Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness

September 2004

Reference Number: 2004-20-155

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 29, 2004

MEMORANDUM FOR CHIEF INFORMATION OFFICER
CHIEF, MISSION ASSURANCE

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness (Audit # 200420003)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has effectively resolved the vulnerabilities associated with its computer security material weakness. The IRS has categorized this material weakness into nine areas,[1] three of which are addressed in this report: security roles and responsibilities, segregation of duties, and security training. From our perspective, these three areas collectively address the root causes of many of the security weaknesses covered in the other six material weakness areas reported by the IRS.

The Department of the Treasury requested that the Treasury Inspector General for Tax Administration (TIGTA) provide an independent assessment of the effectiveness of the IRS' actions to address its computer security material weakness. This review is one of five reviews conducted this fiscal year to meet this request.

In summary, the IRS has taken some key steps to address security roles and responsibilities, segregation of duties, and training. Efforts on segregation of duties, in particular, justify closure of this area from the computer security material weakness. The IRS has effectively defined and segregated security tasks among key employees to reduce the opportunity for any one person to perpetrate and conceal inappropriate or fraudulent activities. Existing security weaknesses were not attributed to inadequate segregation of duties.

[1] The computer security material weakness consists of (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.

Much work remains, though, before the roles and responsibilities and training areas are closed. Until these areas are adequately addressed, the IRS will have little chance of implementing effective security controls, and computer security will remain a material weakness.

While security roles and responsibilities have been defined, we continue to identify significant security weaknesses throughout the IRS that we attribute to key employees not performing those responsibilities. For example, vulnerabilities continue to exist on the network and in sensitive systems across the IRS. Patch management and/or audit trail weaknesses are prevalent in the Mainframe, UNIX, and Windows computer environments. In addition, business owners have not carried out their responsibilities to accredit their systems and to annually assess the security controls of those systems.

The IRS has initiated actions to address the training material weakness area; however, more actions are needed before it is downgraded or closed. Several steps were not completed or were not effective. Specifically, the following steps need further improvement: identifying employees with key security responsibilities, effectively communicating the security core training curriculum and training courses, and periodically monitoring for course participation.

While we recommended the Chief, Mission Assurance, remove the segregation of duties area from the computer security material weakness, we recommended the security roles and responsibilities area remain part of the computer security material weakness until corrective actions related to prior TIGTA recommendations have been addressed. The Chief, Mission Assurance, should also keep the security training area as part of the computer security material weakness until all employees with key security responsibilities are identified, monitored, and adequately trained. We also recommended the Chief Information Officer ensure his employees with key security responsibilities are adequately trained to perform security duties and tasks.

Management's Response: Management's response was due on September 27, 2004. As of September 28, 2004, management had not responded to the draft report.

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 Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness

Background

The Federal Managers' Financial Integrity Act of 1982[1] 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 evaluations, agency managers identify control areas that can be considered material or significant weaknesses.

The Department of the Treasury has defined a material weakness 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." The Office of Management and Budget (OMB) monitors progress on these weaknesses.

When the Internal Revenue Service (IRS) Security Program evaluated the state of security within the IRS in 1997, it noted the lack of detailed security policies, procedures, standards, and requirements. It found that IRS officials were interpreting policies and procedures in a variety of ways. In some cases, IRS officials were unaware of, or were ignoring, the policies and procedures, resulting in an undisciplined security environment. As a result, the IRS declared five security areas as material weaknesses.[2]

In October 2002, the IRS combined the five security material weaknesses that were mostly based on facility types into one material weakness. Its goal was to address computer security from an enterprise-wide approach and better align the weakness areas with the new organizational structure. The IRS further categorized the computer security material weakness into nine areas.[3]

[1] 31 U.S.C. §§ 1105, 1113, 3512 (2000).

[2] The five material weaknesses were Computing Center Security, Field Office Security, Service Center Security, Other IRS Facility Security, and System Certification.

[3] The computer security material weakness consists of (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 Department of the Treasury requested that the Treasury Inspector General for Tax Administration provide an independent assessment of the effectiveness of the IRS' actions to address the computer security material weakness. This report is one of five reviews we conducted this fiscal year to meet this request and addresses the following three weaknesses:

1) Computer security roles and responsibilities were not defined for functions in the business units and the office of the Chief Information Officer as required by the Federal Information Security Management Act (FISMA).[4]
2) Duties were not segregated between system administrator and security administrator responsibilities.
3) Computer security training was not provided to employees who are assigned key security responsibilities.

From our perspective, the three areas collectively address the root causes of many of the security weaknesses covered in the other six material weakness areas reported by the IRS (network access, application and system access, system software configuration, audit trails, disaster recovery, and certification and accreditation of sensitive systems).

This audit was conducted in the Office of Mission Assurance and the Information Technology Services (ITS) organization at the IRS Headquarters in New Carrollton, Maryland; the Brookhaven, New York, and Memphis, Tennessee Campuses;[5] and the Martinsburg, West Virginia, and Memphis, Tennessee, Computing Centers[6] during the period August 2003 through May 2004. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in

[4] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[5] IRS campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.
[6] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

Appendix I. Major contributors to the report are listed in Appendix II.

Better Implementation of Roles and Responsibilities Is Needed Before This Material Weakness Area Is Downgraded

IRS policy requires all IRS employees and contractors to be responsible for ensuring the confidentiality, integrity, and availability of data processed or stored on the computer systems. Each employee and contractor has a security role, sometimes several roles, with a corresponding set of routine responsibilities.

The IRS has assigned technical computer security responsibilities to system administrators and security administrators. Generally, system administrators are responsible for day-to-day systems operations, and security administrators are responsible for specific security tasks and security oversight. The ITS organization has responsibility for ensuring system administrators carry out their system-related duties, while the Office of Mission Assurance has responsibility for providing oversight and guidance when needed.

Other employees also have security-related responsibilities. For example, business owners must conduct annual security self-assessments of their systems, as required by the FISMA. Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. In addition, business owners are required to accredit their information systems at least once every 3 years.

National Institute of Standards and Technology (NIST) guidance states that a successful information technology (IT) security program includes: 1) developing an IT security policy that reflects business needs tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and 3) establishing processes for monitoring and reviewing the program.[7]

The IRS planned to complete the following actions to address the roles and responsibilities material weakness area:

[7] NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003).

- Define security roles and responsibilities.
- Finalize procedures and guidelines for security roles and responsibilities. Pilot test security roles and responsibilities at model facilities.
- Complete rollout schedules and the training program needed to execute and enforce security standards.
- Implement security procedures and guidelines.
- Conduct compliance assessments to ensure roles and responsibilities are effectively implemented.

The IRS has taken some key steps to address the security roles and responsibilities material weakness area by completing the following actions:

- Developed a roles and responsibilities matrix incorporating guidance from the Internal Revenue Manual (IRM), NIST, public laws, and regulations.
- Verified that the security roles and responsibilities matrix was appropriate, reasonable, and complete.
- Obtained feedback on the roles and responsibilities matrix from business units and other IRS stakeholders.
- Defined physical security roles and responsibilities.
- Prepared draft handbooks on the approved roles and responsibilities for executives, managers, technical employees, and users.
- Distributed draft handbooks to executives, managers, technical employees, and users.
- Carried out compliance assessments but omitted some functions from this process. The IRS deferred some compliance assessments due to organizational issues and time constraints. In addition, these compliance checks were mainly based on interviews with system administrators and security specialists and did not include any comprehensive testing.

Despite these actions, existing weaknesses in other computer security material weakness areas indicate that security roles and responsibilities have not been effectively

implemented. These weaknesses existed because responsible employees were not carrying out their duties as prescribed in the IRM or other guidance. Specifically, we found:

- Network administrators did not ensure routers were configured to established standards.
- System administrators did not correct known vulnerabilities on mainframe, UNIX, and Windows computer systems and did not install security patches to vulnerable UNIX and Windows computer systems, as required by established procedures.
- Contractors did not install security patches on the modernized security system.[8]
- Security specialists did not review audit trails on UNIX computer systems and modernized systems.[9]
- Business owners did not accredit their systems and did not complete annual self-assessments as required by the FISMA.[10]

Not carrying out these crucial responsibilities increases the likelihood that intruders or insiders could access unauthorized information or disrupt computer operations without detection. Until roles and responsibilities are effectively carried out, the IRS will have little chance of implementing effective security controls and computer security will remain a material weakness.

We believe the breakdowns in roles and responsibilities occurred because IRS employees are not being held accountable for carrying out their security responsibilities.

---

[8] The three issues caused by network administrators, system administrators, and contractors were presented in our audit report, *Network Access, System Access, and Software Configuration Should Remain Part of the Computer Security Material Weakness* (draft report issued August 17, 2004).

[9] The issue on audit trails caused by security specialists was presented in our audit report, *The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness* (Reference Number 2004-20-131, dated September 2004).

[10] The issue caused by business owners was presented in our audit report, *The Certification and Accreditation of Computer Systems Should Remain in the Computer Security Material Weakness* (Reference Number 2004-20-129, dated August 2004).

While the IRS has required all employees to complete annual UNAX[11] and computer security awareness briefings, it has not ensured specific security responsibilities have been adequately emphasized throughout the IRS, as required by the FISMA.

The other related audit reports on the IRS' computer security material weakness contain recommendations to address the specific breakdowns in security roles and responsibilities. Therefore, we are not repeating those recommendations in this report.

Recommendation

1. The Chief, Mission Assurance, should keep security roles and responsibilities as part of the computer security material weakness until corrective actions related to recommendations in our prior report[12] on security roles and responsibilities and in the aforementioned material weakness reports[13] have been addressed.

Management's Response: Management's response was due on September 27, 2004. As of September 28, 2004, management had not responded to the draft report.

Efforts on the Segregation of Duties Material Weakness Area Justify Closure

The Department of the Treasury requires bureaus to divide and separate duties and responsibilities of critical functions among different individuals to reduce the risk of fraudulent or criminal activity. Segregation of duties should prevent a single individual from being able to disrupt or corrupt a

[11] UNAX is synonymous with Unauthorized Access and refers to the security requirement that employees access taxpayer data only for official purposes. UNAX was established by the Taxpayer Browsing Protection Act, 26 U.S.C.A. §§ 7213, 7213A, 7431 (West Supp. 2003).
[12] *Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses* (Reference Number 2004-20-027, dated January 2004).
[13] *Network Access, System Access, and Software Configuration Should Remain Part of the Computer Security Material Weakness* (draft report issued August 17, 2004), *The Certification and Accreditation of Computer Systems Should Remain in the Computer Security Material Weakness* (Reference Number 2004-20-129, dated August 2004), and *The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness* (Reference Number 2004-20-131, dated September 2004).

critical security process without colluding with another employee. For example, system administrators should not be able to make unauthorized changes to computer configurations without colluding with security administrators responsible for detecting unauthorized changes to the configurations.

To address the segregation of duties material weakness area, the IRS planned and completed the following actions:

- Defined and finalized security roles and responsibilities, focusing on roles for system administration, security administration, management, and other related security functions.
- Documented and distributed procedures and guidelines that recognize the principle of segregation of duties by specifying the responsibilities of key employees with security duties.
- Implemented security roles and responsibilities relating to segregation of duties.

The procedures explaining segregation of duties for system administrators and security administrators were clear and the duties were separated to ensure there were no conflicting duties. The issues we identified in other reviews of computer security material weakness areas were not attributable to weaknesses in segregation of duties.

Recommendation

2. The Chief, Mission Assurance, has completed actions to correct weaknesses regarding segregation of duties and should remove this area from the computer security material weakness.

More Actions Are Needed Before the Security Training Material Weakness Area Is Downgraded

Department of the Treasury policy requires that employees and contractors with significant security responsibilities receive annual training specific to their security responsibilities. The level of training should be commensurate with each individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of IT systems security. The policy also requires bureaus to have a means

to track, by name and position, who has received what training and the costs of the training.

To address the security training material weakness area, the IRS planned to complete the following actions by December 31, 2003:

- Identify security-related training needs to correspond to defined security roles and responsibilities and establish a core curriculum for those positions.
- Identify employees with key security responsibilities.
- Validate and update current online and classroom courses for key personnel.
- Communicate training opportunities and guidance to key personnel on a periodic basis.
- Monitor curriculum course participation quarterly.

The IRS took the following actions in Calendar Year 2003 to address the security training material weakness:

- Identified available security training courses, matched courses to specific computer job positions, and developed a core curriculum for key security positions.
- Designated all Office of Mission Assurance employees as those employees who have significant computer security-related duties.
- Began development of the Enterprise Learning Management System (ELMS), which will integrate with the Department of the Treasury's human resources system (HR Connect) and help meet goals set by the OMB for E-Government[14] and E-Training initiatives.

[14] The President's Management Agenda established E-Government as the use of IT and the Internet, together with the operational processes and people needed to implement these technologies, to deliver services and programs to constituents, including citizens, businesses, and other government agencies. E-Government improves the effectiveness, efficiency, and quality of Federal Government services.

While the IRS initiated actions to address this material weakness area, several steps were not completed or were not effective. Specifically, the following steps need further improvement: identifying employees with key security responsibilities, effectively communicating the security core training curriculum and training courses, and periodically monitoring for course participation.

The Office of Mission Assurance did not identify all employees with significant computer security-related duties. The 288 employees identified as having key responsibilities all reported to the Chief, Mission Assurance. Employees with significant security duties assigned to the ITS organization (e.g., system administrators, computer specialists, and telecommunications specialists) were not included.

While the IRS developed a core curriculum that lists specific security classes for various IT positions, the curriculum and guidance for using the curriculum had not been effectively communicated to employees.

We interviewed 50 employees from 5 locations who had significant security responsibilities. Eleven of 15 employees from the Office of Mission Assurance and 24 of 35 employees from the ITS organization were not aware of the curriculum.

More importantly, employees were not receiving sufficient training. During the last 2 calendar years, 7 (1 from the Office of Mission Assurance and 6 from the ITS organization) of the 50 employees had only 1 training class, and 9 employees (1 from the Office of Mission Assurance and 8 from the ITS organization) had not received any security training.

To monitor course participation, the IRS is touting the ELMS as a tool to be used by all learners, managers, training administrators, and instructors. Until this system becomes fully operational, the IRS is using the Automated Corporate Education System (ACES) to track and monitor training classes.

However, information on the ACES is not reliable. We reviewed the ACES data for 33 employees at the 5 sites we visited and found that training records were incomplete for

11 employees. Recent training classes were not listed, including e-learning (online) classes.

Inadequate security training for IRS employees with key security responsibilities has been an ongoing problem. In January 2004, we reported that employees with key security responsibilities did not have sufficient training.[15] Eight of 29 system administrators we interviewed during that review did not receive sufficient training to perform their security-related duties. In addition, weak educational backgrounds in computer-related courses of some employees made the need for training even more critical. Twelve of the 29 system administrators had no formal computer-related education, and 2 of those did not have any computer experience prior to getting their current positions. These results also raised concerns about whether employees were fully qualified to perform their assigned responsibilities.

We attribute the inadequate security training to insufficient emphasis, particularly for those employees whose duties require them to implement security policies and procedures. In addition, the Office of Mission Assurance has not established a minimum number of security-related training hours, or a time period by which the key employees should obtain training, and did not clearly establish who was responsible or accountable for providing computer security-related training to the key employees.

We believe computer security training should remain as part of the computer security material weakness. Until employees with key security responsibilities are adequately trained, the IRS will have little chance of implementing effective security controls and computer security will remain a material weakness.

Recommendations

The Chief, Mission Assurance, should:

3. Keep the security training area as part of the computer security material weakness until all employees with key

[15] *Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses* (Reference Number 2004-20-027, dated January 2004).

security responsibilities, not just those in the Office of Mission Assurance, have been adequately trained.

4. Establish a process to identify employees with key security responsibilities, monitor their participation in training courses, and follow up with their managers, if necessary. In addition, the Chief, Mission Assurance, should consider requiring a minimum number of security training hours for all employees with key security responsibilities, to encourage enrollment in training classes.

The Chief Information Officer should:

5. Ensure his employees with key security responsibilities, particularly system administrators and security specialists, are adequately trained to perform security duties and tasks.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) has effectively resolved the vulnerabilities associated with its computer security material weakness. The IRS segregated this material weakness into nine areas,[1] three of which are addressed in this report: security roles and responsibilities, segregation of duties, and training.

I. To determine whether the IRS identified the significant vulnerabilities that need to be corrected before closing the weaknesses, we interviewed Office of Mission Assurance and Information Technology Services (ITS) organization staff and reviewed relevant IRS and Treasury Inspector General for Tax Administration documentation and reports on the IRS' approach to resolving the material weakness. We specifically followed up on our report on security roles and responsibilities.[2]

II. To determine whether the actions taken to resolve the specific vulnerabilities were sufficient to close the weaknesses, we interviewed IRS staff, reviewed documentation, conducted site visits of IRS validations and corrective actions, and evaluated the actions.

III. To determine whether the actions taken to resolve the vulnerabilities were fully implemented nationwide, we interviewed ITS organization staff and reviewed implementation schedules, coverage of implementation, and methodology behind the implementation.

IV. To determine the effectiveness of the IRS' actions to resolve the specific vulnerabilities, we interviewed 50 employees from the Mission Assurance and ITS organizations at 5 locations (the IRS Headquarters in New Carrollton, Maryland; the Brookhaven, New York , and Memphis, Tennessee, Campuses;[3] and the Martinsburg, West Virginia, and Memphis, Tennessee, Computing Centers[4]), reviewed documentation, and identified criteria for resolving the vulnerabilities. The sites visited were based on IRS offices with high numbers of mainframe systems, Unix-based servers, and Windows-based servers. The employees selected were based on available System

[1] The computer security material weakness consists of (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.

[2] *Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses* (Reference Number 2004-20-027, dated January 2004).

[3] IRS campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.

[4] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

Administrators and Security Specialists who had responsibility over the selected servers in our other material weakness reviews.

A. For the security roles and responsibilities area, we determined if:

1. Federal Information Security Management Act[5] (FISMA) reviews were effective.
2. Managers actively provided employees with security awareness training.
3. Managers reviewed and approved Automated Information System (AIS) User Registration/Change Requests (Form 5081) for system access privileges.
4. Weaknesses identified in other computer security material weakness reviews could be linked to employee rules of behavior and security roles and responsibilities.

B. For the segregation of duties area, we determined if the following roles were appropriately segregated:

1. Approving and installing system patches and upgrades.
2. Approving, adding, and removing users from systems.
3. Performing system administration, reviewing systems for security violations, and responding to security violations.
4. Any other key roles identified through the interview process.

C. For the training area, we determined if:

1. IRS managers had identified core skills for security personnel and employees were familiar with the core training curriculum for their positions.
2. The Office of Mission Assurance had identified specific security classes and schedules for security staff.
3. Continuing professional education requirements had been established, monitored, and met.
4. Security personnel received necessary and relevant training for 33 of the 50 employees where training information was available.
5. Training issues identified from our audit results on the FISMA[6] were addressed.

[5] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[6] *Performance Data for the Security Program Should Be Corrected* (Reference Number 2004-20-093, dated April 2004).

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Mary Jankowski, Senior Auditor
Louis Lee, Senior Auditor
Abraham B. Millado, Senior Auditor
Charles Ekholm, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Associate Chief Information Officer, Information Technology Services OS:CIO:I
Director, Assurance Programs OS:MA:AP
Director, Business Systems Development OS:CIO:I:B
Director, End User Equipment and Services OS:CIO:I:EU
Director, Enterprise Networks OS:CIO:I:EN
Director, Enterprise Operations Services OS:CIO:I:EO
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 Management Controls OS:CFO:AR:M
Audit Liaisons:
    Chief Information Officer OS:CIO
    Chief, Mission Assurance OS:MA