Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks

August 2, 2016

Reference Number: 2016-20-035

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.

IMPROVEMENTS ARE NEEDED FOR INFORMATION TECHNOLOGY CONTRACT ADMINISTRATION CONTROLS TO MITIGATE RISKS

Highlights

Final Report issued on August 2, 2016

Highlights of Reference Number: 2016-20-035 to the Internal Revenue Service Chief Information Officer and Chief Procurement Officer.

IMPACT ON TAXPAYERS

The IRS relies on contracting support for its information technology products and services. It is important that the IRS adheres to Federal Acquisition Regulation requirements to mitigate risk for its information technology contracts. Effective contract administration processes include post-award activities performed by IRS officials after a contract has been awarded to determine how well both the IRS and the contractor meet the requirements of the contract.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to determine whether the IRS information technology contract administration processes incorporate appropriate means to mitigate risk in contracting activities and ensure adherence to applicable policies and procedures.

WHAT TIGTA FOUND

Risks for information technology contracts awarded between October 2008 and May 2014 were not adequately mitigated to protect the IRS's systems and sensitive data and to ensure that the IRS receives services and products that meet contractual requirements. TIGTA analyzed 14 information technology contract files and supporting documentation. The estimated value of these contracts is $81.3 million. The sample was selected from 6,045 information technology contracts with total obligations of $3.3 billion. The obligation amount of the contracts is based on the respective award date for each contract.

TIGTA assessed controls within 13 high-risk areas.

TIGTA identified two key areas in which overall improvements are needed to address the control weaknesses identified during our review. First, clarification is needed to ensure consistent and reliable implementation of reviews required to mitigate security risks through the information technology contract administration process. Second, the overall operational controls for contract administration and fraud controls for individual information technology contracts should be carefully reexamined to ensure that post-award contract file reviews are reliable. Overall, TIGTA found control weaknesses with: 1) Security Compliance Reviews, 2) contract file documentation, 3) Contractor Exclusion Reviews, 4) Contract Administration Plans, and 5) Contracting Officer's Representatives' Appointment Letters.

WHAT TIGTA RECOMMENDED

TIGTA made five recommendations. TIGTA recommended that the Chief Technology Officer ensure that IRS policy and procedures are updated to provide clear guidance and instructions for the Security Compliance Review Checklist certification process. In addition, the Chief Procurement Officer should ensure that: IRS policy and procedures are improved to ensure that the security checklists are sufficiently documented, maintained, and reviewed and that information technology contract files are maintained in a complete, organized, and consistent manner for review purposes.

In management's response to the report, the IRS agreed with three recommendations and partially agreed with two others. The IRS plans to implement corrective actions for all five recommendations. The IRS also expressed concern about the sample size of information technology contracts selected for review. TIGTA believes that our sample selection methodology and statistical projections and other audit evidence adequately support the audit results and recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 2, 2016

MEMORANDUM FOR CHIEF INFORMATION OFFICER
CHIEF PROCUREMENT OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks (Audit # 201520017)

This report presents the results of our review of how the Internal Revenue Service (IRS) managed controls over post-award information technology contract administration activities. The overall objective of this review was to determine whether the IRS's information technology contract administration processes incorporate appropriate means to mitigate risk in contracting activities and ensure compliance with Federal policies and guidelines. This audit is included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Achieving Program Efficiencies and Cost Savings.

Management's complete response to the draft report is included as Appendix VIII. We also included an Office of Audit comment to a general response about the sample size of information technology contracts 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 Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

CO	Contracting Officer
COR	Contracting Officer's Representative
EPLS	Excluded Parties List System
FAR	Federal Acquisition Regulation
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
SAM	Federal System for Award Management

Background

The Federal Acquisition Regulation (FAR) sets forth acquisition principles, policies, and procedures that govern acquisitions for Federal agencies. The FAR governs contracts, orders, and agreements entered into by the Internal Revenue Service (IRS).

The IRS's Office of Procurement, within the Deputy Commissioner for Operations Support organization, is responsible for purchasing equipment, services, and supplies for the IRS. The Office of Procurement is made up of six suborganizations, one of which is the Office of Information Technology Acquisition. This office is responsible for planning, negotiating, executing, and managing the procurement of information technology products and services. As such, this office provides technical and administrative support throughout all stages of the acquisition life cycle.

The Office of Information Technology Acquisition procurement process begins when an IRS program determines that a requirement for information technology products or services exists. This requirement is:

1. Defined by the requester in a Statement of Work.
2. Initiated by processing a requisition in the Integrated Procurement System.[1]
3. Authorized (funding identified and approved) through the requisition in the Integrated Procurement System.
4. Awarded to a contractor by a contracting officer (CO).
5. Technically managed by the contracting officer's representative (COR).

Our audit focused on post-award activities and controls for information technology contract administration within the IRS's procurement environment. Post-award contract management includes the activities that are managed by the COR and outlined in individual COR Appointment Letters. Our overall objective was to determine whether the IRS's information technology contract administration processes incorporate appropriate means to mitigate risk in contracting activities and to ensure compliance with Federal policies and guidelines.

[1] The Integrated Procurement System is the IRS's electronic procurement solution. The system creates and tracks all new requests for goods and services; captures and creates the information necessary to make awards (such as purchase orders, delivery orders, task orders, contract awards, and interagency agreements and associated modifications); and creates critical financial transactions (commitments, obligations, vendors, receiving) with the IRS's Integrated Financial System. The Integrated Procurement System also provides for printing of pertinent acquisition documents and standard reports required for internal and external management and operations.

Federal contract administration includes post-award activities performed by Government officials after a contract has been awarded to determine how well the Government and the contractor meet the requirements of the contract. This phase of the process encompasses all dealings between the Government and the contractor from the time the contract is awarded until the work has been completed and accepted or the contract has been terminated, payment has been made, and disputes have been resolved.

IRS Office of Procurement guidance stipulates that a CO is the only person who can enter into a contract and thereby financially obligate the Government. All IRS COs work within this office and must be certified. The COs are also responsible for the business management of IRS contracts, including making contractual determinations, effecting legal remedies, and issuing contract modifications. Prior to the contract award, only the CO can legally represent the Government.

After contracts are awarded, the CO is responsible for appointing a qualified COR for all contracts exceeding the $150,000 Simplified Acquisition Threshold.[2] This process includes issuing a signed letter of appointment (COR Appointment Letter). The COR Appointment Letter authorizes the COR to perform specific contract administration duties. The COR's primary responsibility is to assist the CO in the administration of the contract, and he or she plays a vital role in affecting the outcome of the contract administration process.

The CORs are employees within the IRS program office that initiate acquisitions, and, like the COs, they serve as a legal representative of the Government. The CORs have limited authorities that are stipulated in individual COR Appointment Letters. In general, the CORs are expected to provide technical direction, monitor contract performance, and maintain an "arm's-length" relationship with the contractor, ensuring that the Government pays only for the goods and services authorized and delivered under the contract. The CORs must also ensure that risks to the Government are mitigated, contractors fulfill contract terms and conditions, and taxpayer dollars are prudently spent.

The Federal Information Technology Acquisition Reform Act of 2014[3] was enacted on December 19, 2014. This legislation outlines specific requirements related to:

1. Agency Chief Information Officer Authority Enhancements.
2. Enhanced Transparency and Improved Risk Management in Information Technology Investments.
3. Portfolio Review.
4. Federal Data Center Consolidation Initiative.

[2] The Simplified Acquisition Threshold is $150,000, except for acquisitions of supplies or services that, as determined by the head of the agency, are to be used to support a contingency operation or to facilitate defense against or recovery from nuclear, biological, chemical, or radiological attack.
[3] Title VIII, Subtitle D, of the National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 11 3-291.

5. Expansion of Training and Use of Information Technology Cadres.
6. Maximizing the Benefit of the Federal Strategic Sourcing Initiative.
7. Governmentwide Software Purchasing Program.

This review was performed at the Office of Information Technology Acquisition in Lanham and Oxon Hill, Maryland, during the period May 2015 through January 2016. 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. Appendix I provides detailed information on our audit objective, scope, and methodology. Appendix II lists the major contributors to this report.

Results of Review

A detailed review of a sample of the IRS's information technology contracts found that improved controls are needed to address high-risk areas. We performed a structured analysis of voluminous paper and electronic contract files. Our review identified control weaknesses with: 1) Security Compliance Reviews, 2) contract file documentation, 3) Contractor Exclusion Reviews, 4) Contract Administration Plans, and 5) COR Appointment Letters. Our sample was selected from 6,045 information technology contracts awarded between October 2008 and May 2014 with total obligations of $3.3 billion.[4] Results were derived from a stratified random sample of 14 information technology contracts[5] totaling $81.3 million and a comprehensive evaluation of select controls to address 13 high-risk areas.[6]

It is important that the IRS clarify information technology security risks and enforce appropriate controls with its contract review process to ensure compliance with all applicable policy and guidance for information technology contracts. Moreover, the sufficiency of overall operational controls for post-award contract administration along with fraud controls for individual information technology contracts should be carefully reexamined to ensure that post-award contract file reviews are complete and reliable for risk mitigation purposes. Based on conditions found with a sample of 14 contract files, our review concluded that the IRS should take prompt steps to address recommendations in both of these areas and to ensure that risks for more than 6,000 information technology contracts with estimated obligations of $3.3 billion, as well as for other contracts, are sufficiently mitigated. Improvements in two key areas are needed to address the overall control weaknesses in the area of information technology post-award contract administration. These risk areas should be addressed with the IRS's ongoing efforts to improve information technology acquisition management processes and controls, including key risk mitigation roles and responsibilities being considered under the provisions of the Federal Information Technology Acquisition Reform Act of 2014.[7]

Following our review, the IRS took important steps to reorganize and elevate responsibilities for the procurement function that were managed by the Chief, Agency-Wide Shared Services, during our audit. Effective December 27, 2015, the IRS realigned responsibilities for the Office of Procurement to the Office of the Chief Procurement Officer. Under this reorganization, the IRS Chief Procurement Officer reports directly to the Deputy Commissioner for Operations Support.

[4] The obligation amount of the contracts is based on the respective award date for each contract.
[5] Appendix IV provides details regarding our sample selection methodology and the information technology contracts selected. The Treasury Inspector General for Tax Administration's statistician verified that the results of our analysis of the 14 information technology contracts could be projected to the population.
[6] Appendix V provides details for the 13 high-risk areas that we analyzed.
[7] Title VIII, Subtitle D, of the National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 11 3-291.

To reflect this reorganization and additional information provided by the IRS on its revised procurement responsibilities, our draft report recommendations to the Chief, Agency-Wide Shared Services, are addressed to the new Chief Procurement Officer.

Security Checklists and Process Improvements Are Needed to Help Ensure Security Compliance Through Contract Reviews

The IRS recognizes that security is an increasingly important aspect of the acquisition process, and, within the Information Technology organization, the Office of Cybersecurity is responsible for ensuring that products or services being acquired are in alignment with prevailing internal and external security guidance and mandates and established internal systems, data and physical security policies, and technology standards. The IRS program offices that initiate information technology requisitions[8] are required to complete and approve a Security Compliance Review Checklist[9] for each requisition. According to current IRS policy, the checklist serves as a critical security control that helps provide the analysis required to determine whether a product is compliant, is considered an exception, or requires a waiver from applicable requirements. The purpose statement for the checklist states the following:

> *The purpose of the Security Compliance Review Checklist is to document compliance with Clinger-Cohen Act of 1996, also known as the Information Technology Management Reform Act (ITMRA), Government Information Security Reform Act (GISRA), Federal Information Security Management Act of 2002 (FISMA), OMB A-130, 123, and 127, Treasury Directive P 85-70 and IRM 10.8.1. These primary policy statements are augmented by other OMB, FAR, NIST, Treasury and/or IRS guidance and/or mandates, established internal systems, data and physical security policies and technology standards. These more recent, detailed mandates may have necessary technical guidance applicable to current acquisitions.*[10]

The IRS required contracts awarded on or after October 1, 2009, to have a Security Compliance Review Checklist.[11] Ten of the 14 contracts in our sample met this criterion. Unlike the other post-award documentation we reviewed, the IRS does not presently require that the Security Compliance Review Checklist be included in contract files. We requested that the IRS provide copies of the Security Compliance Review Checklist for each of the 10 contracts selected in our sample to determine whether this critical security control was completed, signed by the program

[8] An information technology acquisition is defined as an information technology product (*e.g.*, hardware and/or software, including telecommunications, or maintenance) or service (*e.g.*, contractor resources).
[9] Appendix VI depicts the Security Compliance Review Checklist template.
[10] OMB = Office of Management and Budget. NIST = National Institute of Standards and Technology.
[11] Of the 6,045 information technology contracts from which we selected our sample, 5,043 were awarded as of October 1, 2009.

office, and also signed by the Office of Cybersecurity as required. The IRS was only able to provide eight of the 10 checklists for review.

During our review, an Office of Cybersecurity representative explained that a Security Compliance Review Checklist must be completed by the initiating program office for all information technology acquisitions. Current guidance requires that checklists for individual information technology contracts be provided to the Office of Cybersecurity for its review and certification based on the program office's responses to specific questions. Our sample review found that the Office of Cybersecurity was not provided and had not reviewed security checklists for any of the 10 information technology contract files analyzed.

Further, our review found a need for additional guidance for the security checklist to ensure that both product and service risks are adequately considered and contract administration policy and procedures are enforced. Our review of the Security Compliance Review Checklists identified the following concerns:

1. Contractor service risks are not considered.
2. Justifications are not required to support the answers provided.
3. Additional technical reviews and signatures are not required.
4. Approval signatures are not used consistently.

Following our discussions about the sufficiency of the checklist as a risk mitigation process, the IRS stated that the security checklist along with guidance for its implementation are inadequate and are being reviewed and updated.

For the contract files we analyzed, we observed that neither Internal Revenue Manual (IRM) 2.21.1[12] nor instructions for the Security Compliance Review Checklist provide clear direction or adequate guidance to consistently ensure that the requesting program office adequately responds to the questions used to determine whether further reviews from the Office of Cybersecurity are needed.

Half of our sample contract files included information technology contractor services, which are not considered with the current checklist. We noted that two of these information technology service contract files were to support the Customer Account Data Engine 2 initiative.[13] For the checklists we reviewed, we found that the responses provided with the checklist did not ensure consistent or sufficient verification to support the IRS's decision to not provide the checklists to the Office of Cybersecurity for review and certification of contract security controls.

[12] The IRM is the IRS's primary official source of instructions to staff relating to the administration and operations of the IRS. It contains the directions employees need to carry out their operational responsibilities.
[13] An IRS application that will replace the existing Individual Master File and Customer Account Data Engine applications. The Customer Account Data Engine 2 strategy, as designed, will allow the IRS to modernize the processes it uses to account for the records of individual taxpayers and create a single overall system of records.

Therefore, it was unclear whether the checklists and associated guidance for the 10 post-award contract files we reviewed effectively served as a critical control point or adequately assisted the IRS in determining the adequacy of security for information technology products or services. Improvements are needed to help the IRS ensure that all products or services being acquired are in alignment with prevailing security guidance and mandates and established internal control systems, security policies, and technology standards. We discussed these concerns with the IRS, and it agreed that IRM 2.21.1 and the security checklist process need improvement and that the current security checklist template does not provide the detailed instructions and analysis required to determine whether a product or service is complaint, is considered an exception, or requires a waiver.

Due to deficiencies identified with the current security review checklist process, the security checklists for the 5,043 contracts awarded since October 1, 2009, have not provided sufficient information to adequately document risk mitigation controls as needed. Because of these conditions, we did not apply the pass/fail ratings for individual checklists reviewed with our sample for this high-risk area. Overall, we found that the checklist was not an effective control for addressing the risks, which is the stated purpose for the checklist. Figure 1 provides a list of the 10 contracts in our sample that were awarded after October 1, 2009.

Figure 1: Sampled Contracts Awarded After October 1, 2009

Risk No.	Information Technology Contracts
9	• Sample Group 1.A, Contract 1 (TIRNO11D00052, 0001) • Sample Group 1.B, Contract 2 (TIRNO11K00522) • Sample Group 2, Contract 1 (TIRNO11K00234) • Sample Group 2, Contract 2 (TIRNO10S00002, 0010) • Sample Group 2, Contract 3 (TIRNO06D00041, 0156) • Sample Group 2, Contract 4 (TIRNO11D00007, 0004) • Sample Group 2, Contract 5 (TIRNO12K00583) • Sample Group 3, Contract 1 (TIRNO99D00001, 0158) • Sample Group 3, Contract 2 (TIRNO11D00027, 0009) • Sample Group 3, Contract 5 (TIRNO12K00355)

Source: Treasury Inspector General for Tax Administration analysis of contract files provided by the IRS.

Because this important contract administration and risk-mitigation control is not considered adequate for its stated purpose, the IRS may not adequately 1) mitigate the risk that the

information technology contracts do not provide sufficient assurance that products and services for its systems are in compliance with security policies and standards and 2) ensure that IRS systems and operations reliant on these contracts adequately protect the IRS's systems and sensitive data.

Office of Cybersecurity officials stated that they have begun efforts to update the checklist and strengthen guidance for this important control. They stated that the specific control weaknesses we identified are being considered with these efforts. They also noted that improvements will include additional information technology acquisition controls required under the Federal Information Technology Acquisition Reform Act of 2014 and the Federal Information Security Modernization Act of 2014.[14]

Recommendations

Recommendation 1: The Chief Technology Officer should ensure that IRM 2.21.1 is updated to provide clear guidance for effectively completing the Security Compliance Review Checklists.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that the Security Compliance Review Checklist is currently undergoing a major revision that will result in an update to IRM 2.21.1. The Office of Cybersecurity will coordinate with the subject matter experts within the Information Technology organization to deliver updates to IRM 2.21.1 that provide clear guidance for effectively completing the Security Compliance Review Checklists.

Recommendation 2: The Chief Technology Officer should ensure that the Security Compliance Review Checklist template is updated to provide clear instructions for effectively completing the Security Compliance Review Checklists.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that the Security Compliance Review Checklist currently in use was partially updated in March 2016 to provide clear guidance and is undergoing a major revision that is scheduled to be completed by October 2016. The Office of Cybersecurity procedures will be updated with clear instructions to ensure that subject matter experts within the Information Technology organization and the Office of the Chief Procurement Officer effectively use the updated Security Compliance Review Checklist.

Recommendation 3: The Chief Procurement Officer should ensure that IRS Policy and Procedures Memorandum Number 4.1 (*File Content Checklists*) is updated to ensure that Security Compliance Review Checklists are maintained as needed for review.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS stated that IRS Policy and Procedures Memorandum Number 4.1 (*File Content*

[14] Pub. L. No. 113-283, 128 Stat. 3073.

Checklists) will be updated to include elements of the Information Technology Requisition Checklist, which includes the Security Compliance Review Checklist.

Operational and Fraud Controls Were Not Consistently Followed

Within the IRS's contract administration environment, Contract File Content Reviews are required[15] in order to ensure that procurement documents are complete, organized, current, consistent, and maintained in contract files. Our review of specific contract documents found that some Contract File Content Reviews had not been conducted.

As a result, critical processes including operational and fraud controls may not be in place and operating as intended for information technology contracts. Areas of concern include: 1) Contractor Exclusion Reviews were not always conducted, 2) nonappointed IRS employees performed some contract administration duties, 3) contract administration plans were not always developed, and 4) contract files were sometimes incomplete. As such, the IRS may be unable to effectively evaluate services or products that contractors are required to provide. These incomplete contract administration processes could also result in the IRS paying for services or products that do not meet all the requirements.

Controls were not consistently followed to ensure that the COs and the CORs completed key contract administration responsibilities[16]

Contractor Exclusion Reviews were not always conducted

FAR Subpart 9.4 (*Debarment, Suspension, and Ineligibility*) requires that contractors debarred, suspended, or proposed for debarment are excluded from receiving contracts and that agencies shall not solicit offers from, award contracts to, or consent to subcontracts with these contractors unless the agency head determines that there is a compelling reason for such action. A contractor can be excluded from receiving contracts for several reasons, some of which include: 1) delinquent Federal taxes that exceed $3,000; 2) conviction of or civil judgment for the commission of fraud; 3) commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property; and 4) violation of the terms of a Government contract or subcontract so serious as to justify debarment, such as willful failure to perform in accordance with the terms of one or more contracts or a history of failure to perform or unsatisfactory performance of one or more contracts.

After receipt of contract proposals and prior to contract award, the COs are required to check the Federal System for Award Management (SAM)[17] to determine whether the contractor is listed as

[15] Contract File Content Reviews are required pursuant to IRS Policy and Procedures Memorandum Number 4.1(b), *Procurement Reviews* (August 14, 2013).
[16] See Appendix VII for statistical projections for information technology contract sample analysis results.

being excluded from receiving an award. The SAM is the primary Federal Government repository that contains a list of the contractors who are excluded from receiving Federal awards. The contractor exclusions system that predated the SAM was the Excluded Parties List System (EPLS). EPLS reports were used to identify contractors who were excluded from receiving Federal awards.

Our review of contract file documentation determined that Contractor Exclusion Reviews were not conducted and documented as required for three (21 percent) of 14 contracts in our sample. We discussed the results of our analysis with the IRS, and it agreed that the EPLS reports were not saved in the contract files. Without these reports, the IRS has not consistently determined whether the COs verified contractor eligibility as needed. Figure 2 provides detailed results for our analysis of Contractor Exclusion Reviews.

Figure 2: Detailed Results for Our Analysis of Contractor Exclusion Reviews

Risk No.	Total	Failure Details
13	11 of 14 Passed	The IRS could not provide an EPLS report to verify that a Contractor Exclusion Review was conducted. • Sample Group 1.B, Contract 2 (TIRNO11K00522) • Sample Group 2, Contract 2 (TIRNO10S00002, 0010) • Sample Group 3, Contract 3 (TIRNO06D00026, 0043)

Source: Treasury Inspector General for Tax Administration analysis of contract files provided by the IRS.

Nonappointed IRS employees performed some contract administration duties

Separation of duties is a key component of internal control to help reduce the risk of fraud or errors. It entails separating key duties and responsibilities and assigning them to more than one individual. IRS management is responsible for considering the potential for fraud when identifying, analyzing, and responding to risks.

Further, IRS Policy and Procedures Memorandum Number 1.6(c) (*Appointment of CORs and Alternate CORs*) requires that the COs appoint a qualified COR for all contracts that exceed the $150,000 Simplified Acquisition Threshold by issuing a signed COR Appointment Letter. The COR Appointment Letter must be tailored to meet the needs of each contract action assigned. The COR Appointment Letter authorizes the COR to perform specific contract administration duties, such as maintaining an organized contract administration file to record all contractor and

[17] The SAM is the primary Government repository for prospective Federal awardee and Federal awardee information and the centralized Government system for certain contracts, grants, and other assistance-related processes. It includes: 1) data collected from prospective Federal awardees required to conduct business with the Government and 2) prospective contractor-submitted annual representations and certifications.

Government actions, monitoring the contractor's performance, and certifying and documenting receipt and acceptance of goods and services. The COR is responsible for accepting the terms and conditions of the COR Appointment Letter by signing and submitting the signed letter to the CO and keeping a copy of the signed letter in the contract file.

The COR Appointment Letter is an important control to help ensure the separation of duties between the CO and the COR for post-award contract administration activities. For example, the CO is the only person who has the authority to sign and award a contract on behalf of the Federal Government. However, the CO should not also perform receipt and acceptance of goods and services for that contract. The COR Appointment Letter assigns these types of responsibilities to the COR, which helps to ensure a separation of duties between the CO and the COR.

We reviewed contract file documentation for the 14 contracts in our sample to determine whether the COR Appointment Letters were issued and signed as required. For three of the 14 contracts, the CORs were not assigned because these contracts fell under the Simplified Acquisition Threshold amount of $150,000; therefore, there were no COR Appointment Letters in the contract files to review.

Our review of the remaining 11 contract files determined that three (27 percent) of the 11 COR Appointment Letters were not fully completed as required. For example, the IRS was unable to produce one of the 11 COR Appointment Letters; therefore, the IRS could not verify whether it was completed. In addition, the IRS provided incomplete copies of the COR Appointment Letters for two of the 11 contracts. These two COR Appointment Letters were not signed by the respective CORs, and the IRS was not aware of this issue at the time of our review. In response to our review, the IRS provided documentation to confirm that, while the COR Appointment Letters were not in place, the CORs had certifications for these 11 contracts. However, we believe that the COR Appointment Letters should be maintained in the contract files to clearly document the separation of duties between the CO and the COR. We discussed the results of our analysis with the Office of Information Technology Acquisitions, and it agreed that the COR Appointment Letters should have been issued and signed to help mitigate this risk. Figure 3 provides detailed results for our analysis of COR Appointment Letters.

Figure 3: Detailed Results for Our Analysis of COR Appointment Letters

Risk No.	Total	Failure Details
12	8 of 11 Passed	The COR Appointment Letter was included in the contract file, but was not signed by the COR. • Sample Group 2, Contract 1 (TIRNO11K00234) • Sample Group 2, Contract 3 (TIRNO06D00041, 0156) The IRS was unable to locate and provide the COR Appointment Letter for the IRS employee who performed the contract administration duties of the COR. • Sample Group 2, Contract 2 (TIRNO10S00002, 0010)

Source: Treasury Inspector General for Tax Administration analysis of contract files provided by the IRS.

Contract Administration Plans were not always in place to guide key contract responsibilities

The IRS Office of Procurement requires that the COs develop written Contract Administration Plans for each contract. The Contract Administration Plan outlines the critical processes for successfully administering the contract, including processes for inspection and acceptance, invoice reviews, and contract deliverables. IRS Policy and Procedures Memorandum Number 4.1 (*File Content Checklists*) requires the Contract Administration Plan be saved in the contract file.

We reviewed contract file documentation for the 14 contracts in our sample to determine whether the respective COs completed Contract Administration Plans. For three of 14 contracts, Contract Administration Plans were not required because the contracts fell under the Simplified Acquisition Threshold amount of $150,000.

Our review of the remaining 11 contract files identified that Contract Administration Plans were not developed as required for two (18 percent) of 11 contracts. We discussed the results of our analysis with the Office of Information Technology Acquisitions, and it agreed that Contract Administration Plans were required to be developed. The Office of Information Technology Acquisitions explained that the COs should ensure that Contract Administration Plans are developed and saved in their respective contract files as required. Figure 4 provides detailed results for our analysis of Contract Administration Plans.

Figure 4: Detailed Results for Our Analysis of Contract Administration Plans

Risk No.	Total	Failure Details
4	9 of 11 Passed	A Contract Administration Plan was not developed. • Sample Group 2, Contract 1 (TIRNO11K00234) • Sample Group 3, Contract 3 (TIRNO06D00026, 0043)

Source: Treasury Inspector General for Tax Administration analysis of contract files provided by the IRS.

Operational controls were generally not followed to ensure that contract files included all documentation as required in accordance with FAR and IRS guidance

FAR 4.8 (*Government Contract Files*) requires contract files to be established for each contract containing the records of all contractual actions. It also requires that documents in contract files be sufficient to constitute a complete history of the contract transactions as a basis for making informed decisions at each step in the acquisition process, supporting actions taken, and providing information for reviews and investigations.

In addition, IRS Policy and Procedures Memorandum Number 4.1 (*File Content Checklists*) establishes a uniform structure for file content of contractual documents. This memorandum also provides contract file content checklists, which describe the documents required to be saved in the contract file. The IRS stated that some of the items listed on the checklists are optional; therefore, those items are not required to be saved in the contract file. Our review noted that this memorandum and its checklists do not provide clear instructions to consistently identify which documents are optional versus which documents are required to be saved in the contract file.

We reviewed contract file documentation for the 14 contracts in our sample to determine whether the CO and the COR sufficiently maintained a complete contract file. We determined whether the following documents were saved in the contract files as required:

- COR Nomination Letter.
- COR Appointment Letter.
- COR Certification.
- Contract Administration Plan.
- EPLS Report.

Our review determined that 11 (79 percent) of the 14 contract files were not complete. We discussed the results of our analysis with the IRS, and it confirmed that these documents are, in fact, missing from the contract files. The IRS explained that some of the documents were not saved in its respective contract files due to simple oversight. We also concluded that a lack of

clear instructions provided in the IRS's policy and checklists for contract file content contributed to missing and incomplete contract file documentation. Figure 5 provides detailed results for our analysis of the contract files.

Figure 5: Detailed Results for Our Analysis of Contract File Completeness

Risk No.	Total	Documents Missing From the Contract Files
3	3 of 14 Passed	• Sample Group 1.A, Contract 1 (TIRNO11D00052, 0001) – The EPLS report. • Sample Group 1.B, Contract 2 (TIRNO11K00522) – The EPLS report. • Sample Group 2, Contract 1 (TIRNO11K00234) – The Contract Administration Plan and the COR Nomination Letter. • Sample Group 2, Contract 2 (TIRNO10S00002, 0010) – The COR Certification, COR Nomination Letter, COR Appointment Letter, and the EPLS report. • Sample Group 2, Contract 3 (TIRNO06D00041, 0156) – The Alternative COR Appointment Letter. • Sample Group 2, Contract 5 (TIRNO12K00583) – The COR Certification. • Sample Group 3, Contract 1 (TIRNO99D00001, 0158) – The COR Nomination Letter and the EPLS report. • Sample Group 3, Contract 2 (TIRNO11D00027, 0009) – The Contract Administration Plan, EPLS report, and the COR Appointment Letter. • Sample Group 3, Contract 3 (TIRNO06D00026, 0043) – The Contract Administration Plan, and the EPLS report. • Sample Group 3, Contract 4 (TIRNO09T00080) – The COR Appointment Letter. • Sample Group 3, Contract 5 (TIRNO12K00355) – The COR Appointment Letter and the EPLS report.

Source: Treasury Inspector General for Tax Administration analysis of contract files provided by the IRS.

Recommendations

Recommendation 4: The Chief Procurement Officer should ensure that all reviewers, including the COs, execute Contract File Content Reviews so that all procurement documents for information technology contracts are complete, organized, current, consistent, and saved in contract files as required by Federal and IRS guidance.

Management's Response: The IRS partially agreed with this recommendation. The IRS explained that IRS Policy and Procedures Memorandum Number 4.1 (*File Content Checklists*) requires use of the appropriate checklist based on the acquisition type. In addition, IRS Policy and Procedures Memorandum Number 4.1(b) (*Procurement*

Reviews) details the requirements for contract file reviews. The Office of Procurement Policy will emphasize the importance of conducting contract file reviews in the annual lessons learned training scheduled in May 2016. The Director, Procurement Policy, has developed a Knowledge Power Hour presentation on how to conduct Peer and Tier file reviews that will be presented on April 21, 2016. The Chief Procurement Officer will issue a memorandum to all managers and the COs reiterating the importance of file content and document retention. The IRS subsequently stated that it partially agreed with the recommendation because it already has a process in place regarding contract files and file reviews.

Office of Audit Comment: Pursuant to IRS Policy and Procedures Memorandum Number 4.1(b) (*Procurement Reviews*), Contract File Content Reviews are required to ensure that procurement documents are complete, organized, current, consistent, and maintained in contract files, and the COs are required to review all contract files for information technology acquisitions above $3,000. Our review of specific contract documents found that some Contract File Content Reviews had not been conducted. For example, our review determined that 11 (79 percent) of the 14 contract files were not complete. As a result, critical processes including operational and fraud controls may not be in place and operating as intended for information technology contracts. We maintain that the IRS needs to take additional steps to ensure that all reviewers, including the COs, execute Contract File Content Reviews as required.

Recommendation 5: The Chief Procurement Officer should ensure that IRS Policy and Procedures Memorandum Number 4.1 (*File Content Checklists*) is updated to clarify post-award contract administration information and/or data that are required to be maintained in contract files.

Management's Response: The IRS partially agreed with this recommendation. The IRS stated that IRS Policy and Procedures Memorandum Number 4.1 (*File Content Checklists*) adequately identifies post-award contract administration information and outlines documentation retention guidance. The Office of Procurement Policy will emphasize the importance of conducting contract file reviews in the annual lessons learned training scheduled in May 2016. The Director, Procurement Policy, has developed a Knowledge Power Hour presentation on how to conduct Peer and Tier file reviews that will be presented on April 21, 2016. The Chief Procurement Officer will issue a memorandum to all managers and the COs reiterating the importance of file content and document retention.

Office of Audit Comment: Based on our review of specific contract documents, we concluded that a lack of clear instructions provided in the IRS's policy and checklists for contract file content contributed to missing and incomplete contract file documentation. We maintain that Policy and Procedures Memorandum Number 4.1 (*File Content Checklists*) and its checklists do not provide clear instructions to consistently identify

which documents are optional versus which documents are required to be saved in the contract file and needs to be updated.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS's information technology contract administration processes incorporate appropriate means to mitigate risk in contracting activities and ensure compliance with Federal policies and guidelines. To accomplish this objective, we:

I. Identified and reviewed IRS operational controls for 13 high-risk areas within post-award information technology contract administration activities.

A. Obtained from the Integrated Procurement System a list of 6,045 information technology contracts awarded between October 2008 and May 2014. We assessed the reliability of the Integrated Procurement System data by examining contract data fields such as contract award number, award obligated amount, award date, and vendor name. We determined that the data were sufficiently reliable to use for our audit tests.

B. Selected a stratified random sample of 14 information technology contracts from the population of 6,045 information technology contracts. We selected a random sample to make sure that each contract had an equal chance of being selected. The design parameters were:

1. Worst case exception rate of 50 percent.
2. Confidence level of 90 percent.
3. Precision of ± 22 percent.

Using these design parameters, the required sample size was 14.

See Appendix IV for more details related to our sample selection methodology and the information technology contracts selected in our random sample.

C. Coordinated with the Treasury Inspector General for Tax Administration's statistician to determine whether our sample methodology was sound.

D. Analyzed audit documentation, *e.g.*, copies of the contract files. For our selected sample of information technology contracts, we determined whether the CORs sufficiently:

1. Maintained a complete contract file for each assigned contract.
2. Developed a Contract Administration Plan.

II. Determined whether the Security Compliance Review Checklist for information technology acquisitions was applied as required for the selected sample of information technology contracts.

III. Considered the following fraud risk areas for the selected sample of information technology contracts:

A. Separation of duties between the CO and the COR.

B. Vendor exclusions.

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 FAR, the IRM, and policies and procedures related to information technology contract management activities. We evaluated these controls by interviewing procurement personnel and reviewing a large volume of contract files and other related program documentation.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Gwen McGowan, Director
Suzanne Westcott, Audit Manager
David Allen, Lead Auditor
Charlene Elliston, Senior Auditor
Carlos J. Parada-Cardenas, Program Analyst

Appendix III

Report Distribution List

Commissioner
Office of Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Application Development
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise Services
Associate Chief Information Officer, Strategy and Planning
Director, Office of Audit Coordination

Appendix IV

Sample Selection Methodology for Information Technology Contracts

The sampling methodology was a stratified random sample using four strata. The design parameters were:

- Worst case exception rate of 50 percent.
- Confidence level of 90 percent.
- Precision of ± 22 percent.

Using these design parameters, the required sample size was 14.

A wide precision rate was used because of the significant resources needed for a manual, structured analysis of voluminous paper and electronic contract files.

We selected a random sample of 14 information technology contracts totaling $81,306,803. Our sample was selected from 6,045 information technology contracts with total obligations of $3,317,670,467. These contracts were awarded between October 2008 and May 2014. We chose a random sample to make sure that each contract had an equal chance of being selected. We stratified the population of 6,045 information technology contracts into the following three groups based on obligated dollar amount:

SAMPLE GROUP 1 ($0 – $999,999)

Number of Awards	5,493
Number of Awards Percent	90.87%
Obligated Dollars	$457,825,108
Obligated Dollars Percent	13.80%

SAMPLE GROUP 2 ($1,000,000 – $4,999,999)

Number of Awards	418
Number of Awards Percent	6.91%
Obligated Dollars	$928,919,315
Obligated Dollars Percent	28.00%

SAMPLE GROUP 3 ($5,000,000 and Greater)

Number of Awards	134
Number of Awards Percent	2.22%
Obligated Dollars	$1,930,926,044
Obligated Dollars Percent	58.20%

We selected a random sample of five information technology contracts from each group for an initial sample size of 15. However, the IRS destroyed the Group 1, Selection 5, contract file. The IRS explained that this contract file was destroyed because it was past its required retention period. Therefore, the IRS was unable to provide this contract file. As a result, we excluded this contract from our initial sample size of 15, for a revised sample size of 14. Our review subsequently verified that the file was destroyed after the required retention period.

In addition, four of the five contracts selected for Group 1 (Selection Numbers 1, 3, 4, 5) are less than $150,000 and are administered using the IRS's Simplified Acquisition Procedures. As a result, we stratified Group 1 into the following two subgroups (Groups 1.A and 1.B):

SAMPLE GROUP 1.A ($0 – $150,000)		**SAMPLE GROUP 1.B ($150,001 – $999,999)**	
Number of Awards	4,655	Number of Awards	838
Number of Awards Percent	77.01%	Number of Awards Percent	13.86%
Obligated Dollars	$116,224,270	Obligated Dollars	$341,600,838
Obligated Dollars Percent	3.5%	Obligated Dollars Percent	10.30%

The information technology contracts selected in our random sample include the following by stratified group:[1]

Sample Group	Selection Order	Award/Contract Number	Award/Contract Delivery Order Number	Award/Contract Obligated Amount
1.A	1	TIRNO11D00052	0001	$50,000
1.A	3	TIRSE09P00275	N/A	$1,019
1.A	4	TIRSE09K00023	N/A	$5,383
1.A	5	TIRNO09P00169	N/A	$16,241
Total				**$72,643**

Sample Group	Selection Order	Award/Contract Number	Award/Contract Delivery Order Number	Award/Contract Obligated Amount
1.B	2	TIRNO11K00522	N/A	$272,856
Total				**$272,856**

[1] We present the information for all 15 contracts even though we were only able to review 14 contracts.

Sample Group	Selection Order	Award/Contract Number	Award/Contract Delivery Order Number	Award/Contract Obligated Amount
2	1	TIRNO11K00234	N/A	$2,765,939
2	2	TIRNO10S00002	0010	$3,956,115
2	3	TIRNO06D00041	0156	$1,101,725
2	4	TIRNO11D00007	0004	$1,426,144
2	5	TIRNO12K00583	N/A	$1,961,688
Total				**$11,211,611**

Sample Group	Selection Order	Award/Contract Number	Award/Contract Delivery Order Number	Award/Contract Obligated Amount
3	1	TIRNO99D00001	0158	$16,388,507
3	2	TIRNO11D00027	0009	$31,246,627
3	3	TIRNO06D00026	0043	$5,638,156
3	4	TIRNO09T00080	N/A	$6,997,703
3	5	TIRNO12K00355	N/A	$9,494,941
Total				**$69,765,934**

Appendix V

The Thirteen High-Risk Areas Assessed for the Information Technology Contract Sample

Risk Number	13 High-Risk Areas Assessed for Information Technology Contract Sample
1	Was the CO's warrant level appropriate for each contract, as required?
2	Was the COR's certification level appropriate for each contract, as required?
3	Was a complete contract file maintained for each contract?
4	Was a Contract Administration Plan developed for each contract?
5	Did the CO hold a post-award conference meeting with the contractor for each contract, if required?
6	Does the contract file for each contract contain progress reports from the contractor to monitor contractor performance, if required?
7	Was Receipt and Acceptance adequately completed for each contract?
8	Was security language added to each contract, if applicable?
9	Were Security Compliance Review Checklists adequately completed for each contract?
10	Was privacy/system of records language added to each contract, if applicable?
11	Was a legal counsel review conducted for each contract modification, if applicable?
12	Was a COR Appointment Letter fully completed for each contract to help ensure separation of duties between the CO and the COR, if applicable?
13	Were Contractor Exclusion Reviews conducted for each contract?

Legend: The highlighted rows indicate risk areas for which failures were identified. Details are provided about these failures in the body of the report.

Source: Treasury Inspector General for Tax Administration analysis of high-risk areas for information technology contract administration.

Appendix VI

Security Compliance Review Checklist for Information Technology Acquisitions Template

SECURITY COMPLIANCE REVIEW CHECKLIST FOR IT ACQUISITIONS

To obtain funding approval for any IT acquisition, purchase requestors must complete and submit this form as a paper or electronic attachment to the requisition. An IT acquisition is defined as an IT product – hardware and/or software, telecommunications software or equipment, and maintenance/service (including consulting services) on any hardware and/or software products.

The purpose of the Security Compliance Review Checklist is to document compliance with Clinger-Cohen Act of 1996, also known as the Information Technology Management Reform Act (ITMRA), Government Information Security Reform Act (GISRA), Federal Information Security Management Act of 2002 (FISMA), OMB A-130, 123, and 127, Treasury Directive P 85-70 and IRM 10.8.1. These primary policy statements are augmented by other OMB, FAR, NIST, Treasury and/or IRS guidance and/or mandates, established internal systems, data and physical security policies and technology standards. These more recent, detailed mandates may have necessary technical guidance applicable to current acquisitions.

If you have questions regarding the Security Compliance Review Checklist, please contact the Cybersecurity points of contact in Exhibit 2.21.1-2 of the IRM – Requisition Processing for IT Acquisition Products and Services.

Date:			
Requisition Number:			
Requisition Amount:			
Items Purchased:			
Vendor:			
Person who completed checklist			
First Name:		Last Name:	
Phone:		Email:	
QUESTION 1: Is this acquisition for a system with a current Security Certification and Accreditation, or an Interim Authority to Operate?			
Yes ☑ No ☐			
*If your answer is **NO**, contact the MITS ITSE (listed to the right) for guidance.*	Cybersecurity Policy & Programs IT Security Strategy & Performance, Manager, Strategic Planning, Investments and Governance (SPI-GOV) John Woodard OS:CIO:C:PP:SSP:IG O:(202) 283-4801 email: john.woodard@irs.gov Carl Christiansen O:(202) 283-0366 email: carl.c.christiansen@irs.gov		
*If your answer is **YES**, proceed to the Question 2*			
QUESTION 2: Is this IT acquisition either approved as in compliance with established Tier standards (i.e., Common Operating Environment), or has received a waiver from the applicable Tier Office(s)?			
Yes ☑ No ☐			
*If your answer is **NO**, contact the MITS ITSE (listed to the right) for guidance.*	Cybersecurity Policy & Programs IT Security Strategy & Performance, Manager, Strategic Planning, Investments and Governance (SPI-GOV) OS:CIO:C:PP:SSP:IG John Woodard O:(202) 283-4801 email: john.woodard@irs.gov Carl Christiansen O:(202) 283-0366 email: carl.c.christiansen@irs.gov		
*If your answer is **YES**, proceed to the Question 3*			

SECURITY COMPLIANCE REVIEW CHECKLIST FOR IT ACQUISITIONS

QUESTION 3: **Does this IT acquisition change/impact the current system's configuration as certified and accredited, or described in an Interim Authority to Operate?** (For example, if the IT acquisition is to add a desktop computer with a modem port to a system where the existing desktops do not have modem ports, then you are changing the system's configuration.)	
Yes ☐ No ☑	
*If your answer is **NO**, proceed to Question 4*	
*If your answer is **YES**, contact the MITS ITSE (listed to the right) for guidance.*	Cybersecurity Policy & Programs IT Security Strategy & Performance Strategic Planning, Investments and Governance (SPI-GOV) OS:CIO:C:PP:SSP:IG. John Woodard O:(202) 283-4801 email: john.woodard@irs.gov Carl Christiansen O:(202) 283-0366 email: carl.c.christiansen@irs.gov
QUESTION 4: **Does this IT acquisition provide a new function or service that uses one or more of the "security criteria" listed below:** ■ Exchange of Sensitive but Unclassified (SBU) information with any external body, agency, or activity? (Note: SBU includes Taxpayer Information, Privacy Act information, and information critical to the operation of the Service.) ■ Exchange of information across the Internet? ■ Changes in IRS infrastructure, including workstations, networks, or communications equipment, or firewalls or protective security mechanisms, whether by adding, changing, upgrading, or removing hardware or software components? ■ Involves implementations with the following critical issues: – Mobile Code technologies, including Active-X, JAVA Scripts, etc. – Data Warehousing – E-commerce – Use of ASP's through the Internet – Secure messaging technologies – Encryption technologies – Wireless – Remote maintenance access	
Yes ☐ No ☑	
*If your answer is **NO**, proceed to Question 5*	
*If your answer is **YES**, contact the MITS ITSE (listed to the right) for guidance.*	Cybersecurity Policy & Programs IT Security Strategy & Performance, Manager, Strategic Planning, Investments and Governance (SPI-GOV) OS:CIO:C:PP:SSP:IG John Woodard O:(202) 283-4801 email: john.woodard@irs.gov Carl Christiansen O:(202) 283-0366 email: carl.c.christiansen@irs.gov

SECURITY COMPLIANCE REVIEW CHECKLIST FOR IT ACQUISITIONS

QUESTION 5: Does this IT acquisition procure Windows XP, VISTA Workstation or Servers, or Internet Explorer?	
Yes ☐ No ☒	
*If your answer is **NO**, proceed to the next step*	
*If your answer is **YES**, use the FDCC contract language to the right in the procurement language/order.*	The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows http://csrc.nist.gov/itsec/guidance_WinXP.html Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: html, and for the Windows Vista settings see: http://csrc.nist.gov/itsec/guidance_vista.html. In accordance with OMB issued Policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems: "operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations."

Requester Certification

I have determined that each of the previous answers did not require contact with the Cybersecurity Organizations. If any of the above answers required contact for Guidance, I have made effective contact with the cited organization, and have received either a written Waiver, guidance, or established a Security Plan or C&A plan for this acquisition.

Printed Name	Signature	Date
Title		

Technical Point of Contact for Authorized Requester

First Name:		Last Name:	
Phone:		Email:	
Location:		GSS ISSO:	

Security Review and Certification

I have reviewed the requestor's checklist, SOW, requirements description, or other technical information.
I have provided appropriate security guidance in accordance with IRS Security policy and FISMA requirements.
I approve of this security review for the requisition. (If not recommended for approval, provide an explanation of the issue, what the requestor must perform and by when to obtain Cybersecurity's approval. If necessary elevate to Cybersecurity executive for additional review.)

If necessary, I have instructed the requestor to obtain a written waiver, Contractor Site Review, security engineering support or guidance, establish a Security Plan or request a C&A for this acquisition.

Printed Name	Signature	Date
Title		

Appendix VII

Statistical Projections for Information Technology Contract Sample Analysis Results

High-Risk Areas 3 and 13

All 6,045 contracts were subject to the controls of Risks 3 and 13. Of these, we found that 47 percent failed for Risk 3 and 16 percent failed for Risk 13. Projected to the entire population, we estimate that 2,858 contracts failed for Risk 3 and 948 contracts failed for Risk 13. The total contract dollars associated with these contracts are $2.99 billion (Risk 3) and $710 million (Risk 13). Figure 1 provides the details of our estimates.

Figure 1: Summary of Contracts for Failed Operational and Fraud Controls for High-Risk Areas 3 and 13[1]

High-Risk Areas	Estimated Number of Failed Contracts	Estimated Population Exception Rate	Estimated Exception Obligated Dollars
Contract Files Were Incomplete (Risk 3)	Point Estimate: 2,858	Point Estimate: 47%	Point Estimate: $2.99 billion
	Confidence Interval Estimate: 11 – 5,903	Confidence Interval Estimate: 0.18% – 98%	Confidence Interval Estimate: $1.65 billion – $3.32 billion
Contract Exclusion Reviews Were Not Conducted and Documented (Risk 13)	Point Estimate: 948	Point Estimate: 16%	Point Estimate: $710 million
	Confidence Interval Estimate: 778 – 1,119	Confidence Interval Estimate: 13% – 19%	Confidence Interval Estimate: $3.66 million – $1.42 billion

Source: Treasury Inspector General for Tax Administration analysis of contract files provided by the IRS.

[1] All projections are based on a two-sided 95 percent confidence interval.

High-Risk Areas 4 and 12

Of the 6,045 contracts, 1,390 were subject to the controls for Risks 4 and 12 because three contracts fell under the Simplified Acquisition Threshold amount of $150,000. Of these, we found that 8 percent failed for Risk 4 and 18 percent failed for Risk 12. Projected to the entire population, we estimate that 110 contracts failed for Risk 4 and 251 contracts failed for Risk 12. The total contract dollars associated with these contracts are $382 million (Risk 4) and $654 million (Risk 12). Figure 2 provides the details of our estimates.

Figure 2: Summary of Contracts for Failed Operational and Fraud Controls for High-Risk Areas 4 and 12[2]

High-Risk Areas	Estimated Number of Failed Contracts	Estimated Population Exception Rate	Estimated Exception Obligated Dollars
Contract Administration Plans Were Not Developed (Risk 4)	Point Estimate: 110	Point Estimate: 8%	Point Estimate: $382 million
	Confidence Interval Estimate: 2 – 281	Confidence Interval Estimate: 0.14% – 20%	Confidence Interval Estimate: $8.4 million – $918 million
COR Appointment Letters Were Not Fully Completed (Risk 12)	Point Estimate: 251	Point Estimate: 18%	Point Estimate: $654 million
	Confidence Interval Estimate: 51 – 450	Confidence Interval Estimate: 4% – 32%	Confidence Interval Estimate: $16 million – $1.29 billion

Source: Treasury Inspector General for Tax Administration analysis of contract files provided by the IRS.

[2] All projections are based on a two-sided 95 percent confidence interval.

Appendix VIII

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

APR 1 9 2016

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks (Audit #201520017) (e-trak #2016-79526)

Thank you for the opportunity to review the draft audit report on the post-award activities of the Information Technology (IT) contract administration process. We work closely with our Office of the Chief Procurement Officer to ensure IT products and services are effectively acquired for IRS programs. We take very seriously our responsibilities to conduct post-award activities in accordance with Federal guidelines to mitigate risk and to ensure all parties fulfill the requirements of the contracts.

While we generally agree with the recommendations, we have some concerns with certain aspects of the report. The audit's findings and projections are based on a sample of 14 contracts selected from a population of 6,045 contracts. Based on our knowledge of this population, we do not believe a representative or realistic picture of our implementation of contract controls is reliably created with so few observations.

Our concerns about the sampling methods give rise to other concerns. For example, the Security Compliance Review Checklist is one component of our comprehensive process to ensure the completeness of specific security requirements for IT and consulting services contracts. As we shared during discussions with the audit team, 8 of the 10 security checklists of interest to the audit did not require IT review and certification. Therefore, we believe concerns expressed in the audit report about inconsistent use and incomplete reviews of the security checklist are not as widespread as depicted, in particular, the outcome measure that security checklists may not have been sufficiently used for all 5,043 IT contracts subject to the checklist. Since we are committed to address any potential gaps, actions are already underway to revise the security checklist guidance and to emphasize existing policies and procedures for completing and retaining all procurement documents.

Although the IRS maintains that post-award IT contract management includes appropriate risk mitigation to deter high-risk contracting activities and complies with Federal policies and guidelines, we appreciate your audit recommendations and will address them in line with our existing commitment to monitor and improve practices for IT acquisitions. Our corrective action plan is attached and was coordinated with our Office of the Chief Procurement Officer.

If you have any questions, please contact me at (240) 613-9373 or a member of your staff may contact Carmelita White, Senior Manager, Program Oversight at (240) 613-2191.

Attachment

Attachment

Draft Audit Report – Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks
(Audit #201520017) (e-trak # 2016-79526)

RECOMMENDATION #1: The Chief Technology Officer should ensure that Internal Revenue Manual 2.21.1 is updated to provide clear guidance for effectively completing the Security Compliance Review Checklists.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The Security Compliance Review Checklist is currently undergoing a major revision that will result in an update to IRM 2.21.1. Cybersecurity will coordinate with the subject matter experts within the Information Technology organization to deliver updates to IRM 2.21.1 that provide clear guidance for effectively completing the Security Compliance Review Checklists.

IMPLEMENTATION DATE: October 15, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #2: The Chief Technology Officer should ensure that the Security Compliance Review Checklist template is updated to provide clear instructions for effectively completing the Security Compliance Review Checklists.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. The Security Compliance Review Checklist currently in use was partially updated in March 2016 to provide clear guidance and is undergoing a major revision that is scheduled to be completed by October 2016. Cybersecurity procedures will be updated with clear instructions to ensure subject matter experts within the Information Technology organization and the Office of the Chief Procurement Officer effectively use the updated Security Compliance Review Checklist.

IMPLEMENTATION DATE: October 15, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

Attachment

Draft Audit Report – Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks
(Audit #201520017) (e-trak # 2016-79526)

RECOMMENDATION #3: The Chief, Agency-Wide Shared Services, should ensure that Internal Revenue Service Policy and Procedure Memo Number 4.1 (*File Content Checklists*) is updated to ensure that Security Compliance Review Checklists are maintained as needed for review.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. Policy & Procedures Memorandum 4.1 (*File Content Checklists*) will be updated to include elements of the Information Technology Requisition Checklist which includes the Security Compliance Review Checklist.

During the course of the audit, the Office of Procurement was part of the Agency-Wide Shared Services organization. Effective December 27, 2015, the Office of Procurement was re-aligned and is now a direct report to the Deputy Commissioner for Operations Support (DCOS). Based on this reorganization, the responsible official for this corrective action will be "The Chief Procurement Officer."

IMPLEMENTATION DATE: April 15, 2016

RESPONSIBLE OFFICIAL: Chief Procurement Officer

CORRECTIVE ACTION MONITORING PLAN: Chief Procurement Officer will enter accepted corrective actions into Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #4: The Chief, Agency-Wide Shared Services, should ensure that all reviewers, including COs, execute Contract File Content Reviews so that all procurement documents for information technology contracts are complete, organized, current and consistent, and saved in contract files as required by Federal and IRS guidance.

CORRECTIVE ACTION #4: The IRS partially agrees with this recommendation. The Policy and Procedures Memorandum (P&P) 4.1 (*File Content Checklists*) requires use of the appropriate checklist based on the acquisition type. In addition, P&P 4.1(B) (Procurement Reviews) details the requirements for contract file reviews. The Office of Procurement Policy will emphasize the importance of conducting Contract File Reviews in the annual lessons learned training scheduled in May 2016. The Director of Procurement Policy has developed a Knowledge Power Hour (KPH) presentation on how to conduct Peer and Tier file reviews that will be presented on April 21, 2016. The Chief

Attachment

Draft Audit Report – Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks
(Audit #201520017) (e-trak # 2016-79526)

Procurement Officer will issue a memo to all managers and Contracting Officers reiterating the importance of file content and document retention.

During the course of the audit, the Office of Procurement was part of the Agency-Wide Shared Services organization. Effective December 27, 2015, the Office of Procurement was re-aligned and is now a direct report to the Deputy Commissioner for Operations Support (DCOS). Based on this reorganization, the responsible official for this corrective action will be "The Chief Procurement Officer."

IMPLEMENTATION DATE: June 15, 2016

RESPONSIBLE OFFICIAL: Chief Procurement Officer

CORRECTIVE ACTION MONITORING PLAN: Chief Procurement Officer will enter accepted corrective actions into Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #5: The Chief, Agency-Wide Shared Services, should ensure that Internal Revenue Service Policy and Procedures Memorandum 4.1 (*File Content Checklists*) is updated to clarify post-award contract administration information and/or data that is required to be maintained in contract files.

CORRECTIVE ACTION #5: The IRS partially agrees with this recommendation. The Policy and Procedures Memorandum 4.1 (*File Content Checklists*) adequately identifies post-award contract administration information and outlines documentation retention guidance. The Office of Procurement Policy will emphasize the importance of conducting Contract File Reviews in the annual lessons learned training scheduled in May 2016. The Director of Procurement Policy has developed a Knowledge Power Hour (KPH) presentation on how to conduct Peer and Tier file reviews that will be presented on April 21, 2016. The Chief Procurement Officer will issue a memo to all managers and Contracting Officers reiterating the importance of file content and document retention.

During the course of the audit, the Office of Procurement was part of the Agency-Wide Shared Services organization. Effective December 27, 2015, the Office of Procurement was re-aligned and is now a direct report to the Deputy Commissioner for Operations Support (DCOS). Based on this reorganization, the responsible official for this corrective action will be "The Chief Procurement Officer."

Attachment

Draft Audit Report – Improvements Are Needed for Information Technology Contract Administration Controls to Mitigate Risks
(Audit #201520017) (e-trak # 2016-79526)

IMPLEMENTATION DATE: June 15, 2016

RESPONSIBLE OFFICIAL: Chief Procurement Officer

CORRECTIVE ACTION MONITORING PLAN: Chief Procurement Officer will enter accepted corrective actions into Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

Appendix IX

Office of Audit Comments on Management's General Response

In response to our draft report, the Chief Technology Officer included a general response that we believe warrants comment. We summarized the general response and provided our related comment below.

Management's General Response: In the written management response to the draft report, the IRS expressed concerns about the sample size of 14 information technology contracts selected from a population of 6,045 and that it does not believe a representative or realistic picture of its implementation of contract controls is reliably created with so few observations.

> ***Office of Audit Comment:*** The sampling methodology was developed with the assistance of our contracted statistician. Appendices I and IV provide the methodology for the stratified random sample using four strata. Appendix VII presents the statistical projections for our information technology contract sample analysis results. We believe that our sample selection methodology, statistical projections, and other audit evidence provided with this review adequately support the audit report results and recommendations.
>
> The IRS's response also states that eight of the 10 Security Compliance Review Checklists subject to the audit "*did not require IT [Information Technology] review and certification*." However, as stated in our report, our review found a need for additional guidance for the security checklist to ensure that both product and service risks are adequately considered and contract administration policy and procedures are enforced. Following our discussions about the sufficiency of the checklist as a risk mitigation process, the IRS acknowledged that the security checklist along with guidance for its implementation are inadequate and are being reviewed and updated. For the contract files we analyzed, we observed that neither IRM 2.21.1 nor instructions for the Security Compliance Review Checklist provide clear direction or adequate guidance to consistently ensure that the requesting program office adequately responds to the questions used to determine whether further reviews from the Office of Cybersecurity are needed. Improvements are needed to help the IRS ensure that all products or services being acquired are in alignment with prevailing security guidance and mandates and established internal control systems, security policies, and technology standards. We maintain that due to deficiencies identified with the current security review checklist process, the security checklists for the 5,043 contracts awarded since October 1, 2009, have not provided sufficient information to adequately document risk mitigation controls as needed.