CHIEF
MISSION ASSURANCE

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

October 5, 2004

MEMORANDUM FOR ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Daniel Galik Daniel Galik
Chief, Mission Assurance and Security Services

SUBJECT: Response to Draft Audit Report – The Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness (Audit # 200420003)

This is in response to the draft report entitled "The Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness." We appreciate that you acknowledged the key steps taken by the IRS to address security roles and responsibilities, segregation of duties, and training. We are attaching a detailed response to each of the five report recommendations.

Security roles and responsibilities are an important part of the IRS' Security Program. The IRS has defined roles and responsibilities and distributed draft handbooks on the approved roles and responsibilities for executives, managers, technical employees, and users. We concur that the vulnerability in this area is in the implementation of the roles and responsibilities in accordance with the IRM and other guidance. As a result, in response to recommendation #1, we will reopen the security roles and responsibilities issue under the computer security material weakness.

As discussed in the report, the IRS has made substantial progress in resolving the segregation of duties issue such as defining and finalizing security roles and responsibilities and implementing them relating to segregation of duties. In addition to these activities, the IRS has two other efforts that impact this issue. Specifically, these efforts are the expedited Tier 2 consolidation effort and the goal to remove most of the unconsolidated UNIX servers by the end of calendar year 2004. These efforts coupled together will also substantially resolve the segregation of duties issue because audit trail reviews will be conducted using the capabilities in the consolidated UNIX platforms. Since these efforts are in process, in response to recommendation #2, we have determined that we will keep the segregation of duties issue open and continue to monitor it through compliance assessments until May 2005. The additional time allows the IRS to develop specialized scripts and guidance to support audit trail reviews for the approximately 27 unconsolidated UNIX servers that would remain. Moreover, we will track this issue in a multi-functional working group through the end of FY 2005.

Also, we concur with report recommendations #3 through #5 that address technical security-related training of key personnel. The IRS will reopen the issue under the computer security material weakness. Corrective actions are initiated to identify employees with key information technology (IT) security responsibilities that are in the Business Units, and outside Mission Assurance and Security Services, and to track their training as well. We will also identify the appropriate courses for employees with key IT security responsibilities and include these requirements in the security curriculum. Additionally, corrective actions are underway to enhance efforts to deliver training and ensure that employees with key security responsibilities are adequately trained.

If you have any questions, please contact me at (202) 622-8910 or Ellen Pieklo, Acting Director, Certification Testing, Evaluation, and Assessment at (585) 262-1185.

Attachment

Management response to Draft Audit Report –Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness (Audit # 200420003)

RECOMMENDATION # 1: The Chief, Mission Assurance and Security Services (MA&SS) should keep security roles and responsibilities as part of the computer security material weakness until corrective actions related to recommendations in our prior report on security roles and responsibilities and in the aforementioned material weakness reports have been addressed.

CORRECTIVE ACTION TO RECOMMENDATION #1: IRS concurs with the recommendation. MA&SS will reopen the security roles and responsibilities issue under the computer security material weakness. For FY2005, MA&SS is integrating mitigation of material weaknesses into the program plans. All reported non-compliance issues or security vulnerabilities will be included in a detailed Plan of Action and Milestones (POA&Ms). This will include all findings reported in previous TIGTA audits. These POA&Ms will be tracked within the FISMA reporting process and will be reviewed both monthly and quarterly. In addition, MA&SS is establishing a multi-functional working group to address material weakness issues. The working group will be composed of representatives from Modernization and Information Technology Systems, Criminal Investigation, Chief Counsel, and Appeals to address and resolve security related vulnerabilities. The group will identify executive owners of the vulnerabilities to ensure implementation of recommendations issued by the working group.

IMPLEMENTATION DATE: September 30, 2005

RESPONSIBLE OFFICIAL: Director, Assurance Programs, Mission Assurance and Security Services

CORRECTIVE ACTION MONITORING PLAN: Corrective actions will be monitored using the detailed POA&Ms used in the FISMA process and will be reported by the material weakness working group.

Management response to Draft Audit Report – Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness (Audit # 200420003)

RECOMMENDATION # 2: The Chief, Mission Assurance and Security Services (MA&SS) has completed actions to correct weaknesses regarding segregation of duties and should remove this area from the computer security material weakness.

CORRECTIVE ACTION TO RECOMMENDATION #2: As the audit report acknowledges, the IRS has made substantial progress in resolving the segregation of duties issue such as defining and finalizing security roles and responsibilities and implementing them relating to segregation of duties. Additionally, the IRS expedited Tier 2 consolidation effort, coupled with the goal to remove most of the unconsolidated UNIX servers by the end of calendar year 2004, have also substantially resolved the segregation of duties issue. Considering that these efforts are in process, MA&SS has determined that it will retain the issue as open and continue to monitor it through compliance assessments until May 2005. The additional time allows the IRS to develop specialized scripts and guidance to support audit trail reviews for the approximately 27 unconsolidated UNIX servers that remain.

Moreover, for FY2005, MA&SS is integrating mitigation of material weaknesses into the program plans. All reported non-compliance issues or security vulnerabilities will be included in detailed POA&Ms. This will include all findings reported in previous TIGTA audits, regardless of whether they are considered to be material weaknesses. These POA&Ms will be tracked within the FISMA reporting process and will be reviewed both monthly and quarterly. In addition, MA&SS is establishing a multi-functional working group to address material weakness issues. The working group will be composed of representatives from Modernization and Information Technology Systems, Criminal Investigation, Chief Counsel, and Appeals to address and resolve security related vulnerabilities. The group will identify executive owners of the vulnerabilities to ensure implementation of recommendations issued by the working group.

IMPLEMENTATION DATE: September 30, 2005

RESPONSIBLE OFFICIAL: Director, Assurance Programs, Mission Assurance & Security Services

CORRECTIVE ACTION MONITORING PLAN: Corrective actions will be monitored using the detailed POA&Ms used in the FISMA process and will be reported by the material weakness working group

Management response to Draft Audit Report — Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness (Audit # 200420003)

RECOMMENDATION # 3: The Chief, Mission Assurance and Security Services (MA&SS) should keep the security training area as part of the computer security material weakness until all employees with key security responsibilities, not just those in MA&SS, have been adequately trained.

CORRECTIVE ACTION TO RECOMMENDATION #3:

MA&SS concurs that security training of all employees with key security responsibilities continues to be an area of concern. MA&SS will reopen the issue for security-related training to key personnel under the computer security material weakness. Actions have been completed or are underway to address this issue. Please see the response to Recommendation #4 for detailed corrective actions.

IMPLEMENTATION DATE:

October 15, 2005

RESPONSIBLE OFFICIAL:

Director, Assurance Programs, Mission Assurance & Security Services

CORRECTIVE ACTION MONITORING PLAN: Corrective actions will be monitored in the MA&SS FY 2005 Program Plan for Training.

Management response to Draft Report Audit---Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness (Audit # 200420003)

RECOMMENDATION # 4: The Chief, Mission Assurance and Security Services (MA&SS) should 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, MA&SS, should consider requiring a minimum number of security training hours for all employees with key security responsibilities to encourage enrollment in training classes.

CORRECTIVE ACTION TO RECOMMENDATION #4:

The IRS concurs with this recommendation. MA&SS employees with key information technology (IT) security responsibilities have been identified, and actions have been initiated to identify employees with key IT security responsibilities in the Business Units. Training for these employees will be identified, defined, and tracked in partnership with IRS Learning and Education. In lieu of the IRS requiring a number of security training hours for employees with key IT security responsibilities, we will identify the appropriate courses and include these requirements in the security curriculum. The following activities will be addressed and completed by October 15, 2005.

1. Identify employees in the Business Units with key IT security responsibilities.
2. Convene the MA&SS Training Council to identify the appropriate security training courses for employees with significant IT security responsibilities.
3. Begin quarterly monitoring of training for employees with key IT security responsibilities.
4. Validate and update current IT security curriculum.
5. Prepare Communications Plan for periodic communication of training opportunities and guidance to key personnel.
6. Include IT security training in Program Reviews to determine/ensure manager compliance with security policy regarding security training of employees.

IMPLEMENTATION DATE:

October 15, 2005

RESPONSIBLE OFFICIAL: Director, Assurance Programs, Mission Assurance & Security Services

CORRECTIVE ACTION MONITORING PLAN: Corrective actions will be monitored in the MA&SS FY 2005 Program Plan for Training.

Management response to Draft Audit Report — Computer Security Roles and Responsibilities and Training Should Remain Part of the Computer Security Material Weakness (Audit # 200420003)

RECOMMENDATION # 5: The Chief Information Officer (CIO) should ensure that his employees with key responsibilities, particularly system administrators and security specialists, are adequately trained to perform security duties and tasks.

CORRECTIVE ACTION TO RECOMMENDATION #5:

The CIO and Chief Mission Assurance & Security Services (MA&SS) together have initiated a pilot program which offers access to security e-learning appropriate to key responsibilities of system administrators and security specialists. In this one year pilot selected system administrators and security specialists are given access to relevant courses. A record of courses completed and regular progress reports are available through this program.

A) The Chief, MA&SS will send periodic status reports to the CIO identifying which employees have completed courses and which have not.
B) The CIO will use periodic status reports provided by MA&SS to track whether assigned employees have completed the courses to ensure adequate training to perform security duties and tasks.
C) Following the completion of the one-year pilot program, the CIO and Chief, MA&SS will jointly decide on the effectiveness of this training vehicle and determine future training for system administrators and security specialists.

IMPLEMENTATION DATE:

A) June 30, 2005
B) October 31, 2005
C) December 15, 2005

RESPONSIBLE OFFICIAL:

A) Chief Mission Assurance & Security Services
B) Chief Information Officer
C) Chief Mission Assurance & Security Services

CORRECTIVE ACTION MONITORING PLAN:

Corrective actions will be monitored in the MA&SS FY 2005 Program Plan for Training.