

TIGTA noted significant improvement over the submission of proper forms and supporting documents after the Audit Coordination office took ownership of the Planned Corrective Action (PCA) closure process in October 2015.

However, the IRS did not fully implement the PCAs on closed TIGTA cybersecurity recommendations. Specifically, TIGTA reviewed a judgmental sample of 23 closed PCAs and found the IRS fully implemented 13 PCAs. Consequently, one PCA was not implemented and nine PCAs were only partially implemented. For example, one partially implemented PCA related to an automated asset discovery tool to provide an accurate and complete inventory of information system assets. The tool originally deployed was retired and its replacements have yet to be implemented.

TIGTA determined that improvements were needed to the documentation supporting the closure of the PCAs. Specifically, TIGTA reviewed 63 closed PCAs and found 12 had sufficient documentation. However, 19 PCAs had some documentation and 32 had no supporting documentation to support their closures. TIGTA also determined that the reviews performed by various IRS functions to verify and validate the closure process could be improved.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS should change the status of closed PCAs to open for those that were not fully implemented, and update its internal guidelines for reviewers to audit management’s corrective actions to ensure that the PCAs are fully implemented. In addition, the IRS should upload the supporting documentation for the closed PCAs that did not have sufficient documentation in the Joint Audit Management Enterprise System, and provide training to improve the development of its reviewers’ skillsets to obtain sufficient and appropriate evidence.

The IRS agreed with all the recommendations and plans to reopen the PCAs that TIGTA identified as not being fully implemented, and update its PCA review guidance to ensure that the PCAs are fully and appropriately implemented. In addition, the IRS plans to upload sufficient documentation to support the closed PCAs that TIGTA identified as not having sufficient evidence, and craft a training plan that emphasizes critical thinking and analysis skills to conduct more in-depth analytical reviews of controls and closed recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 20, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

Michael E McK

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented (Audit #201820025)

This report presents the results of our review to determine whether prior Treasury Inspector General for Tax Administration (TIGTA) audit recommendations related to cybersecurity have been appropriately addressed, documented, and closed. We initiated this audit to address language in the Consolidated Appropriations Act, 2017,[1] that was accompanied by the House-passed appropriations bill.[2] The House-passed bill directed TIGTA to submit a report to the Committees on Appropriations of the House and Senate on updates to cybersecurity recommendations at the Internal Revenue Service (IRS). This audit addresses the major management challenge of Security Over Taxpayer Data and IRS Resources.

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

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).

[1] Pub. L. No. 115-31.

[2] H.R. 5485, Financial Services and General Government Appropriations Act, 2017.

Table of Contents

Appendices

Abbreviations

BDNA	Business DNA
CFO	Chief Financial Officer
CIO	Chief Information Officer
CTO	Chief Technology Officer
FY	Fiscal Year
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
JAC	JAMES Audit Coordinator
JAMES	Joint Audit Management Enterprise System
OAR	Outreach, Assessment, and Reporting
PCA	Planned Corrective Action
TIGTA	Treasury Inspector General for Tax Administration

Background

Cybersecurity is a long-standing and serious challenge facing our Nation today. The Internal Revenue Service (IRS) relies extensively on its computer systems to support both its financial and mission-related operations. These computer systems collect and process large amounts of taxpayer data. However, the threat landscape continues to evolve, and bad actors are persistent in their pursuit of monetary gain and identity information. Recent cyber events against the IRS have illustrated that these bad actors are continually seeking new ways to attack and exploit IRS systems and processes in order to access tax information for the purpose of identity theft and filing fraudulent tax refunds.

The IRS's Cybersecurity organization manages the IRS's Security Program in accordance with the Federal Information Security Modernization Act of 2014,[3] which includes tracking compliance to security policies, continuously monitoring security risk, and providing remediation recommendations. Its mission is to protect IRS systems, services, and taxpayer information from internal and external cybersecurity-related threats by implementing world class security practices in planning, implementation, management, and operations.

From Fiscal Year (FY) 2012 through FY 2016, the Treasury Inspector General for Tax Administration (TIGTA) issued 26 audit reports containing 82 cybersecurity-related recommendations. In the IRS's management responses to these reports, it fully agreed to 77 of the 82 recommendations and partially agreed to the remaining five. The agreements included descriptions of the IRS's Planned Corrective Actions (PCA), which were recorded and tracked in the Department of the Treasury's Joint Audit Management Enterprise System (JAMES).

The JAMES is a component of the Financial Analysis and Reporting System. The reporting system serves as the Treasury Department's consolidated financial management system and collects key bureau financial, performance, and PCA data from the Treasury Department bureaus for consolidation, analysis, and reporting in products such as the annual financial report and annual performance report. The information in the JAMES is used to assess the effectiveness and progress of the IRS in correcting its internal control deficiencies and implementing corrective actions in response to audit recommendations. In addition, the JAMES allows users to run reports to assess the effectiveness of their programs.

At the IRS, the Office of Audit Coordination, hereafter referred to as the Audit Coordination office,[4] is primarily responsible for the JAMES audit tracking system, which monitors issues,

[3] Pub. L. No. 113-283. See Appendix VIII for a glossary of terms.

[4] On October 1, 2014, this office became operational under the Deputy Commissioner for Operations Support's Planning, Programming, and Audit Coordination organization. When the Office of Audit Coordination became a part of the Chief Financial Officer's office in March 2017, the office name was changed to Audit Coordination.

findings, recommendations, and the current status of the PCAs. One of the Audit Coordination office's responsibilities includes reviewing and validating all status updates entered into the JAMES by the business units' JAMES Audit Coordinators (JAC). One of the primary duties of the JAC is to prepare and submit verification of the completion of the PCAs for significant deficiencies, material weaknesses, remediation plans, and Government Accountability Office and TIGTA audit reports to the Audit Coordination office.

In TIGTA's September 2013 audit report,[5] we identified weakened management controls over closed PCAs from recommendations related to the security of systems involving taxpayer data. The report made six recommendations to the Chief Financial Officer (CFO) and the Chief Technology Officer (CTO) to help ensure that the PCAs are fully and appropriately implemented in the future. One of the six recommendations was for the CFO to conduct a periodic audit of the corrective actions for closed PCAs. The goal was to assist with providing assurance that the PCAs are fully implemented, sufficient documentation is maintained in the JAMES, and the appropriate signatures are on the required documents. To help minimize resource burden, TIGTA suggested conducting these audits annually using a statistical sample of completed PCAs.

In June 2014, the Corporate Planning and Internal Control office, hereafter referred to as the Internal Controls organization,[6] contacted the Statistics of Income Statistical Support office for assistance with designing a sampling methodology to address the TIGTA recommendation. The Statistics of Income Statistical Support office developed a sample selection methodology, determined an appropriate number of the PCAs to review, and assisted with interpreting the statistical results. The Internal Controls organization and the Statistics of Income Statistical Support office decided on a skip interval sampling process, which gives every closed PCA in the population in a given year an equal chance of being selected for review.

On October 1, 2014, the Internal Controls organization's Outreach, Assessment, and Reporting (OAR) office began performing monthly reviews, using a statistical sample of closed PCAs, to ensure that sufficient documentation was submitted to support closing the PCA. The OAR office reviews the Form 13872, *Planned Corrective Action (PCA) Status Update for TIGTA/GAO/MW/SD/TAS/REM Reports*,[7] to determine if it sufficiently supports the closure. It ensures that the narrative in the *Specific Action Taken* section supports the closure of the PCA and that the person who prepared the Form 13872 is not the same person who signed it. The OAR office records the review of each sample on Form 14668, *IRS Quality Assurance Review of Closed Planned Corrective Action (PCA) Notification*.

[5] TIGTA, Ref. No. 2013-20-117, *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Sept. 2013).
[6] On October 1, 2017, the CFO organization's Corporate Planning and Internal Control organization was renamed the Internal Controls organization.
[7] The definition of the acronyms in the title of Form 13872 that are not self-explanatory are: MW for material weakness, SD for significant deficiency, TAS for Taxpayer Advocate Service, and REM for remediation plan.

In addition to the OAR office monthly reviews, the Audit Coordination office conducts a quarterly review. On October 1, 2015, the Audit Coordination office took over ownership of tracking corrective actions to closed PCAs. They both conduct quality assurance reviews of the documentation uploaded into the JAMES by the business units in support of PCA closures. The Audit Coordination office review emphasizes the quality of the documentation and provides both review findings and suggestions to the business units on potential areas for improvement. The OAR office review focuses on verifying that sufficient documentation has been provided and provides its results to the business units on potential areas for improvement. On July 1, 2016, the Audit Coordination office began conducting its quarterly reviews using a random sample of closed PCAs. It prepares written comments for discussion with the business units and tracks the business units' responses and issue resolutions.

In December 2016, February and May 2017, and February 2018, the Audit Coordination office conducted extensive training for the JACs on the requirements and appropriate closure documentation to upload into the JAMES. In the December 2016 training, it used guidance from the *Standards for Internal Control in the Federal Government*[8] and included statements such as, "*auditors must obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions*."

The Consolidated Appropriations Act, 2017,[9] was accompanied by the House-passed appropriations bill.[10] The House-passed bill directed TIGTA to submit a report to the Committees on Appropriations of the House and Senate on updates to cybersecurity recommendations at the IRS. We performed this review with information obtained from the Information Technology organization's Cybersecurity organization in the New Carrollton Federal Building in Lanham, Maryland, and the Associate CFO, Internal Controls, Audit Coordination and OAR offices in Washington, D.C., during the period November 2017 through June 2018. 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[8] Government Accountability Office GAO-14-704G p. 48 (Sept. 2014).
[9] Pub. L. No. 115-31.
[10] H.R. 5485, Financial Services and General Government Appropriations Act, 2017.

Results of Review

The CFO addressed process deficiencies over managing, monitoring, and evaluating the closure of internal control weaknesses previously identified in our September 2013 audit report. We noted significant improvement over the submission of the proper forms and supporting documents after the Audit Coordination office took ownership of the PCA closure process. In addition, we were encouraged by the practices established by the Information Technology organization's primary JAC, whose actions were based on Internal Revenue Manual (IRM) 1.4.30, *Resource Guide for Managers, Monitoring Internal Control Planned Corrective Actions*, updated October 16, 2015. Specifically, the JAC monitors and tracks the PCAs each month and provides a summary of the open PCAs, a chart of the PCAs due in the following six-month period (broken out in 30-calendar day increments), and a table of the PCAs due in the current month's cycle (a cycle runs from the 15th of each month to the 14th of the next month).

Although the CFO's office implemented the recommended audit process and stated it implemented all of the recommendations from the September 2013 audit report, we continue to find similar conditions to the findings reported. Specifically, we identified recommendations that were not fully implemented, which resulted in some previously reported security weaknesses not being addressed. In our review of closed PCAs, we found documentation did not fully support the closure of the PCAs and insufficient documentation both in the JAMES and in the Cybersecurity organization.

IRS officials responsible for TIGTA findings and recommendations are ultimately accountable to address and resolve previously reported findings. We believe a contributing factor to why these conditions occurred was that the IRS did not fully implement TIGTA's recommendation in the FY 2013 audit report to "audit"[11] closed PCAs, which would have provided assurance that the PCAs were fully implemented and sufficient documentation was maintained. Our review of the updated IRM 1.4.30 found that the policy addressed what constituted sufficient documentation, but did not define that auditing the closed PCAs included evaluating for full implementation of the PCA.

To strengthen the IRS's cybersecurity posture and protect taxpayer data, the IRS should ensure that all TIGTA audit recommendations are fully implemented and improve the maintenance of documentation to support the actions taken.

[11] In our prior FY 2013 audit report, we used the word "audit" as a way to emphasize the need to validate corrective actions taken by the IRS to ensure full implementation. It was not our intent that the Internal Control organization should conduct "audits" like those performed by external audit organizations such as TIGTA. Rather, we believe the work done by the Internal Control organization would be part of a collaborative effort with its internal control review process and IRS business units responsible for addressing TIGTA findings and recommendations.

Corrective Actions Were Not Fully Implemented to Address Previously Identified Security Weaknesses

To assess the completion of the corrective actions the IRS took to address the weaknesses identified in prior TIGTA audits related to cybersecurity, we reviewed a judgmental sample[12] of 23 closed PCAs recorded in the JAMES as completed. Our analysis showed that 13 PCAs (57 percent) were appropriately closed as completed, and 10 PCAs (43 percent) were not fully implemented and should not have been closed. Of the 10 PCAs, one did not address the identified weaknesses and nine partially addressed the identified weaknesses. All 10 related to the security of systems that contain or provide access to taxpayer data. The following is the closed corrective action that was not fully implemented and did not address the identified weaknesses.

- **In TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget* (Sept. 2014),**[13] we recommended that the CTO incorporate a process to forward outbound unencrypted e-mail traffic with Personally Identifiable Information from licensed tax preparers/taxpayer representatives to the Office of Professional Responsibility through the business unit liaisons into the current policy and procedures. During our review, we found the corrective action had not been implemented. Specifically, an ongoing TIGTA audit[14] determined that the IRS did not incorporate the recommended process as IRS management had agreed.[15] The IRS explored the possibility of the recommendation to forward outbound unencrypted e-mail traffic to the appropriate IRS organization, but made a decision to take no action. IRS management learned that the Office of Professional Responsibility and the Return Preparer Office had no authority or jurisdiction over unlicensed/unenrolled and enrolled return preparers that were careless regarding the handling of client tax return information. In addition, IRS management made the decision without following its internal guidance[16] that directs them back to TIGTA to submit requests for cancellation/rejection of the PCAs with the appropriate justification. The guidance further provides that any related correspondence be sent to the Internal Controls organization's JAMES staff and uploaded into the JAMES as back-up documentation. We did not find a request for cancellation in the JAMES. As a result, processes and procedures to address unencrypted e-mail traffic in the Data Loss Prevention solution were not fully enhanced.

[12] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[13] We followed up on finding two, recommendation five, and PCA one.
[14] TIGTA Audit Number 201820003, *Data Loss Prevention and Exfiltration.*
[15] TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget* p. 20 (Sept. 2014).
[16] IRM 1.4.30.8.8(10), *Audit Reporting, Monitoring, and Requirements* (Oct. 16, 2015).

The following are examples of closed PCAs that were partially implemented.

- **In TIGTA, Ref. No. 2011-20-111, *Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies (Sept. 2011),***[17] we recommended that the CTO should ensure that standards and processes are developed and implemented enterprise-wide to prevent servers and workstations from being connected to the network without the proper authorization and required compliance documentation. During our review, we found that the corrective action had been partially implemented. Specifically, the IRS developed standard procedures that gave it the authority to purchase, manage, move, and maintain information technology equipment to the Information Technology organization. However, the procedures neither indicated a method nor described a method of how the Information Technology organization would prevent servers and workstations from being connected to the network without proper authorization and required compliance documentation. In another recommendation from the same TIGTA report, the IRS agreed to establish an enterprise-wide Active Directory governing body to, among other things, finalize and enforce standards. We found that another TIGTA audit followed up on the governing body recommendation. TIGTA reported[18] the Active Directory Technical Advisory Board was not providing agencywide oversight. For example, it was unaware of an upgrade to a Windows server located in an IRS organization that, in the FY 2011 report, was reported as having unidentified domains or groups with servers and/or workstations on the IRS network. The current report further stated that the Active Directory governing board failed to meet the basic requirements of its charter. It does not provide adequate governance or oversight of the IRS Application Development architecture.
- **In TIGTA, Ref. No. 2012-20-112, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sept. 2012),**[19] we recommended that the CTO ensure that the IRS completes the deployment of an automated asset discovery tool (or tools if needed), and build an accurate and complete inventory of information technology assets (including hardware and software) that reside on the IRS network. In response to the recommendation, the IRS implemented the tool, "Business DNA" (BDNA), in September 2012, which we verified and obtained inventory samples created from the system. However, the IRS stated the BDNA was retired in November 2015 because it failed to meet an updated Department of Homeland Security requirement. The IRS replaced the BDNA with two new programs that are meeting the upgraded security requirement; however, the two new programs are unable to successfully build an accurate and complete inventory of information technology assets (including hardware and software) that reside on the IRS network, which was part of the original recommendation.

[17] We followed up on finding two, recommendation one, and PCA one.

[18] TIGTA, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* pp. 4, 5 (June 2018).

[19] We followed up on finding one, recommendation one, and PCA one.

IRS officials shared that the inventory aspect of the two new programs would be implemented by September 30, 2018, but the IRS has been without this capability for more than two and one-half years. As a result, the weakness has continued to exist, and the PCA was partially implemented.

- **In TIGTA, Ref. No. 2014-23-072,** ***Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns Project*** **(Sept. 2014),**[20] we recommended that the CTO ensure that processes and procedures are developed to provide direction on how to review and mitigate weaknesses *********2********* vulnerability detection scans run on all databases. We determined the ****2**** vulnerability scans are not being run on all databases, the databases that are being scanned are not running the latest patches, multiple servers generated partial ****2**** scan results due to an incorrect scan inventory, and there are a number of critical vulnerabilities that have been identified but not mitigated. While the processes and procedures were developed, the procedures were to instruct on how to review and mitigate weaknesses, yet, we found that was not always occurring. Therefore, this PCA is partially implemented.

  We asked the IRS to provide us ***2*** scan results on its databases. It provided scan results on five databases that, among other things, house and transmit taxpayer information such as the Automated Underreporter System and the Filing Information Returns Electronically System. The security of these databases is determined at the *********2*********, which are documented in the IRS Master Inventory of the Federal Information Security Modernization Act information systems. We reviewed three of the five scan results and the related ************2************-related Security Assessment Reports and System Security Plans and determined that all weaknesses are not being identified and those that are identified, which include critical vulnerabilities, are not always mitigated. In addition, we determined that one of the databases that was subject to ****2**** scanning is now controlled with the ****2****
  *********************************2*************************************
  *********************************2*************************************
  *********************************2*************************************
  *************2*************.

- **In TIGTA, Ref. No. 2016-20-082,** ***Improvements Are Needed to Strengthen Electronic Authentication Process Controls*** **(Sept. 2016),**[21] we recommended that the Chief Information Officer (CIO) implement enhancements to audit log analysis in order to gain organizational-wide situational awareness. In addition, we recommended that the CIO compile periodic summary data of electronic authentication (eAuthentication) volume

[20] We followed up on finding one, recommendation one, and PCA one.

[21] We followed up on finding three, recommendation one, and PCA one and finding four, recommendation one, and PCA one.

and unusual activity trigger event transactions, for comparison to identify trends. TIGTA issued an audit report[22] that stated the IRS enhanced its audit log analysis capabilities. However, it stated that additional work is needed to ensure that eAuthentication audit log review, analysis, and reporting processes provide useful information to support investigation and response to suspicious activities. During our review, the Cybersecurity organization provided supporting documentation of the enhancements that were included in the TIGTA-issued report. In addition, the Cybersecurity organization stated that it implemented a second enhancement in September 2017 after TIGTA completed its fieldwork for the issued report. The enhancement was to the eAuthentication audit plan because the current thresholds were not producing actionable events. At the end of our fieldwork, the Cybersecurity organization provided evidence of threshold comparisons and updates, and a monitoring road map for applications. However, it was not sufficient for use in the reporting process for gaining situational awareness. Specifically, reports generated from the log analyses have not been shared with investigative outlets to gain situational awareness. For this PCA, we concluded that it is partially implemented.

For the second PCA that addressed the compilation of periodic summary data recommendation, the Cybersecurity organization provided reports for our review that included trigger event transactions that showed comparisons to identify trends. For this PCA, we concluded the Cybersecurity organization addressed the original weakness. However, the documentation will need to be uploaded in the JAMES as sufficient documentation.

Appendix V provides the details of our assessment of the 10 closed PCAs that were not fully implemented. The Information Technology organization JAC receives the documentation from the business unit/functional coordinators and reviews for proof of implementation and an understanding of how the actions taken meet the PCA requirements. The JAC leaves the details about the corrective actions to those responsible for implementing the corrective actions. As reported earlier, the Internal Controls organization is auditing the documentation in the JAMES for closed PCAs; however, it is not auditing to ensure that the PCAs are fully implemented, as we recommended in the September 2013 TIGTA report. As was reported in FY 2013, the reasoning is that they lack the expertise to evaluate the effectiveness of the completed corrective action. We believe the CFO's organization has a good foundation and processes in place to better evaluate the IRS's effectiveness on addressing audit recommendations and the PCAs. As our current audit has shown, the IRS continues to close PCAs that have not been fully implemented.

Until the auditing process includes a review to determine whether the closed PCAs addressed the weaknesses that caused the findings and the recommendations, the Internal Controls organization along with the Information Technology organization JAC will miss an opportunity to help ensure

[22] TIGTA, Ref. No. 2018-20-007, *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented* (Feb. 2018).

that the PCAs are fully and appropriately implemented in the future. In addition, the IRS misses an opportunity to assess its effectiveness and progress in correcting internal control deficiencies.

Recommendations

The Chief Information Officer should:

Recommendation 1: Change the PCA status from closed to open in the JAMES for the corrective actions TIGTA identified as not fully implemented and the status of the PCAs should remain open until they are fully implemented.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity organization will work with the Office of Strategy and Planning to reopen the PCAs TIGTA identified as not fully implemented. The PCAs will remain open in the JAMES until they are fully implemented.

Recommendation 2: Reopen the closed PCA associated with TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget*, and comply with the IRS's internal guidance to submit a request with justification for the cancellation/rejection of the PCA to TIGTA for review and action. Once TIGTA provides a response, the information should be forwarded to the Internal Controls organization for uploading into the JAMES.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity organization will work with the Office of Strategy and Planning to reopen the PCA associated with TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget*, and comply with the IRS's internal guidance to submit a request with justification for the cancellation/rejection of the PCA to TIGTA for review and action. Once TIGTA provides a response, the information will be forwarded to the Internal Controls organization for uploading into the JAMES.

The Chief Financial Officer should:

Recommendation 3: Update the IRM to broaden the Audit Coordination and OAR offices auditing to include reviewing management's corrective actions to ensure that the PCAs are fully and appropriately implemented.

> **Management's Response:** The IRS generally agreed with this recommendation. The Audit Coordination and OAR offices are two separate offices within the Internal Controls organization. The Audit Coordination office will own the responsibility for performing quality checks of closed PCAs, which will involve obtaining a sample and reviewing the PCAs in the sample to assess whether they are properly documented with adequate supporting justification. The OAR office has an Internal Control Review section that will review previously audited areas and closed recommendations (and

accompanying PCAs) to evaluate whether corrective actions have been fully implemented and appear effective. Policies and procedures for both offices are currently being updated or developed as appropriate. It will not be possible to review all, or even a majority of recommendations via either program due to volume and resource constraints, but sampling and selection methodologies will be incorporated into our IRM and/or operating procedures.

Office of Audit Comment: Although IRS management generally agreed with the recommendation, we believe their planned corrective actions are responsive to the recommendation.

Some Supporting Documentation Is Being Maintained, but Improvements Are Needed

In the September 2013 TIGTA audit report in which we reviewed 69 closed PCAs for the period of October 2008 through December 2012, we reported that 65 percent of the PCAs did not have documentation to fully support the closure of the PCAs. Additionally, we found 82 percent of the PCAs did not have any additional supporting documentation uploaded to the JAMES, and 100 percent were not audited to ensure that their implementation was completed. As previously stated, we noted organizational changes, implemented policies and procedures, and training initiatives to educate the JAMES user community on the proper documentation needed to close a corrective action. While these efforts were positive steps to improve the closure process, we found similar conditions to those reported in September 2013, although we noted decreases in the percentages for the conditions previously reported. We also noted that, although the Internal Controls organization is conducting audits of the closed PCAs, the audits were generally designed to only "audit" whether the supporting documentation was uploaded into the JAMES, the Form 13872 included the appropriate executive approvals, and the documentation supports the PCA closure.

Supporting documentation for completed PCAs in the JAMES can be improved

To determine whether there was improvement in the IRS placing supporting documentation in the JAMES, we reviewed the documentation in the JAMES for 63 closed PCAs.[23] We determined that:

- 32 (51 percent) PCAs had the required Forms 13872 in the JAMES, but no other additional documentation to support closing the corrective actions.

[23] Of the 82 cybersecurity-related recommendations, 63 required documentation in the JAMES, and 13 were closed when the IRS issued its management response to the respective draft reports, until April 1, 2017, when the Audit Coordination office did not require documentation to be added to the JAMES. We determined that the remaining six PCAs were still open.

- 19 (30 percent) PCAs had the required Forms 13872 and additional supporting documentation in the JAMES.
- 12 (19 percent) PCAs had sufficient documentation to support the corrective actions the IRS took.

We further determined the effectiveness of the documentation in the JAMES over three different time periods using the 63 closed PCAs. Figure 1 captures the results of the assessed effectiveness using the following three criteria:

- From November 1, 2010, when the Treasury Department mandated that its bureaus upload supporting documentation to the JAMES, to April 25, 2013, before the effective date of the IRS's Internal Controls office mandate. On April 26, 2013, the Internal Controls office took a major step to strengthen the IRS's management control program by publishing the new IRM 1.4.30, *Monitoring Internal Control Planned Corrective Actions*, to strengthen existing policies and procedures on internal controls.
- From April 26, 2013, the effective date of the IRM mandate, to September 30, 2015, the date prior to when the Audit Coordination office transitioned from the Office of Internal Controls and began tracking the corrective actions.
- From October 1, 2015, to March 12, 2018, the latest closed PCA date in our population.

Figure 1: TIGTA's Assessment of the Effectiveness of Documentation in the JAMES for the 63 Closed PCAs

Time Period	Total PCAs Closed During Each Time Period		No Additional Supporting Documentation in the JAMES Besides the Form 13872	Some but Not Enough Additional Supporting Documentation in the JAMES With the Form 13872	Sufficient Documentation in the JAMES to Support Closing the PCA
November 1, 2010, through April 25, 2013	14		14	0	0
April 26, 2013, through September 30, 2015	29		18	7	4
October 1, 2015, through March 12, 2018	20		0	12	8
Total	**63**		**32**	**19**	**12**

Source: TIGTA's assessment of the supporting documentation for the 63 closed PCAs for TIGTA reports from FYs 2012 through 2016.

The results from our analysis supported that the IRS showed incremental improvement from one time period to the next.

- 14 (100 percent) of the 14 closed PCAs for the November 1, 2010, through April 25, 2013, time period did not have supporting documentation for each PCA closure other than the Form 13872, which the Treasury Department required to be uploaded into the JAMES but also made the storing of supporting documentation feature on JAMES mandatory.
- 11 (38 percent) of the 29 closed PCAs for the April 26, 2013, through September 30, 2015, time period had some or all additional supporting documentation in the JAMES. However, only four (14 percent) of the 29 closed PCAs had sufficient documentation in the JAMES to support closing the PCA. For this period, the CFO issued IRM.1.4.30.6.8.(5)a, *Audit Reporting, Monitoring, and Requirements*, requiring that it is **mandatory** that all supporting documentation be stored in the JAMES. The completed, signed, and dated Form 13872 or other executive certification document must be uploaded and attached in the JAMES at the time the PCA is updated.
- 20 (100 percent) of the 20 closed PCAs for the October 1, 2015, through March 12, 2018, time period had some or all additional documentation in the JAMES. However, only eight (40 percent) of the 20 closed PCAs had sufficient documentation in the JAMES to support closing the PCA. The Internal Controls organization has controls in place that include training initiatives for the IRS's JACs and audits that the Audit Coordination and OAR offices conduct for the sufficient documentation.

Supporting documentation for closed PCAs stored outside the JAMES can be improved

As previously presented, we only found 12 of the 63 recommendations in our sample had sufficient documentation in the JAMES to support the closed PCA. For the remaining 51 recommendations, we engaged IRS functional offices that were responsible for the completion of the PCAs to our recommendations and requested whether additional documentation existed to support the closures.

In some cases, the IRS had difficulty locating and providing documentation. For example, we only received documentation for 20 (39 percent) of the 51 closed PCAs after one month from our request. When we expressed our concern about the delays, Cybersecurity organization personnel stated that the delays were primarily due to the unavailability of subject matter experts to obtain the documentation. These experts either left the IRS or were in different jobs elsewhere within the IRS. After two months from our initial request, we received additional documents for review for most of the recommendations in our sample. Figure 2 presents the results of our assessment, followed by examples from our results that show our concerns with the sufficient documentation.

Figure 2: The Retention of Documentation in the Information Technology Organization External to the JAMES for 51 Closed PCAs

Time Period	The PCAs Closed During Each Time Period	Documentation Provided Fully Supported PCA Closures	Documentation Provided Partially Supported PCA Closures	Documentation Provided Did Not Support PCA Closures	No Additional Documentation Provided
November 1, 2010, through April 25, 2013	14	9	3	1	1
April 26, 2013, through September 30, 2015	25	17	6	2	0
October 1, 2015, through March 12, 2018	12	8	1	3	0
Total	**51**	**34**	**10**	**6**	**1**

Source: TIGTA's assessment of the supporting documentation for the 51 closed PCAs for TIGTA reports from FYs 2012 through 2016.

For the 51 closed PCAs that we requested additional information from the Information Technology organization to support the PCA closures, we found:

- 34 (67 percent) had sufficient documentation to support closing the PCAs.
- 10 (19 percent) had documentation to partially support closing the PCAs.
- 6 (12 percent) had documentation that did not support the closed PCAs.
- 1 (2 percent) had no supporting documentation.

IRM 1.4.30.6.(7)l and u, *Roles and Responsibilities*, for the JACs requires them to maintain complete audit files to include documentation and ensure sufficient documentation supporting a PCA closure is available for five years after the fiscal year in which the PCA was closed. In September 2010, the Treasury Department updated the retention period for source documentation in the JAMES from five to nine years. While the previously stated IRM addresses documentation stored with the JACs, generally, that documentation is stored in the JAMES too. However, there are instances when the JACs maintain supporting documentation that cannot be uploaded to the JAMES because of its sensitive nature. These documents should be subject to the Treasury Department's updated retention period because they should be in the JAMES but cannot be added. For ease in managing the retention of supporting documentation in the JAMES and outside of it, and to prevent the use of two retention periods, we believe the IRS should update its IRM and align it with the Treasury Department's updated requirement to ensure that all documents are appropriately retained.

IRM 1.4.30.7(1)a and b, *Requirements Governing the Internal Control Process*, provides that the heads of all business operating divisions should adhere to the requirements governing the internal control process for the JAMES by emphasizing the importance of following the guidance in the IRM, the maintenance of supporting documentation, and the certification that corrective actions are met. The heads of all business operating divisions should adhere to the JAMES process by directing business operating divisions' internal control staff to review and update their existing guidance, as necessary, to align with the IRM. Additionally, the Government Accountability Office's *Standards for Internal Control in the Federal Government*[24] provides that all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. In addition, all documentation and records should be properly managed and maintained.

The following are examples of the closed PCAs in which the documentation to support the actions taken could be improved.

- **In TIGTA, Ref. No. 2012-20-115, *Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected* (Sept. 2012),**[25] we recommended the Assistant[26] CIO, Cybersecurity, should appoint a certified project manager with the requisite training and experience to lead the Internal Identity and Access Management project and provide sufficient full-time staffing and resources to the project. The IRS planned to appoint a qualified project manager and to provide the necessary project resources to the project as documented in the Information Technology Integrated Release Plan.

  We found that the JAMES did not have any documentation to support the PCA closure, so we requested:

  - Supporting documents to show that a project manager was appointed and remains within the Information Technology Security Implementation group. During the audit, Cybersecurity organization personnel responded they were unable to find any supporting documentation.
  - Supporting documents to show the project manager has the requisite training and experience to lead the project. During the audit, Cybersecurity organization personnel responded they were unable to find any supporting documentation.
  - Supporting documents to show that the project had or has full-time staffing. During the audit, Cybersecurity organization personnel responded that they were unable to find any supporting documentation as to the level the work was resourced. However,

[24] Government Accountability Office GAO-14-704G p. 48 (Sept. 2014).
[25] We followed up on finding one, recommendation two, and PCA one.
[26] The title "Assistant" was part of the CIO, Cybersecurity's title in 2012 and was shown in the reported recommendation. The title has since been changed to "Associate."

their metrics would indicate that there were sufficient resources assigned to achieve the desired outcome. The information provided did not identify the metrics.

- A copy of the Information Technology Integrated Release Plan. During the audit, Cybersecurity organization personnel responded, "*we do not have a copy of the plan for that time period; it was managed by another area of the Information Technology organization*."

After our fieldwork ended, the IRS provided additional information that included limited details about certified project managers and metrics. For the certified project managers, the IRS did not provide information about the managers' certification or training. For the metrics, the IRS provided documentation that supports progress in the development of two-factor authentication for users and in the virtual private network. However, the documentation shows the IRS needs to improve in developing two-factor authentication for applications. As of March 2018, nine of 130 applications have been enabled with two-factor authentication. This area was part of the reason for recommending a certified project manager to lead the Internal Identity and Access Management project.

- **In TIGTA, Ref. No. 2013-20-127, *While Efforts Are Ongoing to Deploy a Secure Mechanism to Verify Taxpayer Identities, the Public Still Cannot Access Their Tax Account Information Via the Internet* (Sept. 2013),**[27] we recommended the Associate CIO, Cybersecurity, should continue the efforts to acquire appropriate software to enable additional reporting functionality. The IRS referenced the eAuthentication Release 2 project, as already planned, which included integration with existing internal enterprise capabilities to enable broad management information system reporting. This would allow the project to configure the system to produce approved business reports, such as application specific reports, taxpayer account reports, and system infrastructure reports. We requested any test reports that were conducted during the implementation phase to show the report capability was working, such as examples (at least three of each) of any application specific reports, taxpayer account reports, and system infrastructure reports generated during the period of March 2014 to February 2018, and any other supporting documents that are on file that the IRS mentioned in its specific action taken. Cybersecurity organization personnel responded that the Application Development organization point of contact did not have any additional supporting documentation to provide for the PCA. After our fieldwork ended, the IRS provided the majority of the reports we requested. These documents need to be uploaded to the JAMES.

- **In TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012),**[28] we recommended that the CTO should implement oversight of Windows server security at the enterprise-level.

[27] We followed up on finding three, recommendation one, and PCA one.
[28] We followed up on finding one, recommendation one, and PCA one.

This enterprise-level oversight should enforce the standardization of group policy and ensure effective monitoring and remediation of weaknesses reported by the Windows Policy Checker and nCircle scans. We found the Form 13872 was the only document in the JAMES, so we requested: 1) supporting documents that showed the IRS implemented oversight of the Windows server security at the enterprise-level; 2) standard operating procedures or the name of the specific IRM section that provides the Cybersecurity organization is monitoring and enforcing adherence to the Window server security policies; 3) supporting documents that show the Cybersecurity organization's monitoring and enforcing effort; and 4) any supporting documents to show the Cybersecurity organization partnered with the business units to develop remediation plans.

We also requested a few (three, if available) copies of the remediation plans developed in Calendar Years 2013 through 2018 to conduct not only the documentation review, but to determine whether the corrective action addressed the weaknesses identified in the TIGTA report. For sufficiency of documentation, Cybersecurity organization personnel provided the requested documentation and additional information needed; however, the additional documentation was still not sufficient. We obtained access to the Treasury Department's Federal Information Security Modernization Act Inventory Management System to determine whether the Plans of Action and Milestones were prepared as part of the remediation plans and whether they were open or closed to complete our review. All the documentation will need to be uploaded to the JAMES for availability for the appropriate retention period after the fiscal year in which the PCA was closed.

Disparity exists between TIGTA, Audit Coordination office, and OAR office audits for sufficient documentation

We reviewed the results of the Audit Coordination and the OAR offices' periodic reviews of closed PCAs to determine the types of trends they were identifying with sufficient documentation to compare them to the trends TIGTA identified in our review of the 63 closed PCAs. For the Audit Coordination office, we looked at its quarterly review results beginning with FY 2016[29] through the first quarter of FY 2018. For consistency and trending, we selected the same period for the OAR office's monthly reviews. We determined there is a disparity between what TIGTA considers as sufficient documentation to close the PCAs and what the Information Technology organization JAC and the Internal Controls organization personnel consider as sufficient documentation. While TIGTA, the Internal Controls organization, and the JAC evaluate sufficient documentation using the same basic criteria – the Form 13872, which presents the recommendation and the action the IRS took to respond to it, TIGTA seeks more verification or documentation to corroborate statements and actions that the IRS took to arrive at

[29] The Audit Coordination office's FY 2016 results were from its pilot review that was used internally to assess its effectiveness and were not shared with the IRS business units. The Audit Coordination office began sharing its results with the business units in the first quarter of FY 2017.

reasonable evidence. The Internal Controls organization stated in its December 2016 training on appropriate documentation that, "*auditors must obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions*." It further stated in the "Secrets of Effective Documentation" section that, "*Although an information source might be considered reliable, verification of accuracy should be documented.*" Lastly, the training material stated that "*If you didn't document it[,] it didn't happen*."

- **For the Audit Coordination office quarterly review results**, we identified six closed PCAs for the Information Technology organization that were reviewed for the period. However, the Audit Coordination office did not look at closed PCAs for the Cybersecurity organization. We examined the Audit Coordination office results and determined that in four of the closed PCAs, the reviewers found that the documentation in the JAMES was sufficient to support closing the PCA. In the remaining two, the documentation was not necessary to be loaded in the JAMES because the recommendation was addressed when the IRS signed the management's response.[30] None of the six were included in our population of 63 closed PCAs; therefore, we were unable to conduct any comparisons for trends.

- **For the OAR office monthly review results**, we identified seven closed PCAs for the Cybersecurity organization that were reviewed for the period. The OAR office provided us the documentation it reviewed to decide sufficiency, if the requirement to maintain documentation in the JAMES was applicable, or if the documentation was available. We found:

  - In three PCAs, the corrective actions were taken prior to management's response; therefore, there was no documentation for the OAR office to review. We compared the dates the IRS took corrective actions with the dates of the management's responses, reviewed the procedure that documentation was not required, and agreed with the OAR office's assessments.

  - In two PCAs that the IRS closed after management's response was signed, the OAR office determined there was sufficient documentation in the JAMES to support the closure. We agreed that the documentation was sufficient.

  - In two PCAs that the IRS closed after management's response was signed, the OAR office determined there was sufficient documentation in the JAMES to support the closure. The documentation the OAR office used to determine sufficiency was not available to us; therefore, we disagreed that the documentation in the JAMES was sufficient. One of the two PCAs was included in our population of 63. Unlike the OAR office, we determined the IRS did not have sufficient documentation in the JAMES and requested the Cybersecurity organization provide additional

[30] Prior to April 1, 2017, the Audit Coordination office did not require the IRS to add documentation to the JAMES if the IRS took corrective action prior to signing the management's response to TIGTA draft reports.

documentation. After receipt, we concluded that the additional documentation was sufficient and that it should be uploaded to the JAMES.

Because our results differed with the OAR office for sufficient documentation in the JAMES, we expanded our testing to the 22 closed PCAs associated with the six TIGTA reports that produced six[31] of the seven sampled PCAs the OAR office reviewed. We determined whether the 22 PCAs were included in our audited population of 63.

- For 10 (45 percent) closed PCAs, we were unable to determine whether the documentation was sufficient because the closed PCAs were not included in our population of closed PCAs.
- For eight (36 percent) closed PCAs, we requested additional documentation from Cybersecurity organization personnel because the JAMES did not contain sufficient documentation. They provided the additional documentation for our review, and we determined that in six of the eight, the documentation was sufficient for closing the PCAs. In the remaining two PCAs, the additional documentation was not sufficient to close the PCAs. Because the documentation was outside of the JAMES, it will need to be uploaded in the JAMES as support for the actions the IRS completed.
- For four (18 percent) closed PCAs, there was sufficient documentation in the JAMES to support closing the PCAs.

Without an effective management control process, the CFO cannot be assured that the management control program is operating as intended, which includes assessing the effectiveness and progress of the IRS in correcting its internal control deficiencies and implementing corrective actions in response to audit recommendations. When this happens, the IRS cannot assure its stakeholders, which includes the Treasury Department, that the PCAs were implemented as reported in correcting security vulnerabilities and that the information in the JAMES is reliable. The Treasury Department produces the annual financial report and the annual performance report that serves as congressional justification for appropriated dollars. It is imperative that the information in the JAMES is reliable and that the developed processes to assist with supporting the management control process are effective.

[31] The seventh TIGTA report produced six closed recommendations that IRS management corrected before the management's response was signed. We did not conduct independent testing because the report was not in our review population.

Recommendations

The Chief Financial Officer should:

Recommendation 4: Ensure that the Associate CFO, Internal Controls, works with the Cybersecurity organization to upload the supporting documentation for the 51 closed PCAs TIGTA determined did not have sufficient documentation in the JAMES, provided that the appropriate PCA retention period after the fiscal year in which the PCA was closed has not expired.

> **Management's Response:** The IRS agreed with this recommendation. The designated officials will coordinate staff efforts to ensure that they upload appropriate documentation, with the caveat that the documentation will be reviewed before it is uploaded to ensure that it contains no Personally Identifiable Information or other sensitive data, because the JAMES is neither an IRS system nor a secure database. The IRS will not upload documentation found to contain such information but will retain it according to appropriate guidelines.

Recommendation 5: Ensure that Internal Controls organization reviewers improve the development of their skillsets to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions. Part of the development could include attending audit evidence training courses offered by the Federal Government and the private sector.

> **Management's Response:** The IRS agreed with this recommendation. The IRS is expanding the Internal Controls organization's Internal Control Review section, and existing staff are crafting a training plan that will emphasize critical thinking and analysis skills. The IRS appreciates the suggestion about audit evidence training courses and will try to identify such training opportunities. Because the Internal Control Review section will be conducting the more in-depth analytical reviews of controls and closed recommendations, the training plan development activities will focus on these staff.

Recommendation 6: Update the retention period in the IRM for maintaining documentation with the JACs to align with the Treasury Department's retention period for maintaining supporting documentation in the JAMES.

> **Management's Response:** The IRS agreed with this recommendation. The new Audit Coordination IRM will include a requirement that the IRS maintains documentation supporting PCA closures not uploaded into the JAMES for a period consistent with that specified in the Treasury Department's guidance for data retention in the JAMES.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether prior TIGTA audit recommendations related to cybersecurity have been appropriately addressed, documented, and closed. To accomplish our objective, we:

I. Determined whether the IRS, specifically the Audit Coordination office in the CFO's office and the Cybersecurity organization, has an effective process and is complying with requirements in closing the PCAs.

   A. Identified and reviewed policies, procedures, and guidelines related to the identification, tracking, and closing of the PCAs reported in the JAMES.

   B. Interviewed JAC personnel within the Cybersecurity organization to determine the process used for tracking and closing the PCAs.

   C. Identified discrepancies between the process in place and the policies and guidelines, and interviewed appropriate personnel to determine the causes of the variances.

   D. Evaluated the process to determine whether it is effective in closing the PCAs and if any improvements could be made to the process to increase effectiveness and efficiency.

II. Determined whether the Audit Coordination office and the Cybersecurity organization maintain required documentation to support actions taken on 82 TIGTA recommendations with which IRS management agreed[1] and is responsible for addressing.

   A. Reviewed TIGTA Security and Information Technology Services audit reports from FY 2012 through FY 2016 to identify all audit reports related to cybersecurity.

   B. Using the list in Step II.A., obtained the JAMES summary report on all recommendations related to cybersecurity.

   C. Identified the status of the recommendations.

   D. Summarized the status of all TIGTA recommendations, *e.g.*, open, closed, or rejected, identified from the reports listed in the Security and Information Technology Services Annual Assessment and sensitive but unclassified audit reports from FY 2012 through FY 2016.

[1] Fully and partially agreed recommendations.

E. Determined whether the required additional supporting documentation was recorded. If additional supporting documentation was not recorded, we determined why through interviews and review of the information in the JAMES.

III. Determined whether the Cybersecurity organization’s actions taken on cybersecurity-related PCAs addressed report findings and recommendations.

A. Selected the population of cybersecurity recommendations from TIGTA reports from FY 2012 through FY 2016.

B. Selected a judgmental sample[2] of 23 from 63 closed PCAs for the period FY 2012 through FY 2016 and conducted on-site validation of the systems to ensure that the PCAs have been fully implemented, and weaknesses have been corrected and remain corrected if the IRS indicates that the weaknesses have been corrected. Either we conducted site visits and appropriate tests to validate the claims, as appropriate, or we relied on the audit work of other auditors because they were conducting follow-up audits of some of the PCAs in our sample.

C. Evaluated the Cybersecurity organization’s supporting documentation for each recommendation.

1. Determined whether the documentation supported implementation of the PCA and the closure of the weakness.

2. Evaluated and determined whether the action taken to correct the weakness/finding was fully implemented.

D. Determined whether the Cybersecurity organization through the CIO obtained concurrence from TIGTA on the PCAs that were cancelled.

E. Determined whether the Internal Controls organization, responsible for monitoring and the proper closure of the PCAs prior to the establishment of the Audit Coordination office, and the Audit Coordination and the OAR offices reviewed the supporting documentation of agreed-upon PCAs for sufficient documentation submitted to support closing the PCAs.

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 Office of Internal Controls,

[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population. We judgmentally selected closed PCAs based on the location of points of contacts and subject matter experts.

and Audit Coordination and OAR offices' policies, procedures, and practices for the identification, tracking, and closing of the PCAs reported in the JAMES, and the Cybersecurity organization's policies, procedures, and practices for addressing and documenting the PCAs reported in the JAMES. We evaluated these controls by interviewing the JAC for the Information Technology organization, reviewing relevant IRM sections and other guidance documents as appropriate, reviewing documents supporting the closure of the PCAs, and validating a sample of the PCAs.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Deborah Smallwood, Audit Manager
Cindy Harris, Lead Auditor
Michael Segall, Senior Auditor
Linda Nethery, Information Technology Specialist

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Financial Officer
Chief Information Officer
Deputy Chief Financial Officer
Deputy Chief Information Officer for Operations
Associate Chief Financial Officer for Internal Controls
Associate Chief Information Officer, Cybersecurity
Director, Corporate Budget and Strategic Planning
Director, Outreach, Assessment, and Reporting
Director, Office of Audit Coordination

Appendix IV

Outcome Measure

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; 10 closed PCAs were not fully implemented; therefore, the weaknesses were not corrected (see page 5).

Methodology Used to Measure the Reported Benefit:

Using a judgmental[1] sample of 23 PCAs, we found that nine of the sampled closed PCAs were partially implemented and the remaining one was not implemented because of IRS actions. Because the weaknesses were not corrected, they were all prematurely closed off the JAMES and should be reopened.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 51 closed PCAs did not have sufficient documentation stored in the JAMES to support their closure (see page 10).

Methodology Used to Measure the Reported Benefit:

We determined that 51 of 63 closed PCAs did not have sufficient documentation uploaded in the JAMES to support closing the PCAs. As a result, we requested additional documentation from the Information Technology organization that yielded the following results, for:

- 34 (67 percent) of the 51 closed PCAs, sufficient documentation was provided to support closing the PCAs.
- 10 (19 percent) of the 51 closed PCAs, the documentation provided partially supported closing the PCAs.
- 6 (12 percent) of the 51 closed PCAs, the documentation provided did not support the closed PCAs.
- 1 (2 percent) of the 51 closed PCAs, no supporting documentation was provided.

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

As a result, the IRS needs to upload documentation for the closed PCAs that we determined had insufficient documentation in the JAMES providing that the appropriate PCA retention period after the fiscal year in which the PCA was closed has not expired.

Appendix V

Assessment of 10 Planned Corrective Actions That Were Not Fully Implemented

Weaknesses From Issued Audit Reports	Recommendations	PCAs	Specific Actions Taken	TIGTA's Assessment of Corrective Actions
Ref. No. 2011-20-111 PCA 2-1-1[1] Not all Windows servers and workstations connected to the network reside in authorized domains.[2]	The CTO should ensure that standards and processes are developed and implemented enterprise-wide to prevent servers and workstations from being connected to the network without the proper authorization and required compliance documentation.	The IRS agreed with the recommendation. The IRS will ensure that standards and processes are developed and implemented enterprise-wide to prevent servers and workstations from being connected to the network without proper authorization and required compliance documentation.	The IRS developed standard procedures that gave it the authority to purchase, manage, move, and maintain information technology equipment to the Information Technology organization.	**Implementation: Partial** Although procedures were developed, neither indicated a method nor described a method of how the Information Technology organization would prevent servers and workstations from being connected to the network without proper authorization and required compliance documentation.

[1] The PCA reference number used throughout Appendix V consists of three numbers, which coincide with information in the JAMES from the referenced audit report. The first number accounts for the placement of the finding in the report, the second number is the report's recommendation number, and the third number is the IRS's corrective action for that recommendation, which is from management's response to the audit report.

[2] See Appendix VIII for a glossary of terms.

Weaknesses From Issued Audit Reports	Recommendations	PCAs	Specific Actions Taken	TIGTA's Assessment of Corrective Actions
Ref. No. 2011-20-111 PCA 2-2-1 Not all Windows servers and workstations connected to the network reside in authorized domains.	The CTO should ensure that scanning tools, such as the BDNA, are utilized to locate unauthorized servers, workstations, and domains on the IRS network, and adequate procedures are developed and implemented to ensure that they are removed.	The IRS agreed with the recommendation to use automated scanning tools for asset identification and has been in the process of implementing this capability, even prior to this audit. IRM 2.14.1[3] defines the process for inventory reconciliation of all information technology assets. The IRS will ensure that the IRM addresses the issue of the proper handling and potential removal of any unauthorized assets found, regardless of how discovered.	The IRS has implemented a wireless security program through the use of the BDNA tool to identify servers, workstations, and domains. In addition, procedures have been updated to ensure proper handling of any unauthorized assets found.	**Implementation: Partial** The IRS implemented the BDNA scans tool; however, the IRS retired it on November 30, 2015. According to the IRS, the ForeScout tool, which is used, can identify every device on the network. However, it cannot produce a report without including duplicate results showing devices with multiple connections. As a result, the IRS uses ForeScout to merge with other tools, but the duplicate information is still included. Because the servers, workstations, and domains cannot be clearly identified, the PCA is partially implemented.
Ref. No. 2012-20-063 PCA 1-1-1 Windows server security settings did not always comply with standards.	The CTO should implement oversight of Windows server security at the enterprise-level. This enterprise-level oversight should enforce the standardization of group policy and ensure effective monitoring and remediation of weaknesses reported by the Windows Policy Checker and nCircle scans.	The IRS agreed with this recommendation. The IRS will implement oversight of Windows server security at the enterprise-level. The Cybersecurity organization will monitor and enforce adherence to the Windows server security policies by scanning reports and partnering with the business operating divisions to develop remediation plans.	The IRS has implemented oversight of Windows server security at the enterprise-level. The Information Technology organization Cybersecurity organization is monitoring and enforcing adherence to Windows server security policies by scanning reports and partnering with the business operating divisions to develop remediation plans.	**Implementation: Partial** Although the Cybersecurity organization provided all of the requested documents, the documents provided do not support the closure of the PCA. We determined that monitoring was occurring for Tripwire vulnerability scans, but not for Windows Policy Checker scans. We determined that remediation may not be done consistently for findings noted on both Windows Policy Checker and Tripwire scans.

[3] IRM 2.14.1, *Information Technology Asset Management* (Nov. 8, 2011), has since been replaced with IRM 2.149.1; *Information Technology Asset Management* (Sept. 23, 2015); IRM 2.149.2, *Asset Management Process Description* (Oct. 19, 2015); IRM 2.149.3, *Asset Management Hardware Procedures* (Oct. 19, 2015); and IRM 2.149.4, *Asset Management Software Procedures* (Sept. 23, 2015).

Weaknesses From Issued Audit Reports	Recommendations	PCAs	Specific Actions Taken	TIGTA's Assessment of Corrective Actions
Ref. No. 2012-20-099 PCA 1-4-1 Process improvements are needed to ensure that audit trails effectively support unauthorized access investigations.	Revise policies and procedures to ensure that timestamp guidance is clear and readily available to application owners. Guidance should include which devices serve as authoritative time servers for synchronization, how to configure local systems to synchronize with authoritative time servers, and where to locate assistance if needed.	The IRS partially agreed with this recommendation. Guidance that describes which devices serve as authoritative time servers and how local systems are configured to align with those servers did exist, but was not readily available for the auditors. The IRS will review existing policies and procedures for timestamps and ensure that the guidance is clear and available to all stakeholders.	The IRS updated ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** Guidance that describes which devices serve as authoritative time servers and how local systems are configured to align with those servers now exist.	**Implementation: Partial** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** ***************2************** Neither is it specified in the other named IRM references. TIGTA issued an Office of Audit Comment explaining that the IRS needs to adequately document or log the actual time zone in the Audit Plan or within the audit trail. The current process leaves time zones up to interpretation, which can be detrimental to any administrative or criminal investigation, and resulting adjudications of potential unauthorized access cases.
Ref. No. 2012-20-112 PCA 1-1-1 An automated means to control inventory information technology assets has not been fully implemented.	The CTO should ensure that the IRS completes the deployment of an automated asset discovery tool (or tools if needed) and builds an accurate and complete inventory of information technology assets (including hardware and software) that reside on the IRS network.	The IRS agreed with this recommendation. The BDNA is an automated asset discovery tool for non-mainframe networked systems. The IRS will complete the BDNA deployment by October 2012. Once deployed, enterprise assets will be provisioned with BDNA credentials, and the BDNA will assist in building an accurate and complete hardware and software inventory for the Knowledge Incident/Problem Service Asset Management system. The BDNA will provide data in accordance with National Institute of Standards and Technology 800-40, section 2.2.1, that addresses information technology inventory for network port, software configuration, and hardware configuration.	The BDNA exited enterprise lifecycle milestone 4b on September 26, 2012, completing its deployment. Provisioning of BDNA credentials for agency-wide asset discovery is completed. The BDNA asset discovery data are imported into the cybersecurity data warehouse where the data are available to the Knowledge Incident/Problem Service Asset Management system, the IRS's official enterprise asset management system. BDNA asset data were available for import into the cybersecurity data warehouse and address information technology inventory for network port, software configuration, and hardware configuration, according to National Institute of Standards and Technology 800-40, section 2.2.1.	**Implementation: Partial** The IRS provided documentation demonstrating the implementation and samples of inventories created from the system. However, the BDNA was retired in November 2015. The IRS acquired two new programs to replace and upgrade the functions of the BDNA. However, those two programs are not yet building inventories. Therefore, the original weakness identified has reoccurred.

Weaknesses From Issued Audit Reports	Recommendations	PCAs	Specific Actions Taken	TIGTA's Assessment of Corrective Actions
Ref. No. 2012-20-122 PCA 3-2-1 Identified security issues need to be resolved.	The CTO should ensure that all database issues identified by the *****2***** scan are resolved or an action plan is developed with specific corrective actions and time periods.	The IRS agreed with this recommendation. The Cybersecurity organization worked with the Enterprise Operations organization using an ad hoc process to triage the initial vulnerability findings. A formal process is currently under development.	The IRS has ensured that all database issues identified by database scans executed by the Information Technology organization Cybersecurity organization, using the *****2***** tool, have been resolved or have a Plan of Action and Milestones developed. Each Plan of Action and Milestones has specific corrective actions and time periods included.	**Implementation: Partial** The IRS was unable to provide a list of the scan findings from the original report. IRS officials stated that during the process of resolving the database issues, TIGTA provided permission for the IRS to conduct a rescan of the databases. However, the IRS was unable to produce supporting documentation of this request. Additionally, while the IRS stated that it rescanned the system and addressed the 178 vulnerabilities found, officials were unable to provide TIGTA with the list of the vulnerabilities identified, neither could they support that all of the vulnerabilities were resolved. Our analysis found that some vulnerabilities were resolved; therefore, we have concluded that this PCA was partially implemented.

Weaknesses From Issued Audit Reports	Recommendations	PCAs	Specific Actions Taken	TIGTA's Assessment of Corrective Actions
Ref. No. 2014-20-087 PCA 2-5-1 Data Loss Prevention process and procedures can be enhanced.	To enhance the processes and procedures over the Data Loss Prevention solution, the CTO should incorporate a process to forward outbound unencrypted e-mail traffic with Personally Identifiable Information from licensed tax preparers/taxpayer representatives to the Office of Professional Responsibility through the business unit liaisons into the current policy and procedures.	The IRS partially agreed with this recommendation. The IRS agreed with the part of the recommendation addressing outbound e-mail. The Safeguarding Personally Identifiable Information Data Extracts team will enhance the processes and procedures to forward outbound unencrypted e-mail traffic with Personally Identifiable Information from licensed tax preparers/taxpayer representatives to the Office of Professional Responsibility through the business unit liaisons.	With the implementation of Safeguarding Personally Identifiable Information Data Extracts program into 24 x 7 production operations as of 8:00 a.m. Eastern Daylight Time on June 26, 2015, the recommended workflow process change the IRS agreed to has now been completed.	**Implementation: Not Implemented** TIGTA found that the IRS determined that neither the Office of Professional Responsibility nor the Return Preparer Office had authority or jurisdiction over unlicensed/unenrolled and enrolled return preparers that were careless regarding the handling of client tax return information. The IRS decided not to take any action, which resulted in not implementing the recommendation. In addition, the IRS did not follow its internal guidance that directs it back to TIGTA to submit a request for cancellation/rejection of the PCA with the appropriate justification.

Weaknesses From Issued Audit Reports	**Recommendations**	**PCAs**	**Specific Actions Taken**	**TIGTA's Assessment of Corrective Actions**
Ref. No. 2014-23-072 **PCA 1-1-1** Identified security weaknesses should be fully mitigated.	The CTO should ensure that processes and procedures are developed to provide direction on how to review and mitigate weaknesses **************2************* vulnerability detection scans run on all databases.	The IRS agreed with this recommendation. The Information Technology organization Cybersecurity organization has integrated **************2************* **************2************* **************2************* including creation of Plan of Action and Milestones. The Information Technology organization Cybersecurity organization, working with the Enterprise Operations organization, within the constraints of budget and resources, will revise the processes and procedures developed for the Security Assessment and Authorization process to provide direction on how to review and mitigate vulnerabilities ******2****** *****2***** during continuous monitoring.	The Federal Information Security Modernization Act Security Controls Assessment Standard Operating Procedures have been revised. *****2***** vulnerability scan results are assessed as part of cybersecurity assessments, and findings are documented in the appropriate assessment report. The Enterprise Plan of Action and Milestones Standard Operating Procedures detail the process of the Plan of Action and Milestones preparation by the system owner for assessment report findings.	**Implementation: Partial** We asked the IRS to provide us *****2***** scan results on its databases. It provided scan results on five databases that are information technology-owned information systems that, among other things, house and transmit taxpayer information such as the Automated Underreporter and the Filing Information Returns Electronically System. We determined the *****2***** vulnerability scans are not being run on all databases, the databases that are being scanned are not running the latest patches, multiple servers generated partial *****2***** scan results due to an incorrect scan inventory, and there are a number of critical vulnerabilities that have been identified but not mitigated. While the processes and procedures were developed, the procedures were to instruct on how to review and mitigate weaknesses, yet, we found that was not always occurring. Therefore, this PCA is partially implemented.

Weaknesses From Issued Audit Reports	Recommendations	PCAs	Specific Actions Taken	TIGTA's Assessment of Corrective Actions
*********2*********. *********2*********. *********2*********. *********2********* *********2********* *********2********* *********2********* *********2********* *********2********* *********2********* *********2*****	**************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2************* **************2*************.	****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2***************.	****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2*************** ****************2***************.	*************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************. *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************ *************2************.

Weaknesses From Issued Audit Reports	Recommendations	PCAs	Specific Actions Taken	TIGTA's Assessment of Corrective Actions
Ref. No. 2016-20-082 PCA 3-1-1 The IRS was not monitoring or analyzing systems audit logs for eAuthentication applications.	The CIO should implement enhancements to audit log analysis to provide for automated mechanisms to integrate audit review, analysis, and reporting processes, and to correlate audit records across different repositories to gain organization-wide situational awareness.	The IRS agreed with this recommendation. It completed the action reflected in the automated capability to: 1) collect and aggregate transaction logs in a secure data repository; 2) automate the creation of analytic datasets for in-depth analysis, correlation of transactions attempted to eAuthentication, and gain access to protected applications; 3) automate the indexing, filtering, and correlation of transactions used by 24 x 7 monitoring of eAuthentication; and 4) establish reporting and management processes for security-related events.	Closed per management's response to the draft report.	**Implementation: Partial** TIGTA issued an audit report that the IRS enhance its audit log analysis capabilities. However, it stated that additional work was needed to ensure that eAuthentication audit log reviews, analyses, and reporting processes provide useful information to support investigations and responses to suspicious activities. The Cybersecurity organization stated that it implemented a second enhancement in September 2017 after TIGTA completed its fieldwork for the issued report. The enhancement was to the eAuthentication audit plan because the current thresholds were not producing actionable events. The IRS provided additional evidence that included a monitoring road map for applications. They were not sufficient for use in the reporting process to gain situational awareness.

Appendix VI

List of 34 Planned Corrective Actions With Full Documentation That Needs Uploading to the Joint Audit Management Enterprise System

Count	Report Number	Finding Number	Recommendation Number	PCA Number
1	2012-20-019	1	1	1
2	2012-20-019	2	1	1
3	2012-20-019	2	2	1
4	2012-20-019	3	1	1
5	2012-20-019	3	2	1
6	2012-20-019	3	3	1
7	2012-20-099	1	1	1
8	2012-20-099	1	2	1
9	2012-20-099	1	3	1
10	2012-20-112	1	1	1
11	2012-20-112	2	1	1
12	2012-20-112	2	3	1
13	2012-20-112	2	4	1
14	2012-20-115	1	1	1
15	2012-20-115	1	3	1
16	2012-20-115	1	5	1
17	2012-20-115	2	1	1
18	2012-20-122	3	3	1
19	2013-20-016	1	1	1
20	2013-20-016	1	2	1

Count	Report Number	Finding Number	Recommendation Number	PCA Number
21	2013-20-016	1	3	1
22	2013-20-106	2	1	1
23	2013-20-107	1	2	1
24	2013-20-107	1	3	1
25	2013-20-107	1	4	1
26	2013-20-108	2	4	1
27	2013-20-127	2	1	1
28	2013-23-119	3	2	1
29	2014-20-087	2	6	1
30	2014-23-072	1	3	1
31	2015-20-008	1	3	1
32	2015-20-060	1	1	1
33	2015-20-073	1	1	1
34	2016-40-007	2	1	1

Source: TIGTA's assessment of the supporting documentation for the 51 closed PCAs for TIGTA reports from FYs 2012 through 2016.

Appendix VII

List of 10 Planned Corrective Actions With Partial Documentation That Needs Uploading to the Joint Audit Management Enterprise System

Count	Report Number	Finding Number	Recommendation Number	PCA Number
1	2011-20-111	1	1	1
2	2012-20-063	1	1	1
3	2012-20-063	2	1	1
4	2012-20-115	1	2	1
5	2012-20-122	3	2	1
6	2013-20-127	3	1	1
7	2014-20-083	2	1	1
8	2014-20-083	2	2	1
9	2014-23-072	1	1	1
10	*****2*****	**2**	**2**	**2**

Source: TIGTA's assessment of the supporting documentation for the 51 closed PCAs for TIGTA reports from FYs 2012 through 2016.

Appendix VIII

Glossary of Terms

Term	Definition
Automated Underreporter System	An inventory control system used in the Individual Master File Underreporter Program. An underreporter is a taxpayer case in which the income information associated with a tax return is less than what is reported by third parties, *e.g.*, banks, employers.
Electronic Authentication	The process of establishing confidence in user identities electronically prior to any transaction with an information system.
Department of the Treasury Federal Information Security Modernization Act Inventory Management System	The official Federal Information Security Modernization Act repository tool for all Department of the Treasury bureaus. It is housed and maintained by the Department of the Treasury and is only accessible via an Internet Explorer link and approved access. No IRS data feed directly into it. Data are uploaded via user input into this tool as part of the efforts to comply with the E-Government Act of 2002,[1] the National Institute of Standards and Technology, and Office of Management and Budget regulations and guidance.
Domain	Domains are groups of computers on a network within a forest that are administered as a unit with common rules and procedures.
Federal Information Security Modernization Act of 2014	The Federal Information Security Modernization Act of 2014[2] requires that Federal agencies have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices and to report the results to the Office of Management and Budget.
Filing Information Returns Electronically System	The primary purpose of the Filing Information Returns Electronically system is to enable the IRS to reconcile income tax documents, *e.g.*, income from dividends, interest, *etc.*, filed by taxpayers against those that were provided via forms such as Form 1099-DIV, *Dividends and Distributions*.
Forest	A forest is the outermost design element or boundary in an Active Directory implementation.

[1] Pub. L. No. 107-374.

[2] Pub. L. No. 113-283.

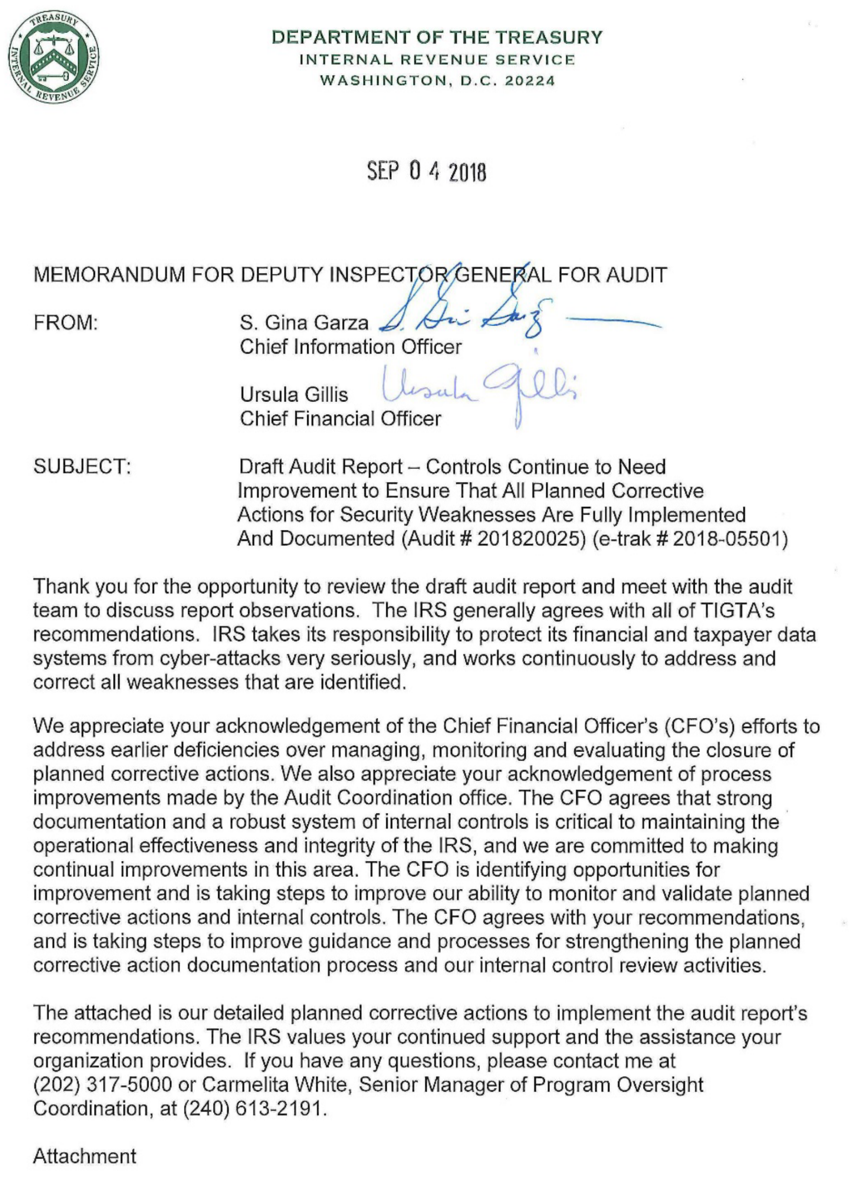
Term	**Definition**
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Master File	A computer record containing information about taxpayers' filing of returns and related documents for both individual tax returns (Individual Master File) and business tax returns (Business Master File). The Master File contains information on the current year plus all years that have had activity within the two previous years.
Office of Professional Responsibility	The Office of Professional Responsibility supports the IRS's strategy to enhance enforcement of the tax law by ensuring that tax practitioners adhere to professional standards and follow the law. The Office of Professional Responsibility is the governing body authorized to interpret and apply Treasury Department Circular No. 230[3] and is generally responsible for matters related to practitioner conduct and exclusive responsibility for discipline.
Personally Identifiable Information	Any information about an individual maintained by an agency, including any information 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.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished and details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The purpose of the Plan of Action and Milestones is to assist agencies to identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in programs and systems.
Practice Before the IRS	"Practice before the IRS" comprehends all matters connected with a presentation to the IRS, or any of its officers or employees, related to a taxpayer's rights, privileges, or liabilities under laws or regulations administered by the IRS.
Return Preparer Office	Provides oversight and support of tax professionals.

[3] 31 United States Code § 330.

Term	Definition
Security Assessment Report	The purpose of the report is to provide the cyber executive and the authorizing official with a more holistic view of risk regarding a system that is being reviewed. It summarizes the risks associated with the vulnerabilities identified during the security assessment activities that were performed on the system. It provides the stakeholders with an assessment of the adequacy of the security and privacy controls used to protect the confidentiality, integrity, and availability of the system and the data it stores, transmits, or processes.
System Security Plan	A plan developed and documented for each General Support System and major application consistent with guidance issued by the National Institute of Standards and Technology. It documents the current and planned controls for the information system and addresses security concerns that may affect the system's operating environment.
Treasury Department Circular No. 230	This statute and the body of regulations are the source of the Office of Professional Responsibility's authority. Circular 230 defines "practice" and who may practice before the IRS, describes a tax professional's duties and obligations while practicing before the IRS, authorizes specific sanctions for violations of the duties and obligations, and describes the procedures that apply to administrative proceedings for discipline.

Appendix IX

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

SEP 0 4 2018

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

Ursula Gillis
Chief Financial Officer

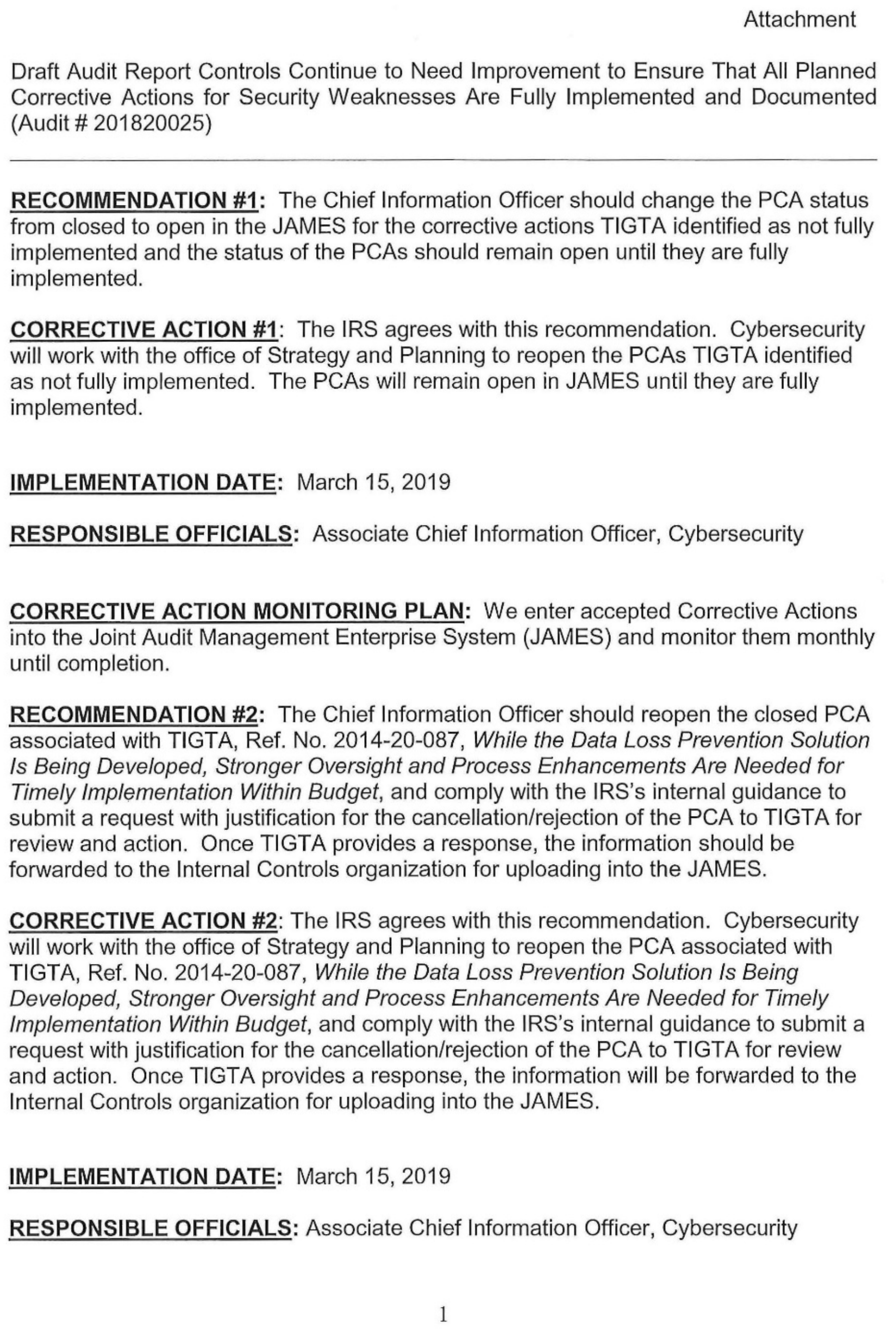
SUBJECT: Draft Audit Report – Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented And Documented (Audit # 201820025) (e-trak # 2018-05501)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss report observations. The IRS generally agrees with all of TIGTA's recommendations. IRS takes its responsibility to protect its financial and taxpayer data systems from cyber-attacks very seriously, and works continuously to address and correct all weaknesses that are identified.

We appreciate your acknowledgement of the Chief Financial Officer's (CFO's) efforts to address earlier deficiencies over managing, monitoring and evaluating the closure of planned corrective actions. We also appreciate your acknowledgement of process improvements made by the Audit Coordination office. The CFO agrees that strong documentation and a robust system of internal controls is critical to maintaining the operational effectiveness and integrity of the IRS, and we are committed to making continual improvements in this area. The CFO is identifying opportunities for improvement and is taking steps to improve our ability to monitor and validate planned corrective actions and internal controls. The CFO agrees with your recommendations, and is taking steps to improve guidance and processes for strengthening the planned corrective action documentation process and our internal control review activities.

The attached is our detailed planned corrective actions to implement the audit report's recommendations. 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 Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment



Attachment

Draft Audit Report Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented (Audit # 201820025)

RECOMMENDATION #1: The Chief Information Officer should change the PCA status from closed to open in the JAMES for the corrective actions TIGTA identified as not fully implemented and the status of the PCAs should remain open until they are fully implemented.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. Cybersecurity will work with the office of Strategy and Planning to reopen the PCAs TIGTA identified as not fully implemented. The PCAs will remain open in JAMES until they are fully implemented.

IMPLEMENTATION DATE: March 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

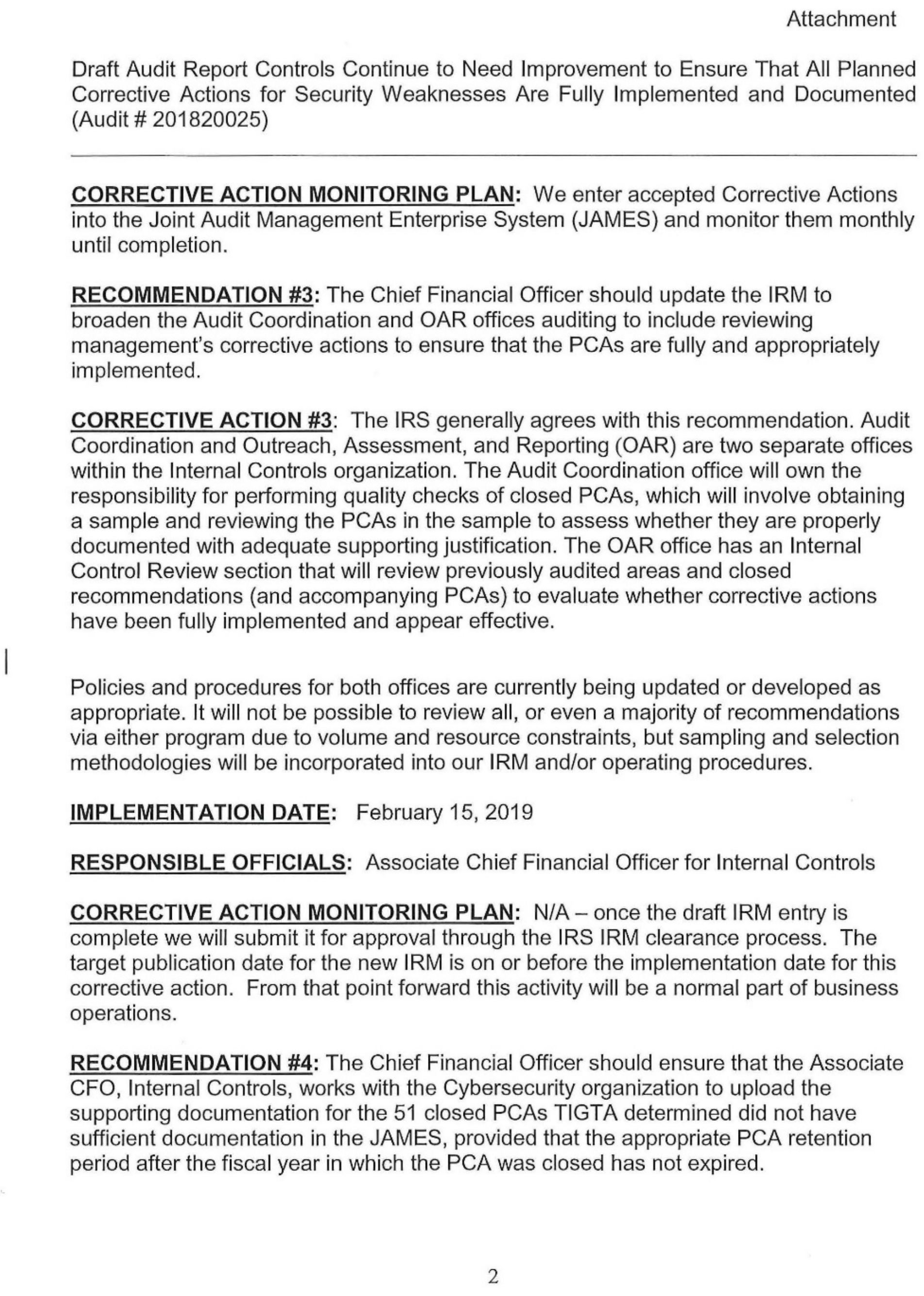
CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

RECOMMENDATION #2: The Chief Information Officer should reopen the closed PCA associated with TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget*, and comply with the IRS's internal guidance to submit a request with justification for the cancellation/rejection of the PCA to TIGTA for review and action. Once TIGTA provides a response, the information should be forwarded to the Internal Controls organization for uploading into the JAMES.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. Cybersecurity will work with the office of Strategy and Planning to reopen the PCA associated with TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget*, and comply with the IRS's internal guidance to submit a request with justification for the cancellation/rejection of the PCA to TIGTA for review and action. Once TIGTA provides a response, the information will be forwarded to the Internal Controls organization for uploading into the JAMES.

IMPLEMENTATION DATE: March 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity



Attachment

Draft Audit Report Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented (Audit # 201820025)

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

RECOMMENDATION #3: The Chief Financial Officer should update the IRM to broaden the Audit Coordination and OAR offices auditing to include reviewing management's corrective actions to ensure that the PCAs are fully and appropriately implemented.

CORRECTIVE ACTION #3: The IRS generally agrees with this recommendation. Audit Coordination and Outreach, Assessment, and Reporting (OAR) are two separate offices within the Internal Controls organization. The Audit Coordination office will own the responsibility for performing quality checks of closed PCAs, which will involve obtaining a sample and reviewing the PCAs in the sample to assess whether they are properly documented with adequate supporting justification. The OAR office has an Internal Control Review section that will review previously audited areas and closed recommendations (and accompanying PCAs) to evaluate whether corrective actions have been fully implemented and appear effective.

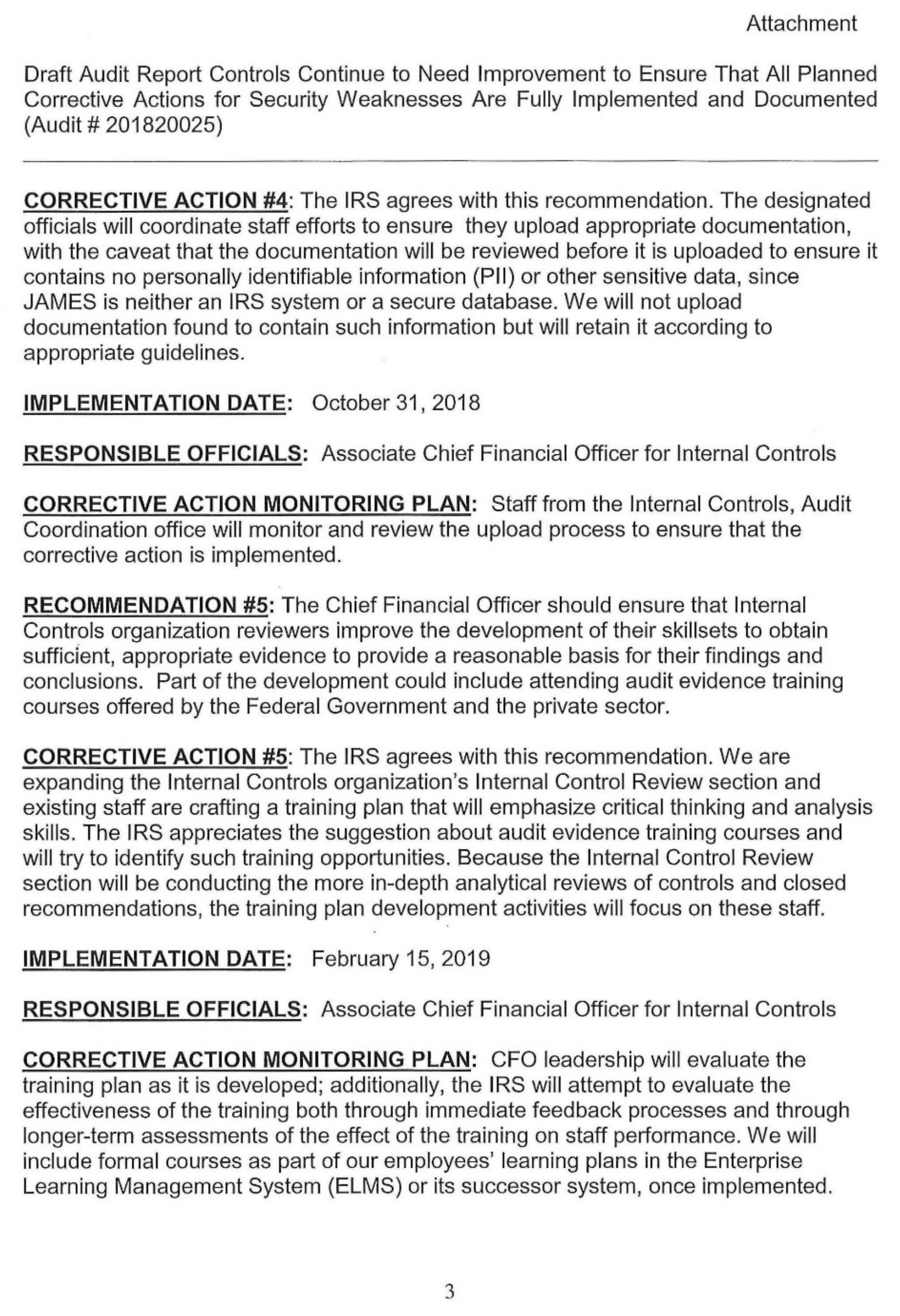
Policies and procedures for both offices are currently being updated or developed as appropriate. It will not be possible to review all, or even a majority of recommendations via either program due to volume and resource constraints, but sampling and selection methodologies will be incorporated into our IRM and/or operating procedures.

IMPLEMENTATION DATE: February 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Financial Officer for Internal Controls

CORRECTIVE ACTION MONITORING PLAN: N/A – once the draft IRM entry is complete we will submit it for approval through the IRS IRM clearance process. The target publication date for the new IRM is on or before the implementation date for this corrective action. From that point forward this activity will be a normal part of business operations.

RECOMMENDATION #4: The Chief Financial Officer should ensure that the Associate CFO, Internal Controls, works with the Cybersecurity organization to upload the supporting documentation for the 51 closed PCAs TIGTA determined did not have sufficient documentation in the JAMES, provided that the appropriate PCA retention period after the fiscal year in which the PCA was closed has not expired.



Attachment

Draft Audit Report Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented (Audit # 201820025)

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. The designated officials will coordinate staff efforts to ensure they upload appropriate documentation, with the caveat that the documentation will be reviewed before it is uploaded to ensure it contains no personally identifiable information (PII) or other sensitive data, since JAMES is neither an IRS system or a secure database. We will not upload documentation found to contain such information but will retain it according to appropriate guidelines.

IMPLEMENTATION DATE: October 31, 2018

RESPONSIBLE OFFICIALS: Associate Chief Financial Officer for Internal Controls

CORRECTIVE ACTION MONITORING PLAN: Staff from the Internal Controls, Audit Coordination office will monitor and review the upload process to ensure that the corrective action is implemented.

RECOMMENDATION #5: The Chief Financial Officer should ensure that Internal Controls organization reviewers improve the development of their skillsets to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions. Part of the development could include attending audit evidence training courses offered by the Federal Government and the private sector.

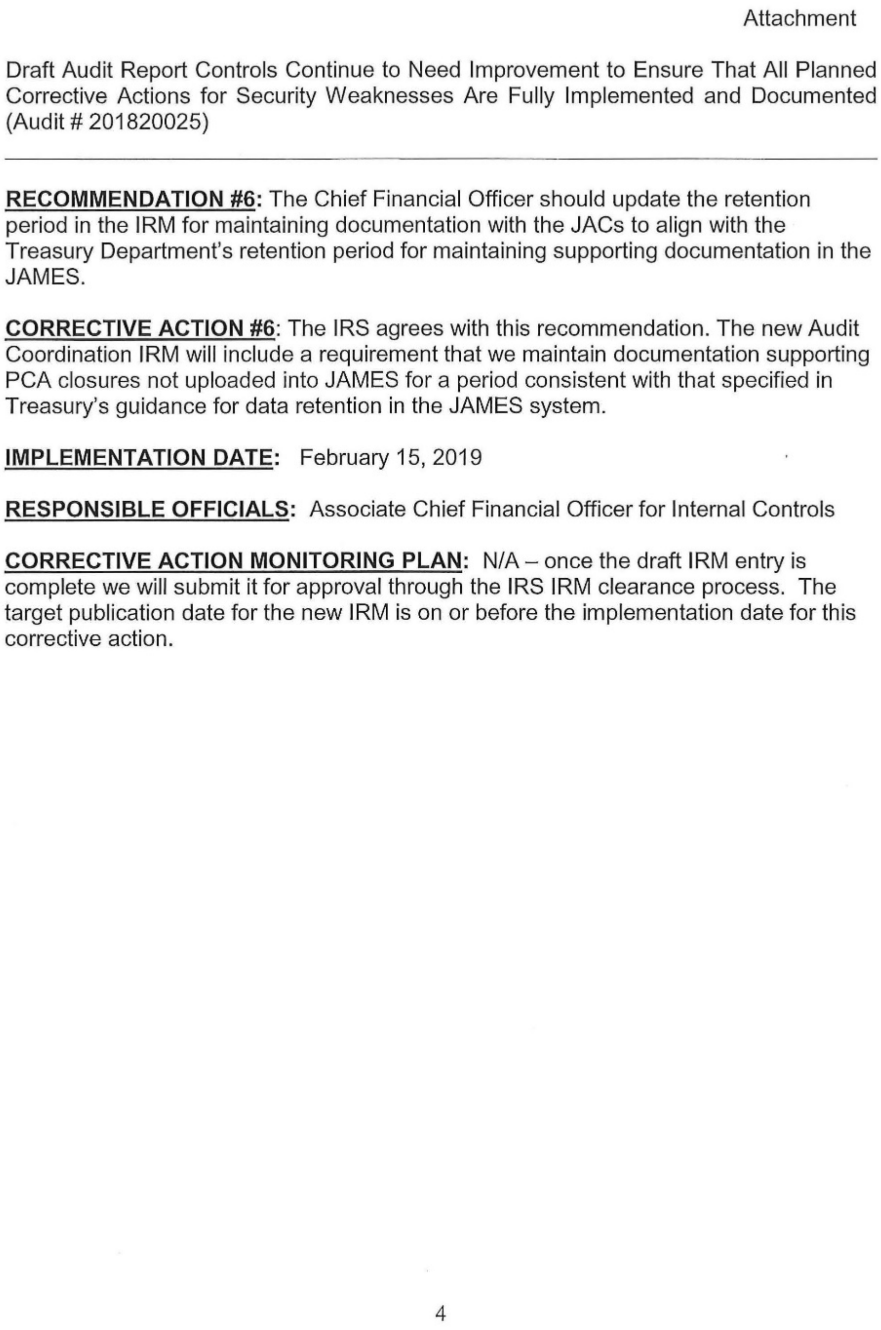
CORRECTIVE ACTION #5: The IRS agrees with this recommendation. We are expanding the Internal Controls organization's Internal Control Review section and existing staff are crafting a training plan that will emphasize critical thinking and analysis skills. The IRS appreciates the suggestion about audit evidence training courses and will try to identify such training opportunities. Because the Internal Control Review section will be conducting the more in-depth analytical reviews of controls and closed recommendations, the training plan development activities will focus on these staff.

IMPLEMENTATION DATE: February 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Financial Officer for Internal Controls

CORRECTIVE ACTION MONITORING PLAN: CFO leadership will evaluate the training plan as it is developed; additionally, the IRS will attempt to evaluate the effectiveness of the training both through immediate feedback processes and through longer-term assessments of the effect of the training on staff performance. We will include formal courses as part of our employees' learning plans in the Enterprise Learning Management System (ELMS) or its successor system, once implemented.

3



Attachment

Draft Audit Report Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented (Audit # 201820025)

RECOMMENDATION #6: The Chief Financial Officer should update the retention period in the IRM for maintaining documentation with the JACs to align with the Treasury Department's retention period for maintaining supporting documentation in the JAMES.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. The new Audit Coordination IRM will include a requirement that we maintain documentation supporting PCA closures not uploaded into JAMES for a period consistent with that specified in Treasury's guidance for data retention in the JAMES system.

IMPLEMENTATION DATE: February 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Financial Officer for Internal Controls

CORRECTIVE ACTION MONITORING PLAN: N/A – once the draft IRM entry is complete we will submit it for approval through the IRS IRM clearance process. The target publication date for the new IRM is on or before the implementation date for this corrective action.