



*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

**August 26, 2010**

**Reference Number: 2010-20-084**

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



## HIGHLIGHTS

### **MORE ACTIONS ARE NEEDED TO CORRECT THE SECURITY ROLES AND RESPONSIBILITIES PORTION OF THE COMPUTER SECURITY MATERIAL WEAKNESS**

## Highlights

**Final Report issued on August 26, 2010**

Highlights of Reference Number: 2010-20-084 to the Internal Revenue Service Chief Technology Officer.

### **IMPACT ON TAXPAYERS**

The Federal Managers' Financial Integrity Act of 1982 requires that each agency conduct annual evaluations of its systems of internal accounting and administrative controls and submit an annual statement on the status of the agency's system of management controls, including identifying areas that can be considered material weaknesses. The Internal Revenue Service (IRS) prematurely closed the security roles and responsibilities component of its computer security material weakness. As a result, the IRS cannot ensure all IRS and contract employees will carry out their responsibilities to protect the confidentiality, integrity, and availability of taxpayer data.

### **WHY TIGTA DID THE AUDIT**

TIGTA initiated this audit at the request of the IRS to provide an independent validation assessment of the effectiveness of the IRS' actions to correct the roles and responsibilities component of the computer security material weakness. This audit was included in TIGTA's Fiscal Year 2010 Annual Audit Plan.

### **WHAT TIGTA FOUND**

While the IRS has made strides in addressing each set of corrective actions, our analysis found that the IRS did not effectively complete four of its six corrective action objectives. Specifically, the IRS did not 1) document all information technology (IT) security roles and responsibilities in the Internal Revenue Manual, 2) develop and document day-to-day IT security

procedures and guidelines, 3) properly conduct compliance assessments to test IT procedures, and 4) establish effective metrics for measuring compliance.

The IRS uses two documents, *IRS Roles Requiring an IT Security Training Curriculum* and *Internal Revenue Manual IT Security Roles and Responsibilities*, to document security roles and responsibilities. While each document is used for different purposes, the Internal Revenue Manual acts as the official policy over security roles and responsibilities. TIGTA identified that for 10 of 18 roles similar in both documents, the manual did not include all responsibilities established in the training curriculum. The IRS also did not document an additional five IT security roles existing at the IRS in the Internal Revenue Manual. Further, the IRS did not properly conduct compliance assessments to verify and validate that IRS and contract employees were executing their security responsibilities. Lastly, because the compliance assessment did not yield significant information, the IRS has yet to establish or collect meaningful performance metrics for this weakness area.

### **WHAT TIGTA RECOMMENDED**

TIGTA recommended that the Associate Chief Information Officer, Cybersecurity, update the Internal Revenue Manual to include all IT security roles in existence at the IRS, establish recurring processes and communications to ensure security roles and responsibilities are periodically reviewed and updated, and develop procedures to validate compliance that incorporate supporting evidence of proper execution of assigned responsibilities. In addition, the roles and responsibilities component of the computer security material weakness should be reopened.

In their response to the report, IRS officials agreed with 3 of the 4 recommendations. The IRS believes the roles and responsibilities component should be downgraded to a "Significant Deficiency" rather than be reopened. TIGTA disagrees with the IRS' assessment and believes repeatable processes are not in place. As such, TIGTA does not agree with the downgrade.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

August 26, 2010

**MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER**

*Michael R. Phillips*

**FROM:**

Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:**

Final Audit Report – More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness (Audit #200920016)

This report presents the results of our review to determine whether the Internal Revenue Service has effectively resolved the vulnerabilities relating to the information technology security roles and responsibilities component of the Internal Revenue Service computer security material weakness and implemented repeatable processes to ensure that this weakness does not recur. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2010 Annual Audit Plan and is part of our statutory requirements to annually review the adequacy and security of IRS information technology. This audit also addresses the major management challenge of Security.

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

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-8510.



*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

## *Table of Contents*

<b>Background</b> .....	Page 1
<b>Results of Review</b> .....	Page 3
Not All Information Technology Security Roles Were Documented in the Internal Revenue Manual, and Day-to-Day Security Procedures and Guidelines Were Not Developed and Documented .....	Page 4
<u>Recommendation 1:</u> .....	Page 8
Compliance Assessments Were Not Properly Conducted to Test and Validate Whether Security Roles and Responsibilities Were Being Carried Out.....	Page 8
<u>Recommendation 2:</u> .....	Page 12
Effective Metrics for Measuring and Improving Compliance With Information Technology Security Roles and Responsibilities Were Not Established .....	Page 13
<u>Recommendation 3:</u> .....	Page 14
<u>Recommendation 4:</u> .....	Page 14
<b>Appendices</b>	
Appendix I – Detailed Objective, Scope, and Methodology .....	Page 16
Appendix II – Major Contributors to This Report .....	Page 17
Appendix III – Report Distribution List .....	Page 18
Appendix IV – Internal Revenue Manual Roles Missing Responsibilities in the Training Curriculum.....	Page 19
Appendix V – Management’s Response to the Draft Report .....	Page 21



*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

## *Abbreviations*

FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IT	Information Technology
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TIGTA	Treasury Inspector General for Tax Information



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

## *Background*

The Federal Managers' Financial Integrity Act of 1982<sup>1</sup> requires that each agency conduct annual evaluations of its systems of internal accounting and administrative controls and submit an annual statement on the status of the agency's system of management controls. As part of the annual evaluations, agency managers identify control areas that can be considered material weaknesses. From its guidance on the Federal Manager's Financial Integrity Act, the Department of the Treasury and the Office of Management and Budget (OMB) define material weaknesses as "*shortcomings in operations or systems which, among other things, severely impair or threaten the organization's ability to accomplish its mission or to prepare timely, accurate financial statements or reports,*" or "*compromises the security of its information, information systems, personnel, or other resources, operations, or assets.*" The OMB monitors progress on material weaknesses declared by Federal Government agencies.

As a result of its Federal Manager's Financial Integrity Act evaluation and financial audit conducted by the Government Accountability Office (GAO) in 1997, the Internal Revenue Service (IRS) designated computer security as a material weakness. Subsequent to this declaration, the IRS further categorized the computer security material weakness into nine components,<sup>2</sup> one of which covered security roles and responsibilities. The IRS defined this component as appropriately delineating security roles and responsibilities within functional business, operating, and program units throughout the IRS. To help in its efforts to improve computer security, the IRS received a \$90 million increase for its information technology (IT) and computer security material weakness initiative for Fiscal Year 2010.

To address this component of the computer security material weakness, the IRS developed a plan to formally track and monitor the following corrective actions for resolving the security roles and responsibilities weakness.

1. Document IT security roles and responsibilities for IRS organizational units and for individual roles or positions.

---

<sup>1</sup> 31 U.S.C. §§ 1105, 1113, and 3512.

<sup>2</sup> The computer security material weakness components include: 1) network access controls; 2) key computer applications and system access controls; 3) software configuration; 4) functional business, operating, and program units security roles and responsibilities; 5) segregation of duties between system and security administrators; 6) contingency planning and disaster recovery; 7) monitoring of key networks and systems; 8) security training; and 9) certification and accreditation. The segregation of duties, security training, and certification and accreditation components have been closed.



*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

2. Develop and document day-to-day IT security procedures and guidelines for the execution and enforcement of security standards consistent with defined security roles and responsibilities.
3. Conduct independent compliance assessments to verify and validate that employees in IT security roles are properly executing their roles and responsibilities.
4. Conduct compliance assessments (i.e., social engineering tests) to revalidate that security roles and responsibilities are being properly carried out.
5. Develop and implement an updated communications strategy targeted at reinforcing IT security roles and responsibilities.
6. Establish and maintain collection and reporting of metrics<sup>3</sup> to assess the successful operation of the policy and ensure continuous monitoring of program areas.

The IRS reported the completion of all action items in its plan in March 2009, and the Security Services and Privacy Executive Steering Committee approved the closure of the security roles and responsibilities component. The IRS requested that the Treasury Inspector General for Tax Administration (TIGTA) provide an independent validation assessment of the effectiveness of the IRS' actions to address the security roles and responsibilities component of the computer security material weakness.

This review, which represents our validation efforts as requested by the IRS, was performed at the IRS National Headquarters in New Carrollton, Maryland, in the Office of Cybersecurity during the period September 2009 through April 2010. 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.

---

<sup>3</sup> Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.



*More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness*

## *Results of Review*

We reviewed available supporting documentation relating to the activities on the IRS’ corrective actions for resolving the security roles and responsibilities component of the computer security material weakness and found that the IRS had completed all actions for only two of six sets of corrective actions presented on its corrective action plan. The IRS effectively developed and implemented updated communications strategies. Specifically, the IRS increased security awareness through displays, electronic newsletters, literature, security surveys, and making security staff available to answer employees’ questions. The IRS also required all IRS and contract employees to complete an annual information protection briefing, which highlights information security policies on roles and responsibilities. In addition, the IRS hired a consulting firm to conduct social engineering efforts to revalidate security roles and responsibilities.

While the IRS has made strides in addressing each set of corrective actions, we found that the IRS did not effectively complete four of its six corrective actions and that not all actions taken by the IRS were effective in achieving its stated objectives. Figure 1 presents our results of each set of corrective actions.

**Figure 1: Assessment by Corrective Actions**

<b>Corrective Actions Necessary to Support Closure of the Roles and Responsibilities Component of the Computer Security Material Weakness</b>	<b>Documentation of Actions Support Corrective Action Closure per IRS</b>	<b>Documentation of Actions Support Corrective Action Closure per TIGTA</b>	<b>Were the Documented Corrective Actions Taken Effective?</b>
1. Document IT Security Roles and Responsibilities	Yes	No	No
2. Develop and Document Day-to-Day IT Security Procedures and Guidelines	Yes	No	No
3. Conduct Compliance Assessments to Verify and Validate Security Roles and Responsibilities	Yes	No	No
4. Conduct Compliance Assessments (i.e., Social Engineering) to Revalidate Security Roles and Responsibilities	Yes	Yes	Yes
5. Develop and Implement Updated Communications Strategy	Yes	Yes	Yes
6. Establish Metrics to Measure Successful Operations	Yes	No	No

*Source: TIGTA Analyses and Interviews*



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

Because of the lack of progress in completing corrective actions and implementing repeatable processes to ensure this weakness does not recur and the recent evidence of employee noncompliance with security responsibilities, we believe the IRS prematurely closed the security roles and responsibilities component, which should have remained open as part of the computer security material weakness. Specifically, the IRS did not:

- Document all IT security roles and responsibilities in the Internal Revenue Manual (IRM) and develop day-to-day IT security procedures and guidelines.
- Properly conduct compliance assessments to test the implementation of day-to-day IT procedures.
- Establish effective metrics for measuring and improving compliance with IT security roles and responsibilities.

***Not All Information Technology Security Roles Were Documented in the Internal Revenue Manual, and Day-to-Day Security Procedures and Guidelines Were Not Developed and Documented***

***Established security roles at the IRS were not included in the IRM***

The IRS issued the IRM section *IT Security Roles and Responsibilities* in December 2005 (and subsequently updated it in March 2007) to define and document IT security roles and responsibilities for IRS and contract employees and to support the closure of one of its planned corrective actions. In addition, the IRS developed and issued the training curriculum *IRS Roles Requiring an IT Security Training Curriculum* for employees performing in IT security roles with significant security duties. This curriculum was issued in April 2008 and was last updated in February 2009. It also defined IT security roles and responsibilities and provided both a curriculum for each role and the number of specialized IT security training hours required. The primary difference in these two documents is that the training curriculum specifically identifies security roles with significant security duties that require specialized training and the manual acts as the IRS' official policy over all security roles and responsibilities.

Although many roles are similar in both documents, the IRS did not document all IT security roles existing at the IRS into the IRM. The following 5 of 28 roles identified in the training curriculum are not included in the IRM. Employees performing in these security roles did not have official security-related responsibilities as set forth in the IRM. As of December 2009, the IRS reported the following number of employees performing in these roles.

1. Computer Audit Specialist (293 employees).
2. Functional Workstation Specialist (222 employees).
3. Technical Support Staff (855 employees).
4. Management/Program Analyst (569 employees).



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

5. System Designer (41 employees).

In addition, we found that for 10 of 18 roles that are similar in both documents, the IRM did not include all of the responsibilities that were established in the training curriculum. These 10 roles, along with the number of missing responsibilities, are as follows:

1. Chief Information Officer (1 responsibility).
2. Designated Accrediting Authority (1 responsibility).
3. Information Systems Security Officer (2 responsibilities).
4. Manager (2 responsibilities).
5. Privacy Official (3 responsibilities).
6. Program Management Official (4 responsibilities).
7. Security Specialist (2 responsibilities).
8. Senior Agency Information Security Officer (1 responsibility).
9. Systems Operations Staff (3 responsibilities).
10. Telecommunications Voice Specialist (5 responsibilities).

Appendix IV provides the details of the missing responsibilities for these 10 roles. Because the IRS uses both documents for different purposes, we believe the differences between the two documents may cause confusion over what each employee's official security-related responsibilities are.

The roles and responsibilities between these two documents were misaligned because the IRS Cybersecurity organization did not effectively communicate within its own groups the intent of each document or define which document contained the authoritative list of security roles and responsibilities for the IRS. During the course of our review, Cybersecurity organization personnel stated that the IRM was developed to document IT security "positions," not "roles" with significant security duties that require specialized training, despite the title of the document and its use to support the closure of their corrective action. They also stated that not all "positions" in the manual have significant IT security duties and did not require specialized training. In addition, Cybersecurity organization personnel stated that the Department of the Treasury policy does not require security "positions" in the IRM and IT security roles in the training curriculum to align. Subsequently, the Cybersecurity organization indicated that the IRM is the IRS' authoritative policy for identifying baseline IT security roles and responsibilities.

IRS and contract employees performing in IT security roles for which the IRS has not established official responsibilities cannot be held accountable for compliance with official duties. In addition, the discrepancy between the IRM and training curriculum roles may cause managers to not properly identify employees and contract employees as performing in IT security roles, whether for completing required specialized training or for assessing compliance with security responsibilities.



---

*More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness*

---

**Treasury-required and National Institute of Standards and Technology (NIST)-recommended security roles were not included in the IRM**

The Department of the Treasury IT Security Program's *Treasury Directive Publication 85-01* designates specific officials with key security responsibilities to ensure the success of the agency's security program. The Treasury Directive states that, in order to protect the integrity, confidentiality, and availability of information and information systems, individuals must understand their security-related roles and responsibilities. The Directive also identifies roles that require annual specialized IT security training. We found that the IRM lacked the following five key security roles that the Treasury Directive required:

- IT Security Policy and Guidance Personnel.
- Help Desk Personnel.
- Incident Handler.
- Quality Assurance Personnel.
- Change Management Staff.

In addition, the NIST Special Publication 800-16, *Draft Information Security Training Requirements: A Role and Performance-Based Model*,<sup>4</sup> recommends specialized training for employees performing in the following security roles, which were not evident in the IRS manual:

- Technical Support Personnel.
- Incident Response Coordinator/First Responders.
- Freedom of Information Act Official.
- Records Management Official.
- Office of General Counsel Staff.
- Source Selection Board Member.
- Risk/Vulnerability Analyst.
- Assessor.
- Risk Executive.
- Security Engineer.
- Data Center Manager.

Our analysis revealed IRS employees with similar responsibilities as the Department of the Treasury and NIST roles listed above. IRS employees who may have been performing in the various security roles listed above that were not yet formally documented in the IRM were sometimes identified with a more general security role category. For example, employees tasked with writing IRS security policy were identified as security specialists when the IT Security Policy and Guidance Personnel role would have been more appropriate. Also, employees tasked

---

<sup>4</sup> NIST is responsible for developing standards and guidelines, including minimum requirements, and for providing adequate information security for all agency operations and assets.



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

with handling incidents were identified as security specialists when the Incident Handler role would have been more appropriate.

This occurred because the IRS had not effectively completed its work to identify and document all existing security roles at the IRS, assign appropriate responsibilities to these roles, and identify the employees performing in these roles. In addition, the IRS did not have an effective repeatable process to ensure the manual is periodically updated to ensure all security roles in existence at the IRS are documented. This should be done through an adequate recurring review of the IRS environment, Treasury regulations, and applicable NIST guidance.

Cybersecurity organization personnel advised us that the lengthy process the IRS undergoes to update the manual prevented them from incorporating all Treasury-required and appropriate NIST-recommended IT security roles since its last update. However, they also advised us that the IRM is currently being updated and that Department of the Treasury and NIST roles are being considered. The Cybersecurity organization will establish recurring communications within its groups to ensure authorized IT security roles are aligned and consistent in both the IRM and training document.

Until the IRS has officially documented all security roles and responsibilities in existence at its agency and implemented a repeatable process to ensure roles and responsibilities are periodically reviewed and updated, it cannot ensure that all IRS and contract employees performing in these roles are complying with their appropriate security-related responsibilities. As a result, the IRS may be at more risk to the latest security threats and vulnerabilities.

**Day-to-day IT security procedures and guidelines were not developed and documented**

The IRS corrective action plan for resolving the roles and responsibilities component of its computer security material weakness required the IRS to develop and document day-to-day IT security procedures and guidelines for organizational units in executing and enforcing security standards consistent with defined security roles and responsibilities. The IRS closed this corrective action in February 2006. However, the sole artifact provided to us in support of this closure was the *IT Security Roles and Responsibilities* manual. This manual is the baseline policy on which specific day-to-day standard operating procedures and guidance for complying with security responsibilities should be based. This baseline policy is broad in nature and does not provide specificity of day-to-day operating procedures and guidance.

The Cybersecurity organization explained that personnel who worked on this corrective action were no longer with the organization and did not leave current Cybersecurity organization personnel with any further documentation. Recognizing this deficiency, the Cybersecurity organization sent out a request to the various business units to provide their standard operating procedures for implementing role-based responsibilities. At the time of our review, the Cybersecurity organization received documentation on day-to-day security procedures from one business unit. The Cybersecurity organization plans to collect and develop a catalog of security



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

role-related procedures and guidelines, which will then be used to ensure the day-to-day procedures align with IRS policy.

Until the IRS has documented and reviewed security role-related day-to-day procedures and guidelines in existence within its business units, it cannot ensure all employees performing in security roles are complying with their security-related responsibilities consistent with IRS policy.

### ***Recommendation***

**Recommendation 1:** The Associate Chief Information Officer, Cybersecurity, should: 1) update the IRM to include all IT security roles in existence at the IRS (including roles from the training curriculum, those required by the Department of the Treasury, and those recommended by the NIST, as appropriate) and the related responsibilities for each of these roles; 2) establish recurring processes and communications to ensure security roles and responsibilities in the IRM are periodically reviewed and updated and alignment between the IRM and the training curriculum is maintained; and 3) establish a process to periodically collect, update, and review security role-related procedures and guidelines to ensure day-to-day procedures align with current IRS policy.

**Management's Response:** IRS management agreed with this recommendation. The IRS will: 1) update the IRM to include all IT security roles and related responsibilities in existence at the IRS; 2) perform a crosswalk of the IRM with the IRS Specialized IT Security Training program annually and align any role differences; and 3) enhance its existing process to periodically collect, update, and review security role-related procedures and guidelines to ensure day-to-day procedures align with current IRS policy.

### ***Compliance Assessments Were Not Properly Conducted to Test and Validate Whether Security Roles and Responsibilities Were Being Carried Out***

#### **Completed assessments did not validate compliance with IRS security policy**

The IRS corrective action plan for resolving the roles and responsibilities component also required the IRS to conduct compliance assessments to verify and validate that employees in IT security roles were properly executing their security responsibilities. The Cybersecurity organization conducted two surveys, in June 2008 and February 2009, on employee compliance with their security roles and responsibilities. The Cybersecurity organization was in the process of reviewing the compliance survey results, as metrics data were not specific enough to demonstrate a trend of improvement, when the roles and responsibilities component was presented to the Security Services and Privacy Executive Steering Committee for closure approval. Based upon actions taken on the roles and responsibilities component, and without the



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

results of the compliance surveys, the Security Services and Privacy Executive Steering Committee approved the closure on March 25, 2009. The Cybersecurity organization subsequently established new metrics and conducted two additional compliance surveys, in May and August 2009, yielding greater than 99 percent of employees being aware of their roles, having knowledge of policies and guidance over their roles, and appropriately performing duties defined for their assigned roles. The Cybersecurity organization plans to continue conducting these compliance surveys at least annually to ensure continued compliance with established policies and procedures.

However, we found that the assessments that the IRS conducted were not sufficient to validate employee compliance with security responsibilities. The compliance surveys did not actually test for compliance with security responsibilities. To “test” selected employees, the Cybersecurity organization developed questionnaires by reproducing the roles and responsibilities listed in the 2005 version of the IRM. Questionnaires were sent to employees in advance of the interviews. The employee responded to the questionnaire by simply answering “yes” or “no” to whether or not they complied with the responsibilities listed or by referring to other organizations or employees if they believed that they were not responsible for that task.

The Cybersecurity organization took no further action to validate employees’ positive responses to ensure employees’ compliance with their responsibilities. Also, referrals of responsibilities made by employees to other organizations or employees were not verified or followed up on to confirm compliance. Furthermore, surveyors conducting the compliance assessments did not have adequate knowledge of the security areas to determine whether responsibilities were correctly referred and, therefore, relied solely on the oral testimony of employees’ understanding of their roles and responsibilities.

Asking employees whether or not they are responsible for various security-related activities may help instill knowledge and understanding of these responsibilities, but their responses do not in themselves provide evidence of compliance with their responsibilities. The Cybersecurity organization subsequently advised us that the intent of the exercise was not to assess employee compliance, but to assess the employee’s knowledge of his or her security responsibilities. To remedy this difference, the Cybersecurity organization informed us that it is in the process of establishing improved compliance assessment procedures that will produce measurable results. For example, the Cybersecurity organization plans to explore using the results of scans run on systems that determine the system’s compliance with security settings for validating employee compliance with security policy.

**Not all IRS and contract employees performing in IT security roles have been identified**

We also found that the delivery of compliance surveys was flawed because not all IRS and contract employees performing in IT security roles were included in the population for compliance testing. IRS business unit managers are responsible for identifying employees



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

performing in IT security roles that require specialized training within their respective business units. To identify their employees in IT security roles, managers are asked to review the role descriptions in the *IRS Roles Requiring an IT Security Training Curriculum* to determine which best matches their employees' responsibilities. Once identified, managers request that these employees be added to the *IT SEC Training Master List* (Master List). The IRS uses the Master List to monitor the identified employees' progress towards completion of their required training hours and for reporting this information to the OMB in accordance with Federal Information Security Management Act (FISMA)<sup>5</sup> requirements.

The Cybersecurity organization relied solely on the Master List as its basis for employee selection when conducting the compliance surveys. Because the Master List contains only IRS employees identified in IT security roles requiring specialized training, not all employees in existing IT security roles specified by the IRM, required by the Department of the Treasury, or recommended by the NIST were included in the population for compliance testing.

The IRM contained 11 additional IT security roles that the training curriculum did not contain. Therefore, IRS and contract employees performing in these roles were not assessed for compliance or for completion of training requirements as needed. To determine the number of IRS employees performing in these 11 roles, we researched the IRS directory for similar titles. However, because the IRS directory position titles do not necessarily align with security role titles, we were unable to identify, with absolute certainty, the number of IRS and contract employees performing in these security roles. Based on our research, we estimated the number of IRS and contract employees potentially filling these roles as follows.<sup>6</sup>

1. Agency Head (1 employee).
2. Certification Agent.
3. Senior Management/Executive (65 employees).
4. Business System Planner.
5. Information Owner.
6. Accrediting Official Designated Representative.
7. Enterprise Architect (9 employees).
8. Chief Financial Officer (1 employee).
9. Physical Security Officer (45 employees).
10. Personnel Security Officer (15 employees).
11. Encryption Recovery Agent.

Cybersecurity organization personnel advised us that they are aware that relying on managers to identify employees in security roles that require specialized training may cause some employees to not be on the Master List or included in the survey population because managers do not

---

<sup>5</sup> 44 U.S.C. §§ 3541 - 3549.

<sup>6</sup> A security role listed without a corresponding number indicates the security role did not align with a position title.



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

always apply the role definitions consistently. The IRS is developing new techniques for identifying employees performing in all existing security roles.

Further, we also found that the Master List did not include contract employees. The IRS is not required to provide specialized training to contract employees because the contract organization is responsible for its contract employees to have and maintain the necessary level of technical expertise to accomplish the various tasks defined within the contracts. The IRS also advised us that no after-hire formal compliance process exists that reports on the accuracy of a contract employee's adherence to published policy and procedures. Instead, assurance for whether a contract employee is performing his or her work in adherence to established policy and procedure is the day-to-day responsibility of the IRS project manager and contract representative overseeing the contract employee's work.

Even so, contract employees may be performing in IT security roles with the same responsibilities as IRS employees and, therefore, should be identified in these roles and included in the population for selection in the compliance testing. We identified more than 1,350 contract employees with system access that held titles related to security roles, such as system administrators, database administrators, programmers, developers, security specialists, system architects, system engineers, and web developers. These job titles may or may not align with IRS security roles.

The IRS has not yet established an adequate method to identify which contractors are performing in IRS security roles. However, the Cybersecurity organization informed us that it plans to develop a process to identify contract employees with system access for inclusion in the compliance assessment population and to include instructions in the compliance assessment standard operating procedures to incorporate contract employees as part of the compliance surveys.

**Employees selected for the compliance surveys were not measured against current or role-based IT security responsibilities**

As mentioned earlier, the IRS developed questionnaires by reproducing the roles and responsibilities listed from the 2005 version of the IRM. Although a 2007 version had been issued, the IRS continued to use the older version<sup>7</sup> in order to facilitate consistent testing and trending of results. However, we identified 6 roles in the 2005 version that were updated with 25 additional responsibilities in the 2007 version. As a result, significant responsibilities were not included in the questionnaires, such as the following two examples.

- Security specialists must conduct security audits, verifications, and acceptance checks, while maintaining documentation on the results.

---

<sup>7</sup> The IRS used the older version of the IRM for all but four of its roles when conducting the compliance assessments. The four roles include Desktop Employee, Manager, Telecom Specialist, and System Administrator.



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

- Contracting Officers Technical Representatives must protect any personally identifiable information that they have in their possession, whether it is paper-based or in electronic form.

In addition, for compliance survey selected employees in roles that did not clearly translate to an IRM role,<sup>8</sup> Cybersecurity organization personnel conducted the compliance survey using generic “employee” responsibilities covering basic security awareness and training instead of against specific role-based responsibilities. This approach occurred because the IRS had not yet fully developed or implemented authoritative security roles and responsibilities enterprise-wide nor developed adequate and repeatable procedures to validate compliance security-related responsibilities.

Until the IRS fully documents its security roles and related responsibilities, is able to identify IRS and contract employees performing in these roles, and develops adequate and repeatable processes to validate employees’ and contractor employees’ compliance with their security-related responsibilities, the IRS cannot ensure that its security procedures and policies are being carried out as intended.

## ***Recommendation***

***Recommendation 2:*** The Associate Chief Information Officer, Cybersecurity, should: 1) develop an effective and repeatable method to identify all IRS and contract employees performing in established IT security roles, 2) include all IRS and contract employees performing in IT security roles in the population for potential selection in the compliance assessments, and 3) develop adequate procedures to validate compliance with current security role-related responsibilities through compliance assessments that incorporate supporting evidence of proper execution of assigned responsibilities.

***Management’s Response:*** IRS management agreed with this recommendation. The IRS has an effective and repeatable method to identify all IRS employees performing in established IT security roles. The IRS will incorporate contract employees in its existing method for identifying IRS employees in established IT security roles by including them in its yearly requests to IRS training coordinators asking for names of all IRS and contract employees who perform security roles. The IRS will use this population of all IRS and contract employees for potential selection in the compliance assessments. In addition, the IRS will improve existing procedures to validate compliance with current security role-related responsibilities through compliance assessments that incorporate supporting evidence of proper execution of assigned responsibilities.

---

<sup>8</sup> These roles are Computer Audit Specialist, Functional Workstation Specialist, Technical Support Staff, Management/Program Analyst, and System Designer.



---

*More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness*

---

**Office of Audit Comment:** The TIGTA disagrees that the IRS has an effective and repeatable method in place to identify all IRS employees performing in established IT security roles. The referenced method is the process the IRS has used to identify employees in IT security roles requiring specialized training, based on the IRS' IT Security Training Curriculum document. As stated in our report, this method was not sufficiently identifying all employees performing in the roles currently requiring specialized training, nor was it sufficient to identify all employees in IT security roles specified by the IRM, required by the Department of the Treasury, or recommended by the NIST. For that reason, the IRS previously informed us that it was developing new techniques for identifying these employees. We maintain that the IRS needs to improve its identification methods of IRS and contract employees performing in all established IT security roles to ensure an accurate population is maintained and compliance with security responsibilities is properly assessed.

***Effective Metrics for Measuring and Improving Compliance With Information Technology Security Roles and Responsibilities Were Not Established***

The final step in the IRS corrective action plan for resolving the roles and responsibilities component of its computer security material weakness required the IRS to establish and maintain the collection and reporting of metrics to assess the successful operation of the policy regarding roles and responsibilities and ensure continuous monitoring of the program area. Because the compliance assessments did not yield significant information, the IRS has yet to establish or collect meaningful metrics.

As with the other incomplete corrective actions, the IRS informed us it plans to: 1) establish sufficient metrics that will allow analysis of key trends or themes that require improvement, 2) communicate these issues to management, 3) use the metrics information to develop targeted communications, and 4) effect continued process improvement in role execution.

The IRS believes the actions taken thus far support the downgrade of the security roles and responsibilities component from a material weakness to a control deficiency, and it has repeatable processes in place that address the key issues and significant risks posed by the original finding.<sup>9</sup> The IRS also believes that its planned additional actions will further strengthen and enhance its existing repeatable processes.

We believe that the repeatable processes are not in place over this computer security material weakness component area. While we agree the actions planned, once implemented, would

---

<sup>9</sup> During the course of this review, the IRS assessed the roles and responsibilities component as a control deficiency; but in their official management response to the draft report, the IRS reassessed this component and increased its materiality one level higher to a significant deficiency.



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

appear to fully address this weakness, we cannot support a downgrade of this component based on planned actions. Because controls have not been fully implemented and repeatable processes are not in place, both the TIGTA and the GAO have continued to identify multiple instances in the past year where employees have not performed their assigned responsibilities. Examples include systems administrators not complying with secure password requirements that led to servers insufficiently protected, security officers not promptly removing employee physical access to restricted areas, employees not properly configuring system access that allowed unencrypted data to be transferred between centers, an employee executing the roles of both database administrator and system administrator despite policy prohibiting this combination of system rights,<sup>10</sup> and Contracting Officers' Technical Representatives not performing day-to-day contract oversight or verifying deliverables.<sup>11</sup>

Until the IRS completes its official documentation of all security roles and related responsibilities, identifies all IRS and contract employees performing in security roles, ensures all employees are equipped with appropriate training, implements adequate procedures to validate compliance with employee security responsibilities, and establishes adequate collection and reporting of metrics to improve roles and responsibilities implementation, the IRS cannot ensure all IRS and contract employees will carry out their responsibilities to protect the confidentiality, integrity, and availability of taxpayer data.

## ***Recommendations***

**Recommendation 3:** The Associate Chief Information Officer, Cybersecurity, should ensure adequate and accurate metrics are established that assess progress and can be analyzed to develop actions to further improve implementation of security roles and responsibilities policy.

**Management's Response:** IRS management agreed with this recommendation. The IRS' Modernization and Information Technology Services Cybersecurity organization will establish memoranda of understanding/memoranda of agreements with IRS business and functional units to ensure adequate and accurate metrics are established. The memoranda will define metrics and establish measures. The Cybersecurity organization will also work with the business and functional units to determine the required metric information, format, and timelines for continuous collection and reporting and to effect continued process improvement.

**Recommendation 4:** The Director of Wage and Investment, Business Systems Planning, and the Associate Chief Information Officer, Cybersecurity, as the Co-Chairpersons of the Security Services and Privacy Executive Steering Committee, should review the findings in this report

---

<sup>10</sup> *Information Security – IRS Needs to Continue to Address Significant Weaknesses* (Reference Number GAO-10-355, dated March 2010).

<sup>11</sup> *Controls Over the Contracting Officer's Technical Representatives Workforce Were Ineffective, Resulting in Significant Risks to the Government* (Reference Number 2009-10-139, dated September 30, 2009).



*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

and reopen the roles and responsibilities component of the computer security material weakness. The roles and responsibilities component should remain open until corrective actions have been fully implemented and completed, repeatable processes are in place, and results can be validated.

**Management's Response:** IRS management disagreed with this recommendation. After reviewing this report and the recurring processes and procedures in place, the IRS believes this component of the computer security material weakness has dropped below the threshold of materiality as defined by the GAO. The IRS considers this component in a state of "Significant Deficiency" and will maintain focus, with appropriate governance oversight, on maturing these processes and procedures to comply with applicable best practices and further reducing their overall risk.

**Office of Audit Comment:** The TIGTA disagrees with IRS' assessment that the roles and responsibilities component of the computer security material weakness be downgraded to a significant deficiency. As stated in our report, the lack of progress in completing four of the six corrective actions and implementing repeatable processes to ensure this weakness does not recur, along with the recent evidence of employee noncompliance with security responsibilities, preclude us from agreeing to a downgrade at this time.



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

## **Appendix I**

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to determine whether the IRS has effectively resolved the vulnerabilities relating to the information technology security roles and responsibilities component of the IRS computer security material weakness, and implemented repeatable processes to ensure that this weakness does not recur. Specifically, we:

- I. Determined whether the actions taken to resolve the security roles and responsibilities vulnerabilities were sufficient to close this component of the IRS computer security material weakness.
  - A. Reviewed prior TIGTA and GAO reports for Fiscal Years 2007–2009 and other applicable IRS documentation regarding the security roles and responsibilities. We determined whether the IRS satisfactorily completed prior TIGTA recommendations relating to security roles and responsibilities and closed them in the Joint Audit Management Enterprise System, if applicable.
  - B. Determined whether the IRS policy for roles and responsibilities complies with Federal and Department of the Treasury regulations.
  - C. Determined whether the IRS has completed its own planned corrective actions for resolving the roles and responsibilities component of the IRS computer security material weakness.
  - D. Determined whether the performance metrics established by the IRS are effective for monitoring compliance and ensuring that the security roles and responsibilities weakness will not recur.
  - E. Interviewed appropriate IRS management as needed to determine causes for deficiencies found in the IRS security roles and responsibilities program.

#### **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: Department of the Treasury regulations, Government guidelines, IRS policies, and the IRS computer security material weakness plan of actions. We evaluated these internal controls by interviewing management and reviewing supporting documentation.



*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

## **Appendix II**

### *Major Contributors to This Report*

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)

Kent Sagara, Director, Systems Security

Jody L. Kitazono, Audit Manager

Louis Lee, Lead Auditor

Richard Borst, Senior Auditor

Kasey Koontz, Auditor



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

## **Appendix III**

### *Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Deputy Commissioner for Services and Enforcement SE  
Commissioner, Wage and Investment Division SE:W  
Associate Chief Information Officer, Cybersecurity OS:CTO:C  
Director, Business Modernization Office, Wage and Investment Division SE:W:BMO  
Director, Business Systems Planning, Wage and Investment Division SE:W:BMO:BSP  
Director, Stakeholder Management Division OS:CIO:SM  
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 Liaison:  
    Chief Technology Officer OS:CTO



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

## **Appendix IV**

### *Internal Revenue Manual Roles Missing Responsibilities in the Training Curriculum*

The following roles defined in IRM 10.8.2 were missing responsibilities listed in the training curriculum document. The discrepancies in these two documents may cause employees confusion over their official security-related responsibilities.

1. Chief Information Officer
  - Conducts training and awareness programs.
2. Designated Accrediting Authority
  - The creation, maintenance, and execution of the plan of action and milestones.
3. Information Systems Security Officer
  - Ensuring there is a current security plan and IT contingency plan for the assigned general support system.
  - Promoting IT security awareness and assisting in the identification of personnel with significant security responsibilities to receive both initial and refresher role-based security training.
4. Manager
  - Providing technical direction of or supervision over an employee or employees with significant security roles, such as Security Specialist; System Administrator (responsible for maintaining access controls or system security parameters), or Network Administrator (responsible for maintaining secure configuration of a network).
  - Providing technical direction of or supervision over employees who ensure the confidentiality, integrity, and availability of the network and its information resources.
5. Privacy Official
  - Establishing and managing privacy policies and the Privacy Impact Assessment processes/procedures.
  - Managing a centralized evaluation capability to oversee compliance with Unauthorized Access policy and program.



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

- Reporting on the progress of the IRS efforts being taken and making recommendations for improving the effectiveness of the Unauthorized Access program to IRS Management.
6. Program Management Official
    - Ensures that the business impact of weaknesses are assessed and prioritized.
    - Ensures all certification and accreditation documents exist and are updated, including the Privacy Impact Assessment.
    - Identifies business unit personnel in need of security training.
    - Escalates issues to appropriate parties as necessary.
  7. Security Specialist
    - Determining strategy and priorities.
    - Performing a role in business continuity planning.
  8. Senior Agency Information Security Officer
    - Oversees the submission of the formal FISMA reports and their supporting processes, and also oversees IRS responses to TIGTA and GAO audits.
  9. Systems Operations Staff
    - Runs all backup and data maintenance tasks according to the systems' specific schedule.
    - Directly accounts for the security of all physical/mechanical aspects of the system and coordinates any external interaction with the system, such as those involving customer engineers/vendor technicians.
    - Keeps logs of the results of all scheduled system tasks and shares that information with systems administration personnel to facilitate monitoring of the system.
  10. Telecommunications Voice Specialist
    - Voice messaging system applications, which includes adding, deleting, and modifying users.
    - All circuitry ingress and egress at all facilities under his/her control.
    - Video applications (compressed and satellite).
    - Employee relocations, ensuring that all telephonic equipment is relocated correctly and timely.
    - Monitoring the network system with authorized tools to ensure a healthy state.



*More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness*

**Appendix V**

*Management's Response to the Draft Report*



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

JUL 26 2010

RECEIVED  
JUL 27 2010

BY: *DAS*

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:

Terence V. Milholland  
Chief Technology Officer

*James M. McNamee for*

SUBJECT:

Draft Audit Report – More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness (Audit #200920016) (i-trak #2010-12202)

Thank you for the opportunity to review and respond to the subject draft audit report. We appreciate the report recognizing the Internal Revenue Service (IRS) made strides in addressing each set of corrective actions for resolving the security roles and responsibilities component of the computer security material weakness (CSMW). Specifically, the report acknowledged we implemented updated communication strategies, increased security awareness, and hired a consulting firm to conduct social engineering efforts to revalidate security roles and responsibilities.

The IRS' Modernization and Information Technology Services organization is committed to continuously improving the security of our information technology systems and processes; your report recommendations will further improve our security posture. We concur with three of the four report recommendations. We do not concur with the recommendation to reopen this component of the CSMW. After reviewing this report and the recurring processes and procedures in place, we believe this component has dropped below the threshold of materiality and is in a state of significant deficiency. We will maintain focus, with appropriate governance oversight, on maturing these processes and procedures and further reducing our overall risk. The attachment to this memo details our planned corrective actions to the report recommendations.

We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (202) 622-6800 or Darrin Brown, Senior Manager of Program Oversight, at (202) 283-4613.

Attachment



*More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness*

Attachment

Draft Audit Report – More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness (Audit # 200920016) (i-trak #2010-12202)

**RECOMMENDATION #1:** The Associate Chief Information Officer, Cybersecurity, should: 1) update the IRM to include all IT security roles in existence at the IRS (including roles from the training curriculum, those required by the Department of the Treasury, and those recommended by the NIST, as appropriate) and the related responsibilities for each of these roles; 2) establish recurring processes and communications to ensure security roles and responsibilities in the IRM are periodically reviewed and updated and alignment between the IRM and the training curriculum is maintained; and 3) establish a process to periodically collect, update, and review security role-related procedures and guidelines to ensure day-to-day procedures align with current IRS policy.

**CORRECTIVE ACTION #1:** The Internal Revenue Service (IRS) will update IRM 10.8.2 to include all Information Technology (IT) security roles and their related responsibilities in existence at the IRS. We will perform a crosswalk of the IRM 10.8.2 with the IRS Specialized IT Security Training program annually and align any role differences into the program from the IRM.

The IRS will also enhance its existing process to periodically collect; update and review security role-related procedures and guidelines to ensure day-to-day procedures align with current IRS policy.

**IMPLEMENTATION DATE:** February 1, 2011

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

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

**RECOMMENDATION #2:** The Associate Chief Information Officer, Cybersecurity, should: 1) develop an effective and repeatable method to identify all IRS and contract employees performing in established IT security roles, 2) include all IRS and contract employees performing in IT security roles in the population for potential selection in the compliance assessments, and 3) develop adequate procedures to validate compliance with current security role-related responsibilities through compliance assessments that incorporate supporting evidence of proper execution of assigned responsibilities.

**CORRECTIVE ACTION #2:** The IRS has an effective and repeatable method to identify all Service employees performing in established IT security roles. IRS will incorporate contract employees in existing methods for identification in established IT security roles by including them in our yearly requests to IRS Training coordinators asking for names of all employees and contractors who perform security roles.



*More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness*

Attachment

Draft Audit Report – More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness (Audit # 200920016) (i-trak #2010-12202)

IRS will use the provided population of all IRS and contract employees performing in IT security roles for potential selection in the compliance assessments based on the information provided. Moreover, IRS will improve existing procedures to validate compliance with current security role-related responsibilities through compliance assessments that incorporate supporting evidence of proper execution of assigned responsibilities.

**IMPLEMENTATION DATE:** February 1, 2012

**RESPONSIBLE OFFICIALS:** Associate Chief Information Officer, Cybersecurity

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

**RECOMMENDATION #3:** The Associate Chief Information Officer, Cybersecurity, should ensure adequate and accurate metrics are established that assess progress and can be analyzed to develop actions to further improve implementation of security roles and responsibilities policy.

**CORRECTIVE ACTION #3:** IRS's Modernization and Information Technology Services (MITS) Cybersecurity organization will establish memoranda of understanding/memoranda of agreement (MOUs/MOAs) with IRS business and functional units, the owners of compliance review results, to ensure adequate and accurate metrics are established. The MOUs/MOAs will define metrics and establish measures. MITS Cybersecurity will work with the business and functional units to determine the required metric information, format, and timelines for continuous collection and reporting and to effect continued process improvement.

**IMPLEMENTATION DATE:** February 1, 2011

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

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

**RECOMMENDATION #4:** The Director of Wage and Investment, Business Systems Planning, and the Associate Chief Information Officer, Cybersecurity, as the Co-Chairpersons of the Security Services and Privacy Executive Steering Committee, should review the findings in this report and reopen the roles and responsibilities component of the computer security material weakness (CSMW). The roles and responsibilities component should remain open until corrective actions have been fully implemented and completed, repeatable processes are in place, and results can be validated.



---

*More Actions Are Needed to Correct the  
Security Roles and Responsibilities Portion  
of the Computer Security Material Weakness*

---

Attachment

Draft Audit Report – More Actions Are Needed to Correct the Security Roles and  
Responsibilities Portion of the Computer Security Material Weakness (Audit # 200920016)  
(i-trak #2010-12202)

---

**CORRECTIVE ACTION #4:** While the IRS appreciates and understands the recommendation provided by TIGTA, we do not concur. After reviewing this report and the recurring processes and procedures in place, this component of the CSMW has dropped below the threshold of materiality as defined by the U.S. Government Accountability Office. We consider this component in a state of “Significant Deficiency” and we will maintain focus, with appropriate governance oversight, on maturing these processes and procedures to comply with applicable best practices and further reducing our overall risk.

**IMPLEMENTATION DATE:** N/A

**RESPONSIBLE OFFICIALS:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** N/A