Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data

September 27, 2013

Reference Number: 2013-20-117

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

IMPROVED CONTROLS ARE NEEDED TO ENSURE THAT ALL PLANNED CORRECTIVE ACTIONS FOR SECURITY WEAKNESSES ARE FULLY IMPLEMENTED TO PROTECT TAXPAYER DATA

Highlights

Final Report issued on September 27, 2013

Highlights of Reference Number: 2013-20-117 to the Internal Revenue Service Chief Financial Officer and Chief Technology Officer.

IMPACT ON TAXPAYERS

Management controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are achieved. When weaknesses are identified within an organization, management controls dictate that these weaknesses need to be tracked, monitored, and reported to ensure that they are corrected. Our audit identified weakened management controls in the IRS over its closed planned corrective actions (PCA) for the security of systems involving taxpayer data. When the right degree of security diligence is not applied to systems, disgruntled insiders or malicious outsiders can exploit security weaknesses and may gain unauthorized access.

WHY TIGTA DID THE AUDIT

This audit was part of our statutory requirement to annually review the adequacy and security of IRS technology, and it addresses the IRS major management challenge of Security of Taxpayer Data and Employees. The overall objective was to determine whether closed corrective actions to security weaknesses and findings reported by TIGTA have been fully implemented, validated, and documented as implemented.

WHAT TIGTA FOUND

The Chief Financial Officer's Office of Internal Control administers the IRS's management control program and is responsible for entering, monitoring, and tracking audit report findings, recommendations, and PCAs in the Department of the Treasury's Joint Audit Management Enterprise System (JAMES). The Office of Internal Control took a major step to strengthen the IRS's management control program by recently publishing new guidance on monitoring internal controls for the PCAs. However, guidance that was in effect since May 2004 was not sufficient.

During our audit, TIGTA determined that eight (42 percent) of 19 PCAs that were approved and closed as fully implemented to address reported security weaknesses from prior TIGTA audits were only partially implemented. These PCAs involved systems with taxpayer data. In addition, documents did not support the closure of the PCAs, and supporting documents were not always uploaded to the JAMES and were not readily available. The Office of Internal Control also has a responsibility to audit IRS PCAs to ensure that they are implemented; however, it did not conduct the audits.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS further strengthen its management controls to adhere to internal control requirements, provide refresher training to employees involved in the JAMES process, audit the corrective actions for closed PCAs, and change the status of closed PCAs to open for those that were partially implemented. In their response, IRS management agreed with five of our six recommendations and plans to issue guidance on internal control requirements, provide training, and revise the procedures to improve the IRS's management controls over the PCAs.

IRS management partially agreed with the sixth recommendation to upload documentation into the JAMES for previously closed PCAs, pending the completion of a cost/benefit analysis and risk-based approach. TIGTA believes the IRS should complete our recommendation as stated, which will ensure that all PCAs over security weaknesses are implemented as reported. In addition, the IRS will be in compliance with the Department of the Treasury's mandate to upload supporting documentation to the JAMES.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 27, 2013

MEMORANDUM FOR CHIEF FINANCIAL OFFICER AND CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data (Audit #201320028)

This report presents the results of our review to determine whether closed corrective actions to security weaknesses and findings reported by the Treasury Inspector General for Tax Administration in prior audits have been fully implemented, validated, and documented as implemented. We conducted this audit as part of our statutory requirement to annually review the adequacy and security of Internal Revenue Service technology. This review addresses the major management challenge of Security for Taxpayer Data and Employees.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

CDW	Compliance Data Warehouse
CFO	Chief Financial Officer
CTO	Chief Technology Officer
GAO	Government Accountability Office
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISR	Infrastructure Security and Reviews
JAC	JAMES Audit Coordinators
JAMES	Joint Audit Management Enterprise System
OIC	Office of Internal Control
PCA	Planned Corrective Actions
POA&M	Plan of Action and Milestones
RAS	Research, Analysis, and Statistics
TIGTA	Treasury Inspector General for Tax Administration

Background

Internal controls, which are synonymous with management controls, are a major part of managing an organization. They comprise the plans, methods, and procedures used to meet missions, goals, and objectives; and in doing so, they support performance-based management. They also serve as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. They help government program managers achieve desired results through effective stewardship of public resources. Systems of internal control provide reasonable assurance that the following objectives are being achieved: 1) effectiveness and efficiency of operations, 2) reliability of financial reporting, and 3) compliance with applicable laws and regulations.

The Department of the Treasury implemented the Joint Audit Management Enterprise System (JAMES) for use by all bureaus to track, monitor, and report the status of internal control audit results. The JAMES tracks specific information on issues, findings, recommendations, and planned corrective actions (PCA) from audit reports issued by the Government Accountability Office (GAO), the Treasury Inspector General for Tax Administration (TIGTA), and the Treasury Office of Inspector General. The Department of the Treasury uses this information to assess the effectiveness and progress of bureaus in correcting their internal control deficiencies and implementing audit recommendations. The JAMES also allows bureau users to run reports to assess the effectiveness of their programs. Tracking issues, findings, recommendations, and the current status of the PCAs is mandatory to comply with the intent of the standard of internal control, the Federal Managers' Financial Integrity Act of 1982,[1] Office of Management and Budget Circulars, and Treasury Directives.

At the Internal Revenue Service (IRS), the Chief Financial Officer's (CFO) Corporate Planning and Internal Control Unit, specifically the Office of Internal Control (OIC), administers the management control program. The OIC's primary responsibilities include entering, monitoring, and tracking audit report findings, recommendations, and PCAs in the JAMES and reviewing and validating all status updates entered into the JAMES by the JAMES Audit Coordinators (JAC). The JACs, who are selected from IRS functions, are responsible for assisting management with the internal control program and serving as their function's primary liaison with the OIC.

[1] 31 U.S.C. §§ 1105, 1113, and 3512.

The JACs also assist management with meeting their reporting requirements under the Federal Managers' Financial Integrity Act, the Federal Financial Management Improvement Act of 1996,[2] and other audit reporting requirements. The JACs ensure that the most current status of action plans are posted in the JAMES and that PCAs are timely implemented. The JAC's primary responsibilities include preparing and submitting verification of the completion of the PCAs to the OIC; maintaining complete audit files to include documentation of corrective actions taken, executive certification of status updates, and concurrence memoranda; monitoring and updating the status of the PCAs; and uploading and entering all implemented status updates and supporting documentation in the JAMES.

Although the IRS has implemented this reporting and tracking process to evaluate and track corrective actions and address previously reported weaknesses, the GAO reported in March 2012[3] and in March 2013[4] that the IRS did not promptly correct known security vulnerabilities and that its process was not always working as intended.

This review was performed at the offices of the CFO and the Chief Technology Officer (CTO) in Washington, D.C., New Carrollton, Maryland, and Memphis, Tennessee, during the period February through July 2013. 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.

[2] Pub. L. No. 104-208, 110 Stat. 3009.
[3] GAO, GAO-12-393, *IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data* p.23 (March 16, 2012).
[4] GAO, GAO-13-350, *IRS Has Improved Controls but needs to Resolve Weaknesses* p.19 (March 15, 2013).

Results of Review

On April 26, 2013, the OIC took a major step to strengthen the IRS's management control program by publishing the new Internal Revenue Manual (IRM), 1.4.30, *Monitoring Internal Control Planned Corrective Actions*, to strengthen existing policies and procedures on internal controls. The OIC previously issued guidance, *Reporting Procedures for Management Controls Coordinators*, on May 25, 2004. However, this guidance was not sufficient to result in a process that was effective in supporting the management control program.

Weakened Management Controls Contributed to Information Security Planned Corrective Actions That Were Not Fully Implemented

To assess the effectiveness of the IRS's internal control program, we selected for review a judgmental sample[5] of 19 PCAs for security weaknesses reported by TIGTA that had been closed as completed.[6] Our analysis showed that eight (42 percent) PCAs had not been fully implemented and should not have been closed. All eight PCAs involve systems containing taxpayer data. Examples of corrective actions that were not fully implemented include servers not being scanned for critical and major vulnerabilities, such as default and blank passwords; databases without the latest software updates; and user accounts with long periods of inactivity that were not locked. The causes for these conditions include the IRS changing the scanning tool for its systems, which required additional time for organizational approval and the need to ensure that useable information was generated by those tools; systems development constraints; and the need for the IRS to minimize the impact of system changes to its users. As a result, the IRS is increasing its exposure to risk for malicious users exploiting accounts with default or blank passwords to steal taxpayer identities and carry out fraud schemes. The IRS is also increasing its susceptibility to performance and security weaknesses inherent in older software versions, its exposure of taxpayer data to unauthorized disclosure, and its exposure to disruptions of system operations. Appendix IV provides the details of our assessment of the eight closed PCAs that were partially implemented.

The IRS has specific guidance over its internal control program. The OIC prior guidance requires that proper documentation is maintained to verify implementation of a corrective action. The recently issued IRM 1.4.30 requires all supporting documentation to be uploaded and stored in the JAMES, along with a completed, signed, and dated Form 13872, *Planned Corrective*

[5] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.
[6] We conducted site visits and performed system accesses of IRS computer systems located in Memphis, Tennessee, and the Washington, D.C., and New Carrollton, Maryland, areas.

Action Status Update for TIGTA/GAO/MW/SD/TAS/REM Reports,[7] or other executive certification. The prior guidance and IRM necessitate that the OIC reject the status of a corrective action if signatures are not received, missing, or invalid. Prior to the newly issued manual, a draft version of these requirements was forwarded to IRS business functions as early as July 2012. This IRM, along with the OIC's prior guidance, further require the JACs to maintain complete audit files to include documentation of corrective actions taken, certification of status updates via executive's e-mail or electronic signature, and concurrence memoranda. Also, three of the IRS's larger business divisions[8] have their own respective IRMs, which some smaller IRS business functions use for guidance. These IRMs require the same process and level of documentation and maintenance.

Additionally, the GAO *Standards for Internal Control in the Federal Government*[9] provide 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 standards also provide that key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing them, and handling any related assets. No one individual should control all key aspects of a transaction or event. The separation of duties requirement is also addressed in IRM 10.8.1, *Information Technology Security Policy and Guidance*, which specifically provides that an employee may simultaneously hold more than one role; however, while performing the duties of one role, that role shall not be used to perform the duties of another. Each role is to be independent of the other.

For the eight PCAs that were not fully implemented and should not have been closed, we found the following internal control deficiencies.

- In three PCAs, we were not provided any documentation to support the closure of the corrective action. For the remaining five PCAs, the supporting documentation did not fully support the closed corrective action.
- In four PCAs, the Form 13872 or equivalent did not include the appropriate executive approval. In two, we identified a separation of duties weakness. The JAC, whose primary responsibility includes preparing and submitting verification of the completion of the PCAs, signed as the executive approving the closure.

[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.
[8] The three larger divisions are the Large Business and International, Wage and Investment, and Small Business/ Self-Employed Business Divisions.
[9] Government Accountability Office (formerly known as the General Accounting Office), GAO/AIMD-00-21.3.1, *Internal Control: Standards for Internal Control in the Federal Government* (Nov. 1999).

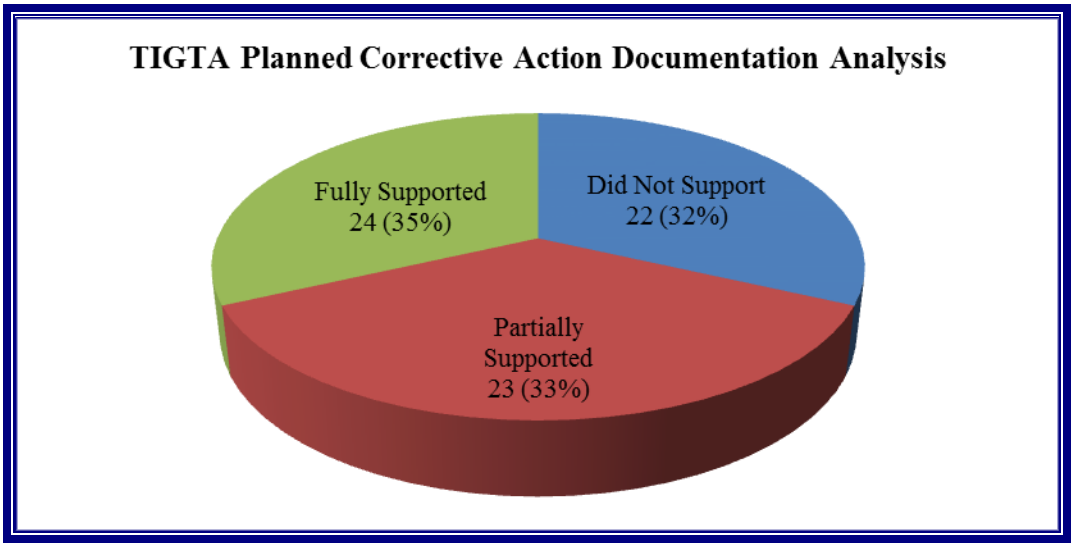
- In all eight PCAs, the OIC did not audit the corrective actions to ensure their implementation and proper closure.

Because the exception sample size of eight PCAs was relatively small, we conducted an assessment of these internal control deficiencies on a larger sample from the entire population of PCAs for security weaknesses reported by TIGTA to provide a better perspective. As such, we conducted further tests of a population of 147 PCAs for security weaknesses reported by TIGTA that were closed from October 2008 through December 2012. In addition, we selected a judgmental sample of 69 PCAs to determine whether the IRS was compliant with the previously mentioned procedures and standards.

Documentation did not fully support the closure of the PCAs

Through the JAMES, we analyzed documents that were available on the system and, when necessary, requested additional supporting documentation from the JACs and business functions to determine if closures of the 69 PCAs were supported. Our assessment is presented in Figure 1, followed by additional details about the results of our analysis.

Figure 1: Assessment of Supporting Documentation for the 69 Sampled PCAs



Source: TIGTA analysis of the 69 sampled PCAs.

- 22 (32 percent) did not support the closure of the PCAs. Some of the reasons the PCAs were not supported included supporting documentation was not maintained in the JAMES or with the office responsible for implementing the PCAs; supporting documentation was maintained on only one computer that crashed and no other copies exist; supporting documentation, according to the IRS, was not needed because the PCA was closed during the course of the audit and the weakness did not need to be tracked in

the JAMES; and the supporting documentation was only the Form 13872. Typically, the Form 13872 provides the same information from the IRS's management response to TIGTA's draft reports, but written in past tense with specific actions taken.

- 23 (33 percent) partially supported the closure of the PCAs. For these, the supporting documentation for all steps or actions as stated in the PCAs was requested, but it was not provided.
- 24 (35 percent) fully supported the closure of the PCAs.

Supporting documentation was not uploaded to the JAMES

On November 1, 2010, the Department of the Treasury mandated that its bureaus upload supporting documentation to the JAMES. Prior to that date, Treasury bureaus, including the IRS, were not required to upload any supporting documentation when the PCAs were closed. While supporting documentation was required to be uploaded to the JAMES, the OIC only enforced uploading the Form 13872. For the 69 judgmental sampled PCAs, 11 were closed after the mandate. The IRS did not upload any additional documentation supporting the implementation of the corrective action for nine of 11 PCAs.

One of the nine PCAs related to a corrective action that was superceded; however, there was no documentation in the JAMES that readily provided a reference to the new PCA. Generally, the PCAs are superceded when the same or similar recommendations are made for previously identified and reported weaknesses. We presented our concern with the superceded PCAs to OIC management. They acknowledged there is no reference to the new PCA but also cautioned that the number of superceded PCAs is minimal. Therefore, they agreed to implement a process that will include inputting reference information into the PCA record and uploading source documents to the JAMES. As a result of their actions, TIGTA will not make a recommendation for superceded PCAs.

Despite established requirements, we identified several factors contributing to why supporting documentation was not uploaded to the JAMES.

- There is no one definitive source for guidance. While the OIC has guidance, last issued on May 25, 2004, they are not widely known or used by the business functions. The OIC did not establish a Service-wide IRM over the JAMES internal control process until April 2013. While some IRS business functions have referenced existing IRM guidance from other business divisions on the internal control process, others have established their own standard operating procedures over the management control procedures that differ slightly.
- The OIC did not consistently enforce existing requirements for supporting documentation to be maintained by the JACs and for it to be uploaded to the JAMES. For example, the OIC required that only Form 13872 be uploaded to the JAMES despite established

requirements from the business functions and the OIC's draft IRMs for all supporting documentation. Prior to the publication of the new IRM, OIC personnel stated that they could not enforce the supporting documentation requirement on the business functions until their IRM was issued.

- The Department of the Treasury mandates supporting documentation be uploaded to the JAMES but does not define supporting documentation because each bureau is unique and it wanted to offer them the flexibility to make that decision.
- The OIC does not always validate whether each PCA was implemented. OIC personnel will validate updates to the IRM and the language on the Form 13872 to ensure that the corrective action addresses the weakness and finding.

Supporting documentation did not include appropriate executive approval

From our population of 147 security-related PCAs where a Form 13872 or equivalent was available, we found that 30 (50 percent) of 60 PCAs were signed by an executive not responsible for correcting the weaknesses. The executives signing as the approving official were CTO Program Oversight managers over the JACs with no delegated responsibility for signing. One manager stated that his or her signature only attested to the language in the corrective action narrative on the Form 13872 that addressed the PCA and not a validation of the actions taken. In a further analysis of the 30 PCAs, we determined that the Form 13872 in 15 (50 percent) contained a typed name that was not associated with the originating e-mail from the executive. A typed name approval is acceptable if the form is associated with the originating e-mail from the executive, but the e-mails were never retained. In addition, 11 (37 percent) of the 30 PCAs appeared to have a conflict with separation of duties. The CTO JAC who signed the Form 13872 also signed as the approving official.

To account for executive review and approval, the Cybersecurity office created an equivalent template to the Form 13872. As stated earlier, a typed name is acceptable if associated with the originating e-mail from the executive. Early this year, the CTO office, recognizing this deficiency, created a new signature line for executives responsible for the corrective actions to sign on the Form 13872. This process was unnecessary because the requirement already exists on the form in the "approving official" box. Also, the OIC does not validate the signatures on the form despite it being a requirement in its recently issued IRM, and its prior guidance to reject the status of a corrective action if the executive certification is missing, invalid, or not received. The OIC stated that it reviews the forms for a signature and that validation of the signature is the responsibility of the JACs.

The conditions existed in the CTO office because responsibilities changed when duties were reassigned or transferred from one employee to another or due to organizational changes. For example, prior to the organizational transfer of responsibilities from the Cybersecurity office to the Program Oversight office, executives responsible for implementing the corrective actions

were required to sign the Form 13872 before sending it to the OIC. After the transfer of responsibility, the Program Oversight manager signed the form, approving that the corrective actions supported the PCA, before it was uploaded to the JAMES. We were concerned with this process because the manager was attesting to the language in the corrective action narrative that addressed the PCA rather than a validation of the actions taken.

Closed corrective actions were not audited to ensure their implementation

As part of its roles and responsibilities, the OIC, which administers the IRS's management control program, has the responsibility for auditing corrective actions. The OIC did not audit corrective actions as required. During our discussions, the OIC cited concerns with implementing this responsibility due to lack of expertise.

Our analysis identified the PCAs that were prematurely closed, which illustrates the importance of the audits to ensure proper implementation. For example, in one report,[10] TIGTA recommended that database security control weaknesses identified during the review be remediated. The PCA stated that the weaknesses will be placed into a Plan of Action and Milestones (POA&M), while giving priority to correcting or mitigating high-risk weaknesses. As the PCA implies, not all weaknesses identified during the audit were remediated, but the PCA was closed as implemented. In a TIGTA follow-up review on database security controls, [11] we could not determine if all weaknesses were tracked, addressed, or closed for this PCA. As such, we made the same recommendation that all identified vulnerabilities be remediated.

Without an effective management control process, the CFO cannot be assured that the management control program is operating as intended. When this happens, the IRS cannot assure its stakeholders, which include the Department of the Treasury, that the PCAs were implemented as reported in correcting security vulnerabilities. The IRS is subject to reviews of the JAMES information by the Department of the Treasury and may not be able to support the corrective actions taken or that they were fully implemented. When reviews occur, the IRS would provide a weakened assurance that corrective actions in the JAMES have been completed and that an executive responsible for implementing the corrective action is attesting to the actions taken as stated on the Form 13872.

Moreover, without a central repository, supporting documentation could be unavailable and lost, and much time and resources could be spent locating documentation to support the PCAs, as was experienced during our audit. Our request to obtain supporting documentation took months before the IRS fully exhausted its resources to provide some of the documentation. In addition, from a security perspective, the lack of fully effective compensating and mitigating controls

[10] TIGTA, Ref. No. 2007-20-129, *Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation* p. 7 (Aug. 2007).
[11] TIGTA, Ref. No. 2011-20-044, *Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected* p. 4 (May 2011).

impair the IRS's ability to ensure that its financial and taxpayer information is secure from internal and external threats. This reduces the IRS's assurance that its financial statement and information are fairly presented or reliable and that sensitive IRS and taxpayer information is sufficiently safeguarded from unauthorized disclosure, modification, and external intrusions.

Recommendations

We recommended that the Chief Financial Officer should:

Recommendation 1: Issue a memorandum to all business functions emphasizing the new IRM to ensure that all adhere to the requirements governing the internal control process for the JAMES. These requirements include: 1) uploading all documents supporting the status of, corrective actions taken on, and closure of the corrective action to the JAMES for both past, beginning November 1, 2010, and present PCAs; at a minimum, supporting documentation should be uploaded for corrective actions to security weaknesses and 2) certification by the executive responsible for the corrective action on its status updates and completion.

> ***Management's Response:*** IRS management partially agreed with this recommendation. The CFO will issue a memorandum to all business units emphasizing adherence to the OIC IRM to ensure that requirements governing the internal control process for the JAMES, with respect to maintaining supporting documents for current closures and executive certification, are met. The CFO will work with the business units to assess the level of effort and cost/benefit to be derived from uploading documentation into the JAMES for previously closed corrective actions. The OIC will issue guidance following a risk-based approach for complying with the retroactive aspects of this recommendation, as appropriate.
>
> ***Office of Audit Comment:*** The IRS management's response addresses our recommendation as it pertains to new closures of corrective action, but may not necessarily address previously closed corrective actions. As previously noted, our audit found only 24 (35 percent) of 69 closed corrective actions were fully supported with adequate documentation. While we recognize the potential resource commitment needed to fully implement our recommendation, we believe the IRS should complete our recommendation as stated, which will ensure that all corrective actions over security weaknesses are implemented as reported. In addition, fully implementing our recommendation will ensure that the IRS is in compliance with the Department of the Treasury's mandate to upload supporting documentation to the JAMES.

Recommendation 2: Coordinate with business function executives to ensure that their existing guidance for the JAMES internal control process aligns with the new OIC IRM.

> ***Management's Response:*** IRS management agreed with this recommendation. The CFO will issue a memorandum to all business unit executives advising them that 1) their

existing guidance for the JAMES internal control process must be aligned with the new OIC IRM, as appropriate and 2) their revisions should be included in their next scheduled IRM update to comply with this corrective action.

Recommendation 3: Provide refresher training to all JACs and other IRS personnel who perform similar duties as the JAC over the JAMES internal control process and documentation requirements as a result of our findings and issuance of the new IRM.

Management's Response: IRS management agreed with this recommendation. The CFO will develop a program to provide refresher training to all JACs and other IRS personnel who perform similar duties as the JACs over the JAMES internal control process and documentation requirements.

Recommendation 4: Ensure that those who sign the Form 13872 as the JAC do not also sign as the approving official to comply with proper separation of duties standards.

Management's Response: IRS management agreed with this recommendation. The OIC is now verifying that those who sign the Form 13872 as the JAC do not also sign as the approving official. The CFO will also issue a memorandum to all business unit executives advising them that proper separation of duties standards must be adhered to in approving the closure of corrective actions.

Recommendation 5: Audit the IRS's completed corrective actions to findings and weaknesses that result from external audit agencies' issued reports beginning with those TIGTA identified as partially implemented once they are fully implemented. This action will 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. We recognize the potential resource commitment needed to audit these completed corrective actions and suggest that this action can be done periodically, at least annually, by conducting a statistical sample of the completed corrective actions. The results can be shared with the respective business functions.

Management's Response: IRS management agreed with this recommendation. The OIC will develop a program to formally audit completed corrective actions annually if adequate resources can be identified. Under this program, the OIC will evaluate the use of statistical sampling techniques and determine the appropriate number of completed corrective actions to be reviewed. These reviews will be conducted with the business units, and the results will be shared with them.

Office of Audit Comment: The IRS management's response outlined a plan to audit completed corrective actions; however, its implementation appears to be contingent upon identifying adequate resources. While we recognize the potential resource commitment needed to fully implement our recommendation, we encourage the IRS to complete our

recommendation as stated, which will provide better assurance that corrective actions in the JAMES have been completed.

We also recommended that the CTO, the Director, Office of Research, Analysis, and Statistics (RAS), and the Commissioner, Wage and Investment Division, should:

Recommendation 6: Coordinate with the OIC and the Department of the Treasury, Office of the Deputy CFO, Risk and Control Group, to change the PCA status from closed to open on the JAMES for the corrective actions TIGTA identified as partially implemented in Appendix IV. The status of these PCAs should remain open until they are fully implemented as agreed to in the prior TIGTA reports.

Management's Response: IRS management agreed with this recommendation. The CFO will work with the appropriate business units and the Department of the Treasury to reopen seven previously closed corrective actions to establish new corrective actions that fulfill the original audit recommendations. The new corrective actions will remain open until fully implemented. The CFO will work with TIGTA and the appropriate business unit on the one remaining closed corrective action to determine whether or not it has been fully implemented.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether closed corrective actions to security weaknesses and findings reported by the TIGTA in prior audits have been fully implemented, validated, and documented as implemented. To accomplish our objective, we:

I. Determined whether the IRS, specifically the offices of the CFO and the CTO, have an effective process and are complying with the requirements for closing completed 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 OIC and JAC personnel to document and assess the procedures and their responsibilities over the JAMES process and to determine the cause when discrepancies were identified.

   C. Researched the IRM and IRS guidance to determine whether other policies, procedures, and guidelines exist regarding the closure of findings and the PCAs tracked on IRS systems that could augment and improve the closing actions of findings and recommendations within the JAMES process.

II. Determined whether the PCAs were fully implemented, validated, and documented as implemented.

   A. Selected a judgmental sample[1] of 69 from 147 closed and implemented PCAs from the JAMES for the period October 2008 through December 2012. We used a judgmental sample because we were not projecting the review results.

   B. Determined whether the sample of closed security weaknesses, findings, and PCAs were fully closed. Specifically, we determined whether:

      1. Supporting documents, Form 13872, *Planned Corrective Action Status Update for TIGTA/GAO/MW/AD/TAS/REM Reports*, and other supporting documentation were uploaded in the JAMES.

      2. Form 13872 contained an executive signature related to the business unit responsible for the corrective action.

      3. Documentation supported implementation of the PCA and the closure of the weakness.

[1] A judgmental sample is a nonstatistical sample, the results of which cannot be projected to the population.

4. Physical testing of the system to ensure that the PCAs had been fully implemented. We selected a judgmental sample of 19 closed and implemented PCAs for validation. We used a judgmental sample because we were not projecting the review results and due to budget constraints from the Federal Government sequestration.

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 the following internal controls were relevant to our audit objective: the OIC's policies, procedures, and practices for the identification, tracking, and closing of the PCAs reported in the JAMES. We evaluated these controls by interviewing OIC management and employees and the JACs, reviewing documents supporting the closure of the PCAs, and physically validating the PCAs.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Deborah Smallwood, Audit Manager
Louis Lee, Lead Auditor
Cindy Harris, Senior Auditor
Michael Mohrman, Information Technology Specialist

Appendix III

Report Distribution List

Acting Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Office of the Deputy Commissioner for Services and Enforcement SE
Commissioner, Small Business/Self-Employed Division SE:S
Commissioner, Wage and Investment Division SE:W
Director, Office of Research, Analysis, and Statistics RAS
Director, Risk Management Division OS:CTO:SP:RM
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Chief Financial Officer OS:CFO
- Chief Technology Officer OS:CTO
- Commissioner, Small Business/Self-Employed Division SE:S
- Commissioner, Wage and Investment Division SE:W
- Director, Office of Research, Analysis, and Statistics RAS

Appendix IV

Assessment of Eight Planned Corrective Actions That Were Not Fully Implemented

Weaknesses From Issued Audit Reports	Recommendations	Planned Corrective Actions	TIGTA's Assessment: Corrective Actions Not Taken
Ref. No. 2008-20-029 **PCA 1-3-1**[1] Database Accounts With Default or Blank Passwords Continue to Be Found	The Chief Information Officer should expand the criteria used for scanning IRS databases for the presence of administrator accounts with default or blank passwords.	Cybersecurity's Computer Security Incident Response Center will implement and expand a quarterly database scanning component to its vulnerability management program. Application Security Inc.'s DBProtect[2] will be used.	**Implementation: Partial** The IRS is using the Guardium scanning tool, rather than DBProtect. Guardium scans are set for critical, major, and patch-level vulnerabilities, which include default and blank passwords. Currently, the IRS is scanning only Enterprise Operations servers; Windows SQL servers are not yet being scanned. As was reported in the 2008-20-029 report, the IRS is still not scanning all IRS databases.
Ref. No. 2008-20-176 **PCA 1-2-1** The Office of RAS Needs to Implement Adequate Security Controls	The Director, Office of RAS, should require system administrators and their managers to: • Disable accounts that have not been accessed in more than 45 calendar days. • Remove accounts that have not been used in more than 90 calendar days.	The Office of RAS has disabled accounts that have not been accessed in more than 45 days on the Compliance Data Warehouse (CDW) system and will continue to follow this practice. It will also develop and implement a policy of removing accounts on the CDW that have not been used in more than 90 days.	**Implementation: Partial** The Office of RAS is not identifying accounts with inactivity on the CDW because it does not have an automatic script to identify the inactivity. It will need to reprogram the CDW so that locking a user's UNIX account, used to access the CDW, does not affect or prevent the user from accessing other applications residing on this platform. The Office of RAS will be working on this problem.

[1] The PCA reference number used throughout Appendix IV consists of three numbers which coincide with information 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 the management response to the audit report.
[2] DBProtect is a precision database security and compliance solution that helps organizations control their database security processes and streamlines key database security activities while enabling organizations to achieve database security, minimize risk, and achieve regulatory compliance.

Weaknesses From Issued Audit Reports	Recommendations	Planned Corrective Actions	TIGTA's Assessment: Corrective Actions Not Taken
Ref. No. 2008-20-176 **PCA 1-4-1** The Office of RAS Needs to Implement Adequate Security Controls	The Director, Office of RAS, should remind managers to periodically review Form 5081, *Information System User Registration/Change Request*, records to validate that access to systems is limited to only those who have a need. Managers should also be reminded to verify that potential users have received favorable background investigations before granting them access to systems.	The Office of RAS will use Online 5081 records to validate that system access is granted on a need-to-know basis. IRS users will not be granted access without first receiving favorable background clearances.	**Implementation: Partial** TIGTA reviewed the employees' Online 5081 of one manager and found that all were contractors. TIGTA verified that all but one contractor had a valid background investigation indicator on the Online 5081 system. TIGTA received verification of a background approval letter for the contractor, but the manager provided system access without knowledge that the background investigation had been approved. The approval letter was obtained from the Contracting Officer Representative, not from the manager approving access.
Ref. No. 2008-20-176 **PCA 1-5-1** The Office of RAS Needs to Implement Adequate Security Controls	The Director, Office of RAS, should ensure that audit and accountability controls are sufficient by requiring audit logs to be maintained a minimum of six years and to be periodically reviewed by the security officer.	The audit logs will now be retained for six years, and the security officer designated will perform these reviews.	**Implementation: Partial** On June 12, 2013, TIGTA requested follow-up documentation of audit log reviews for Office of RAS systems, the YK1 Link Analysis Tool, the Statistics of Income Distributed Processing System, and the CDW but has yet to receive them.
Ref. No. 2009-20-120 **PCA 1-2-1** Although Controls Have Improved, Additional Steps Could Be Taken to Expand the Reporting of Incidents and the Protection of Sensitive Data Description	The CTO should ensure that all backup data are properly protected from unauthorized access and disclosure. Specifically, IRS offices should 1) conduct annual inventory reconciliations of stored backup media at all off-site storage facilities in accordance with IRS policy and 2) validate lists of IRS employees authorized to access the backup data at off-site storage facilities when changes occur or at least annually.	The Modernization and Information Technology Services organization (currently the Information Technology organization) will ensure that backup media is properly protected from unauthorized access and disclosure by ensuring that media management controls and encryption are in place. In addition, it will follow policies and procedures for sending and maintaining backup data to designated off-site storage facilities, schedule and conduct regular off-site storage facility reconciliations as documented in IRM 2.7.5, and validate the authorized access list with the Contracting Officer Representative on an annual basis.	**Implementation: Partial** The IRS no longer has private vendor off-site storage facilities. Backup media is sent to the other campuses or computing centers. IRS personnel stated the annual inventory reconciliation is conducted between the facilities; however, the reconciliation is not documented unless a discrepancy is identified. Backup media controls and encryption are in place.

Weaknesses From Issued Audit Reports	Recommendations	Planned Corrective Actions	TIGTA's Assessment: Corrective Actions Not Taken
Ref. No. 2010-20-028 **PCA 1-6-1** Several Access Controls Have Been Implemented, but Additional Controls Are Needed for the Call Site Employees	The Commissioners, Wage and Investment and Small Business/ Self-Employed Divisions, should instruct all Automated Collection System managers to immediately review the Online 5081 system for all of their employees who need elevated Resource Access Control Facility privileges to ensure that the manager's approval is documented in the employees' Online 5081 profile.	The Wage and Investment and Small Business/Self-Employed Divisions will direct the sites to document managerial approval on all elevated Resource Access Control Facility privileges as reflected in the Online 5081 system. Additionally, both operating divisions have included this security issue in their Fiscal Year 2010 Operational Review Plans.	**Implementation: Partial** The IRS provided print screens of Online 5081. System administrators conducted quarterly reviews of elevated privileges, but they do not document the reviews or the results. The Fiscal Year 2010 Operational Reviews included security issues.
Ref. No. 2010-20-051 **PCA 2-1-1** The IRS Did Not Ensure That Computer Security Weaknesses Identified at Contractor Facilities Are Timely Corrected	The Associate Chief Information Officer, Cybersecurity, should validate correction of Infrastructure Security and Reviews (ISR) office's reported security weaknesses and recommend a process for reporting weaknesses that remain unmitigated to increase the accountability of the responsible parties for remediation of security weaknesses.	Cybersecurity's ISR office will establish a plan that delineates sending out a request for status updates on POA&Ms from the responsible business unit. As appropriate, the ISR office will validate the correction of findings in the POA&M during the POA&M continuous monitoring process or during follow-up security reviews. In addition, the ISR office will forward a copy of the uncorrected weaknesses to the appropriate business unit quarterly to ensure that the responsible parties are made aware of the need to remediate weaknesses.	**Implementation: Partial** The ISR office is no longer sending out a request for status updates nor has the ISR office received all the previously sent requests. In addition, copies of uncorrected weaknesses are not sent to the appropriate business unit quarterly to ensure that the responsible parties are made aware of the need to remediate weaknesses. Instead, the ISR office manages the weaknesses *annually* during the follow-up reviews on a manually tracked POA&M. The ISR office ceased quarterly distribution in 2012 due to a limited response from the Contracting Officer Representatives, planned migration to the Archer Tool,[3] and planned changes in the ISR office standard operations procedures. The ISR office plans to use the Archer Tool in the future for both storage and tracking once the data have been uploaded onto the system.

[3] The Archer Tool offers management solutions to facilitate continuous monitoring by collecting, organizing, and displaying all technical data scan results from information technology tools and analyzes the results with a single risk-scoring capability.

Weaknesses From Issued Audit Reports	Recommendations	Planned Corrective Actions	TIGTA's Assessment: Corrective Actions Not Taken
Ref. No. 2011-20-044 **PCA 2-2-1** Production Environment Databases Were Running Out-of-Date Database Software That No Longer Receives Security Patches and Other Vendor Support	The CTO should ensure that databases with out-of-support Database Management System software are upgraded to currently supported versions within a reasonable time period. For those systems where upgrading the database software or implementing security patches have been determined to be dangerous to the stability of the system, a migration plan should be developed and a properly approved deviation should be on file to justify departure from stated standards.	The Associate Chief Information Officer, Enterprise Services, will coordinate with affected stakeholders to develop a migration plan to upgrade the Database Management System software to currently supported versions. An inventory of all servers with databases on them and their associated versions will be created. The Enterprise Services organization will then outline steps to take to address versions older than n-1 and updates will be installed accordingly. The Enterprise Services organization will establish ongoing monitoring of servers and institutionalize a process to keep software current.	**Implementation: Partial** Not all Database Management System software is at the currently supported versions. In addition, scans did not identify all database versions due to systems development constraints.

Appendix V

Management's Response to the Draft Report

CHIEF FINANCIAL OFFICER

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

September 23, 2013

MEMORANDUM FOR MICHAEL E. MCKENNEY
ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Pamela J. LaRue
Chief Financial Officer

SUBJECT: Draft Audit Report – Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data (Audit # 201320028)

Thank you for the opportunity to review and respond to the draft report titled, "Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data" (Audit # 201320028).

We appreciate your acknowledgement that the Office of Internal Control (OIC) took a major step in Fiscal Year 2013 to enhance the IRS's management control program by publishing the new Internal Revenue Manual (IRM) 1.4.30, *Monitoring Internal Control Planned Corrective Actions*, which strengthens existing policies and procedures on internal controls.

We will continue to work with the IRS business units to ensure that the closures of corrective actions are properly documented. In addition, the OIC will develop a program to audit completed actions to provide assurance that audit agencies' recommendations have been fully addressed.

Our detailed comments to your recommendations are discussed in the attachment. If you have any questions, please contact me at (202) 622-6400, or a member of your staff may contact Peter Rose, Associate Chief Financial Officer, Corporate Planning and Internal Control, at (202) 803-9524.

Attachment

Attachment

RECOMMENDATION 1
The Chief Financial Officer should issue a memorandum to all business functions emphasizing the new IRM to ensure that all adhere to the requirements governing the internal control process for the JAMES. These requirements include: 1) uploading all documents supporting the status of, corrective actions taken on, and closure of the corrective action to the JAMES for both past, beginning November 1, 2010, and present PCAs; at a minimum, supporting documentation should be uploaded for corrective actions to security weaknesses, and 2) certification by the executive responsible for the corrective action on its status updates and completion.

CORRECTIVE ACTION
The IRS partially agrees with this recommendation. The Chief Financial Officer (CFO) will issue a memorandum to all business units emphasizing adherence to the Office of Internal Control (OIC) Internal Revenue Manual (IRM) to ensure that requirements governing the internal control process for JAMES, with respect to maintaining supporting documents for current closures and executive certification, are met. The CFO will work with the business units to assess the level of effort and cost/benefit to be derived from uploading documentation into JAMES for previously-closed corrective actions. The OIC will issue guidance following a risk-based approach for complying with the retroactive aspects of this recommendation, as appropriate.

IMPLEMENTATION DATE
March 31, 2014

RESPONSIBLE OFFICIAL
Chief Financial Officer

RECOMMENDATION 2
The Chief Financial Officer should coordinate with business function executives to ensure that their existing guidance for the JAMES internal control process aligns with the new Office of Internal Control IRM.

CORRECTIVE ACTION
The IRS agrees with this recommendation. The CFO will issue a memorandum to all business unit executives advising them that (1) their existing guidance for the JAMES internal control process must be aligned with the new OIC IRM issued April 26, 2013, as appropriate; and (2) their revisions should be included in their next scheduled IRM update to comply with this corrective action.

IMPLEMENTATION DATE
March 31, 2014

RESPONSIBLE OFFICIAL
Chief Financial Officer

RECOMMENDATION 3
The Chief Financial Officer should provide refresher training to all JACs and other IRS personnel who perform similar duties as the JAC over the JAMES internal control process and documentation requirements as a result of our findings and issuance of the new IRM.

CORRECTIVE ACTION
The IRS agrees with this recommendation. The CFO will develop a program to provide refresher training to all JAMES Audit Coordinators (JACs) and other IRS personnel who perform similar duties as JACs over the JAMES internal control process and documentation requirements.

IMPLEMENTATION DATE
September 30, 2014

RESPONSIBLE OFFICIAL
Chief Financial Officer

RECOMMENDATION 4
The Chief Financial Officer should ensure that those who sign the Form 13872 as the JAC do not also sign as the approving official to comply with proper separation of duties standards.

CORRECTIVE ACTION
The IRS agrees with this recommendation. The OIC is now verifying that those who sign the Form 13872 as the JAC do not also sign as the approving official. The CFO will also issue a memorandum to all business unit executives advising them that proper separation of duties standards must be adhered to in approving the closure of corrective actions.

IMPLEMENTATION DATE
March 31, 2014

RESPONSIBLE OFFICIAL
Chief Financial Officer

RECOMMENDATION 5
The Chief Financial Officer should audit the IRS's completed corrective actions to findings and weaknesses that result from external audit agencies' issued reports

beginning with those TIGTA identified as partially implemented once they are fully implemented. This action will 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. We recognize the potential resource commitment needed to audit these completed corrective actions and suggest that this action can be done periodically, at least annually, by conducting a statistical sample of the completed corrective actions. The results can be shared with the respective business functions.

CORRECTIVE ACTION
The IRS agrees with this recommendation. The OIC will develop a program to formally audit completed corrective actions annually if adequate resources can be identified. Under this program, the OIC will evaluate the use of statistical sampling techniques and determine the appropriate number of completed corrective actions to be reviewed. These reviews will be conducted with the business units and the results will be shared with them.

IMPLEMENTATION DATE
September 30, 2014

RESPONSIBLE OFFICIAL
Chief Financial Officer

RECOMMENDATION 6
The Chief Technology Officer, the Director of Research, Analysis and Statistics, and the Commissioner, Wage and Investment Division, should coordinate with the Office of Internal Control and the Department of the Treasury, Office of the Deputy Chief Financial Officer, Risk and Control Group, to change the PCA status from closed to open on the JAMES for the corrective actions TIGTA identified as partially implemented in Appendix IV. The status of these PCAs should remain open until they are fully implemented as agreed to in the prior TIGTA reports.

CORRECTIVE ACTION
The IRS agrees with this recommendation. The CFO will work with the appropriate business units and the Department of the Treasury to reopen seven previously closed corrective actions to establish new corrective actions that fulfill the original audit recommendations. The new corrective actions will remain open until fully implemented. The CFO will work with TIGTA and the appropriate business unit on the one remaining closed corrective action to determine whether or not it has been fully implemented.

IMPLEMENTATION DATE
March 31, 2014

RESPONSIBLE OFFICIALS
Chief Technology Officer; Director of Research, Analysis and Statistics; and Commissioner, Wage and Investment Division, as appropriate