Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses

January 2004

Reference Number: 2004-20-027

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

January 14, 2004

MEMORANDUM FOR CHIEF, MISSION ASSURANCE

Gordon C. Milbourn III

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

SUBJECT: Final Audit Report – Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses (Audit # 200320006)

This report presents the results of our review of roles and responsibilities of employees with key security duties. The overall objectives of this review were to determine whether the roles and responsibilities of key Internal Revenue Service (IRS) security employees were implemented consistently, and whether the employees had the requisite training, formal education, and experience needed to carry out their responsibilities.

System administrators and security specialists have day-to-day responsibility for ensuring that the computer systems are set up and maintained in a secure manner. Our previous audits,[1] as well as a General Accounting Office review,[2] have identified security vulnerabilities that indicated these duties have not always been effectively performed. We performed this audit to assess how well security responsibilities were carried out on a broader scale.

In summary, our review of local servers and workstations at five locations again identified significant security vulnerabilities. Vendor patches were not applied to hardware and software to ensure known vulnerabilities were adequately mitigated, configuration baselines were not maintained in order to identify unauthorized changes,

---

[1] *The Security of the Integrated Collection System Needs to Be Strengthened* (Reference Number 2003-20-119, dated May 2003), *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2003-20-082, dated March 2003), *Many Advances Made But Additional Emphasis Is Needed on Key Initiatives in the Security Service Organization* (Reference Number 2003-20-005, dated October 2002), and *Computer Security Controls Should Be Strengthened in the Former Northern California District* (Reference Number 2001-20-036, dated January 2001).
[2] *Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks* (GAO-03-44, dated May 2003).

audit trails and event logs were not generated and reviewed, employees were given access to computer systems although there was no record of managerial approval, and user accounts were not deleted when employees separated.

A major underlying cause for these conditions was that accountability for carrying out key security responsibilities was not maintained. Interviews of IRS employees identified widespread confusion in this area. We also identified instances in which duties were not performed or not properly separated and, in some instances, duties were duplicated.

Also, employees with key security responsibilities did not have sufficient training. A significant percentage of employees believe that they had not received sufficient training to adequately perform their security-related duties. The training they received was not always helpful because it was too general, not timely, or not work-related. Some employees had not received any security training in the past 3 years.

The IRS has designated computer security a material weakness, as required by the Federal Managers' Financial Integrity Act of 1982.[3] To correct this material weakness, the IRS has developed a plan that it expects to implement by March 31, 2004. The plan contains action items that address both the security roles and responsibilities issue, and the security training issue. We plan to evaluate the effectiveness of these actions after they have been fully implemented.

We recommended that the Chief, Mission Assurance, develop a methodology to evaluate system administrators' and security specialists' performance of their roles and responsibilities with respect to security requirements. We also suggested conducting periodic computer scans that will identify potential vulnerabilities. The results can be used to evaluate how well the employees are maintaining security on computers under their ownership. We also recommended that the Chief, Mission Assurance, take certain actions to ensure appropriate security training for key security personnel.

Management's Response: The Chief, Mission Assurance, concurred with our recommendations. Mission Assurance is developing a methodology to evaluate system administrators' and security specialists' role and responsibilities, which will be accomplished in two steps. Step one addresses training of system administrators and security specialists, and step two addresses evaluating the performance of those employees. In addition, it has identified employees with key security responsibilities. For those employees, skill sets and appropriate security curriculum will be determined, and a policy statement on assessing skill sets and security training will be issued. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers who are 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.

---

[3] 31 U.S.C. §§ 1105, 1113, and 3512 (2000).

Table of Contents

Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses

Background

In the Internal Revenue Service (IRS), technical computer security responsibilities are assigned to system administrators and security specialists.[1] Generally, system administrators are responsible for day-to-day systems operations and security specialists are responsible for specific security tasks and security oversight. Both positions are needed to ensure proper segregation of duties, similar to a system of checks and balances. For example, system administrators can make changes to computer configurations and settings, while security specialists review audit trails to identify unauthorized accesses and changes to the configurations.

The Internal Revenue Manual (IRM) defines roles and responsibilities for system administrators and security specialists. The IRS' Information Technology Services Office has the responsibility of implementing security duties for the system administrators and security specialists, while the Office of Security Services provides oversight and guidance when needed.

In several of our prior audits,[2] as well as a General Accounting Office (GAO) review[3] of the IRS, not having clear roles and responsibilities and inadequate training for employees with key security responsibilities have been cited as the causes of many security vulnerabilities identified. Those audits were conducted on individual applications or

---

[1] We focused this review on system administrators' and security specialists' responsibilities. While these positions are responsible for most of the computer security tasks in the IRS, they are not the only positions. Other positions, such as telecommunications analysts and database administrators, also have important computer security responsibilities.

[2] *The Security of the Integrated Collection System Needs to Be Strengthened* (Reference Number 2003-20-119, dated May 2003), *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2003-20-082, dated March 2003), *Many Advances Made But Additional Emphasis Is Needed on Key Initiatives in the Security Service Organization* (Reference Number 2003-20-005, dated October 2002), and *Computer Security Controls Should Be Strengthened in the Former Northern California District* (Reference Number 2001-20-036, dated January 2001).

[3] *Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks* (GAO-03-44, dated May 2003).

operating systems and, consequently, we limited our assessments to local concerns. We performed this audit to evaluate these two issues on a broader scale.

This audit was conducted in the Los Angeles, California, and Oklahoma City, Oklahoma, area offices, a Washington, D.C., satellite office, and the Atlanta, Georgia, and Brookhaven, New York, Campuses[4] from December 2002 to June 2003. The employees we interviewed in these offices were responsible for the operation of several diverse systems and applications. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Key Security Employees Did Not Always Perform Their Responsibilities

IRS employees' workstations are usually connected to sensitive data on local network servers as well as on larger computers maintained in IRS computing centers[5] and campuses. Because of the trusted relationship between user workstations and other servers on the network, a high degree of security must be maintained over these computer systems to prevent improper disclosure of taxpayer data, attacks by malicious employees and hackers, and disruption of operations. To provide an adequate level of security, controls must be in place on each of the interconnected workstations as well as the servers.

In November 2001, the IRS began implementing a Common Operating Environment (COE) for all Windows-based workstations. The COE provides a set of applications and security standards and adequately addresses the most common security vulnerabilities associated with workstations. Currently, a majority of all Windows-based workstations have been updated with the COE.

[4] The campuses are the data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.

[5] IRS computing centers support tax processing and information management through a data processing and telecommunications infrastructure.

We purposely selected sites where the COE had been implemented because the COE represents the future of the IRS workstations nationwide, and we wanted to evaluate whether system administrators were maintaining adequate security controls after implementation. All workstations at the sites we visited contained the COE configuration and were adequately secured.

However, we identified several vulnerabilities on the network servers at the sites we visited. A COE type of implementation is not feasible for servers because they have specific functionalities and require different configurations to operate. Instead, the IRS relies upon system administrators for proper configurations.

We identified the following vulnerabilities that are consistent with findings reported in prior reports. We believe these problems are persistent and will remain until security roles and responsibilities are effectively carried out and employees are adequately trained and held accountable.

- Ten of 20 servers had at least 1 of the System Administration, Audit, Network Security (SANS) Institute/Federal Bureau of Investigation (FBI) Top 20 security vulnerabilities[6] that could have been resolved with current patches from the vendors. We consider these to be high-risk vulnerabilities.
- Eight of 12 system administrators were not aware of, or did not maintain or document, configuration baselines for systems under their control. Consequently, they could not compare current configurations against the baseline to identify unauthorized changes.
- Ten of 14 system administrators and security specialists did not generate or review audit trails or

[6] The SANS Institute was established in 1989 as a research and education organization for government and private industry security. The SANS Institute, along with the FBI, periodically announces the list of top 20 computer security vulnerabilities, based on security incidents recently reported.

event logs to identify questionable activities on the network.

- Forty-one (39 percent) of 106 Information Systems User Registration/Change Request forms (Form 5081) were not available for our review. These forms are used to grant employees access to the network and applications. As such, IRS employees may have been given access to computer systems without managerial approval or a proper need to know.
- Twenty-eight (14 percent) of 206 user accounts were still active although the employees had been separated from the IRS an average of 139 days. One of these accounts had two suspicious accesses after the employee had separated. The former employee or another employee who knew the account's password may have made the accesses to the network. These accesses have been referred to the Office of Investigations for further analysis. None of the other 27 user accounts had accesses after the employees separated.

These vulnerabilities can have a significant adverse effect on the overall security of information systems. When patches are not applied, computer components remain vulnerable to compromise. Not having audit trails may permit questionable system accesses and activities to go undetected. Employees given access to computer systems without proper approval or background investigations may misuse taxpayer data. In addition, user accounts of separated employees that are still active may be improperly used to gain access to systems and data.

We attribute these vulnerabilities, in part, to inadequate accountability for security responsibilities and security training for key employees (i.e., system administrators and security specialists).

Key security employees were not accountable for carrying out their responsibilities

The lists of responsibilities for both system administrators and security specialists were specified in the IRM in

January 2002. These responsibilities, if carried out, would have eliminated or at least reduced the vulnerabilities we continue to identify.

For example, system administrator duties include: maintaining an up-to-date listing of current system users and at least annually distributing a list of users and their access profiles to appropriate managers for review, update, and certification; ensuring proper acquisition, installation, testing, protection, and use of system software; and maintaining current documentation that properly defines the technical hardware and software configuration of system and network connections.

Security specialist duties include: ensuring user access is restricted to the minimum necessary to perform his/her duties; monitoring system integrity, protection levels, and security related events; and generating audit trails and security reports and distributing them to the appropriate managers for review.

While these key security procedures were adequately defined, the vulnerabilities we identified and our interviews of system administrators and security specialists in five offices indicate widespread confusion on key security procedures. Even some managers of key security employees were not clear about their own responsibilities and their employees' security related duties.

Our interviews with 29 system administrators and security specialists identified the following examples that demonstrate confusion over responsibilities. Managers did not actively monitor performance of these responsibilities.

- Five employees were confused over who had responsibility for maintaining Windows workstations and servers, as well as applying and testing computer patches.
- Four employees still retained their previous system administrator rights when their new position no longer required this access privilege.

- Three employees were performing both system administrator and security specialist duties on the same system.
- One employee did not know whether the users on the server were authorized users.
- Five employees were performing duties from their previous position, while adding their new security duties.
- Two employees in one office were assigned the same duties of identifying separated employees, yet neither performed this responsibility.

The IRS has designated computer security as a material weakness, as required by the Federal Managers' Financial Integrity Act of 1982.[7] Security roles and responsibilities have been categorized as a subset of this material weakness, and the IRS has developed a plan for resolving this material weakness by March 31, 2004. The plan identifies (1) corrective actions, (2) the agency organization responsible for correcting each type of weakness, (3) key milestones with completion dates, and (4) the status of actions.

The IRS' material weakness plan contains action items designed to appropriately delineate security roles and responsibilities within functional business, operating, and program units and to appropriately segregate system administration and security administration responsibilities. This plan also lists actions to be taken to optimally configure system software to ensure the security and integrity of system programs, files, and data, including development of the process to publish and deploy operating system patches. Many of these actions are pending. We plan to conduct an in-depth analysis of the material weakness plan and validate the results in other reviews.

The plan, however, does not address how Modernization and Information Technology Services managers and employees are going to be held accountable for carrying out

[7] 31 U.S.C. §§ 1105, 1113, and 3512 (2000).

security roles. The National Aeronautics and Space Administration (NASA), for example, has placed responsibility for technical security controls on system administrators and periodically runs computer scans to identify vulnerabilities. System administrators are then evaluated on the number of vulnerabilities reported per workstation. While this approach should not be the only means to evaluate system administrators, it clearly gives managers an indication of potential issues that may need attention and shows administrators how they are doing in relation to others in their agency.

Employees with key security responsibilities did not have sufficient training

When we began our audit work, we asked security officials to identify the IRS employees with key security responsibilities so we could evaluate the training provided IRS-wide. Because the IRS was not able to identify employees with key security responsibilities, we limited our testing to those employees in the offices we reviewed.

The IRS' training database contained accurate training histories for the employees included in our test. However, 8 of the 29 system administrators, security specialists, and customer support personnel we interviewed did not receive sufficient training to perform their related duties. Six of the 8 personnel had not received any security training in the past 3 years. Recommended courses for these positions include: Norton Anti-Virus for Administrators, Microcomputer Security - Windows NT, Voice and Data Security, Securing Communications and Networks, and Internet and System Security.

Twelve of the 29 employees stated that they had not received sufficient training to adequately perform their duties. They believe the training they had received was not always helpful because it was too general, not timely, or not sufficiently work-related.

In addition to training, we evaluated the formal education and experience of employees that we interviewed. The interviews showed that 5 of the 29 employees had received a computer-related college degree. An additional

12 employees had taken college computer-related courses, most of which were taken prior to the employees getting their current positions. The remaining 12 employees had no formal computer-related education, and 2 of those did not have any computer experience prior to getting their current positions. Not having computer-related education and experience may indicate that some employees in the field are not fully qualified to perform their assigned responsibilities.

The National Institute of Standards and Technology (NIST) and the GAO recommend that computer security training should be role-based. Role-based learning focuses on the job functions employees perform rather than on their job titles. In particular, it provides security training that satisfies the specific requirements of an employee's role. The NIST and the GAO also recommend that methods should be employed for determining whether employees have learned and retained what they have been taught and whether their performance has improved.

The IRS has also designated security training as a subset to the computer security material weakness. The IRS' material weakness plan provides steps to deliver sufficient technical security-related training to key personnel. The plan includes steps to identify security-related training needs for employees based on their roles and responsibilities and to update current online and classroom courses for key personnel. These actions are still in process.

Subsequent to the start of this audit, the IRS identified 288 employees with significant computer security responsibilities, based on the criteria that 25 percent of their time is spent on computer security activities. We disagree with this methodology because other employees have important computer security responsibilities even though those responsibilities do not consume 25 percent of their time. These employees include system administrators, telecommunications analysts, and database administrators.

Recommendations

The Chief, Mission Assurance, should:

1. Develop a methodology to evaluate system administrators' and security specialists' performance of their roles and responsibilities. We encourage the Chief, Mission Assurance, to consider methodologies similar to those used by the NASA that provide quantifiable results and suggest conducting periodic computer scans that will identify vulnerabilities. The results can be used to evaluate how well the employees are maintaining security on computers under their stewardship.

Management's Response: Mission Assurance management plans to develop a methodology to evaluate system administrators' and security specialists' roles and responsibilities in a two-step process. Step one involves linking training to position descriptions and developing related training courses that address current technology and policies. Step two involves developing a strategic planning document that identifies implementation schedules and milestones for evaluating employee performance.

2. Ensure the current effort to identify security training needs will result in appropriate security training for employees with key security duties by:

    - Identifying employees in all offices with key roles and responsibilities.
    - Establishing Knowledge, Skills, and Abilities (KSA) standards for key personnel.
    - Assessing the KSAs of key personnel.
    - Allocating sufficient funds to ensure key personnel are recruited and trained.

Management's Response: Mission Assurance management has identified employees with key security responsibilities and has moved qualified individuals into security positions. For these employees, they plan to identify skill sets and appropriate training, and issue a policy statement on assessing those skill sets and security training.

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objectives of this review were to determine whether the roles and responsibilities of key Internal Revenue Service (IRS) security employees were implemented consistently, and whether these employees had the requisite training, formal education, and experience needed to carry out their responsibilities.

I. To evaluate the adequacy of policies and guidelines that had been developed to ensure Windows computer systems were installed and maintained in a secure manner, the administrators were properly trained in their jobs, and there was appropriate separation of duties, we:

   A. Reviewed guidance documents from Federal Government sources (e.g., Internal Revenue Manual, Treasury Directives, and the National Institute of Standards and Technology) and computer industry sources (e.g., the System Administration, Audit, Network Security Institute[1]).

   B. Interviewed End User Equipment and Services (EUES) management to determine the roles of the system administrators and security specialists and how they differed, and determine the roles of the EUES organization for ensuring adequate Local Area Network (LAN) security. Also, we determined what training was available, and what other guidelines or policies had been established to assist the administrators and specialists.

   C. Evaluated the system administrators' and security specialists' roles and responsibilities to determine whether duties were adequately separated.

II. To determine whether security roles and responsibilities were effectively carried out, we selected 5 sites that employed the IRS' Common Operating Environment and interviewed 29 system administrators, security specialists, and customer support personnel available during our on-site visit. At these sites, we:

   A. Used the Internet Security Scanner software and scanned a total of 90 workstations and 20 servers to identify security threats to the systems.

   B. Evaluated controls used by either the system administrator or security specialist to ensure users had a business need to access the LAN and were authorized to access it. Also, we identified recent employee departures to determine if their LAN access was still active.

[1] The System Administration, Audit, Network Security Institute was established in 1989 as a research and education organization for government and private industry security.

C. Determined whether the system administrators or security specialists ran system logs and audit trails for the network, and whether the logs and audit trails were reviewed for inappropriate accesses.

D. Interviewed the system administrators and security specialists to determine what functions they perform, the level of training they had received, and the accuracy of the IRS' training database.

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
Louis Lee, Senior Auditor
Bill Lessa, Senior Auditor
Abraham Millado, Senior Auditor
Joan Raniolo, Senior Auditor
Larry Reimer, Senior Auditor
Stasha Smith, Senior Auditor
Charles Ekholm, Auditor
Suzanne Noland, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Director, End User Equipment & Services OS:CIO:I:EU
Director, Enterprise Operations OS:CIO:I:EO
Acting Director, Portfolio Management OS:CIO:R:PM
Acting Director, Regulatory Compliance OS:MA:RC
Acting Director, Strategy, Program Management, and Personnel Security OS:MA:SP
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 Liaison: Chief, Mission Assurance OS:MA

Appendix IV

Management's Response to the Draft Report

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

RECEIVED
JAN 05 2004

December 29, 2003

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR
TAX ADMINISTRATION

FROM: Daniel Galik
Chief, Mission Assurance

SUBJECT: Response to Draft Audit Report – Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses (Audit # 200320006)

We have reviewed the audit report entitled "Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses" and concur with both report recommendations. Your recommendations are consistent with continuing IRS efforts to achieve an enhanced security program that effectively manages risks. This is demonstrated in our accomplishments for correcting computer security material weakness items, and reflected in our detailed response to this draft report. In addition, we have determined that both recommendations are the responsibility of the Chief, Mission Assurance, as reflected in our attached corrective action response. Please adjust your tracking to reflect the change in the first recommendation from the Chief Information Officer to the Chief, Mission Assurance.

We would also like to take this opportunity to update the status of your finding on page 4 of the draft report relating to active user accounts of separated employees. Since the time of the audit, the IRS' Online 5081 application has installed an enhancement that addresses this issue. The Online 5081, which controls and records user access to IRS systems and applications, receives daily data updates from the TAPS personnel system. Through that link, a separation personnel action triggers Online 5081 to send an e-mail notification to each system administrator of the applications to which the user had been granted access. A courtesy notification is also sent to the manager of record in the event that a TAPS personnel action was generated in error. Ongoing activities are underway to improve automated notification relating to contractor employees. Each of these improvements further strengthens the IRS' computer security.

If you have any questions, please call me at (202) 622-8910 or Colleen Murphy, Director, Assurance Programs at (202) 283-4500.

Attachment

Management Response to Draft Audit Report – The Inadequate Accountability and Training for Key Security Employees Contributed to Significant Computer Security Weaknesses (Audit #200320006)

RECOMMENDATION # 1: The Chief Information Officer (CIO) should: Develop a methodology to evaluate system administrators' and security specialists' performance of their roles and responsibilities. We encourage the CIO to consider methodologies similar to those used by the NASA that provide quantifiable results and suggest conducting periodic computer scans that will identify vulnerabilities. The results can be used to evaluate how well the employees are maintaining security on computers under their stewardship.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The Chief, Mission Assurance will take responsibility for this recommendation. Mission Assurance (MA) concurs that performing scans is an effective tool for identifying vulnerabilities. We already perform scans and through heightened computer security awareness these efforts were increased. We will consider the NASA methodologies identified by TIGTA as we manage this program.

To date, MA has completed the training curriculum for security personnel. Early in FY2003, Security Services, which recently merged into the newly established Mission Assurance organization, completed a review of the security training curriculum with the assistance of the Hay Group. The curriculum identifies courses by security disciplines, and is contained in the Learning & Education's (L&E) training catalog. The courses also appear in the Administrative Corporate Education System (ACES).

Also, to address this recommendation, MA is developing a methodology to evaluate system administrators' and security specialists' roles and responsibilities. The methodology will be accomplished in a two-step process and includes the following detailed activities:

- Step One - Training:
  - Conduct training needs assessment linking courses to standardized position descriptions (SPDs).
  - Coordinate with the Human Capital Office to ensure that security training courses are developed or procured to coincide with key security roles and responsibilities.
  - Ensure that courses address current technology and policies applicable to physical, personnel, and information security.

- Step Two - Evaluation:
  - Develop a strategic planning document that identifies the implementation activities and milestones necessary to establish a Mission Assurance National Training, Test, and Exercise (TT&E) Program that will evaluate systems administrators' and security specialists' performance.

PROPOSED IMPLEMENTATION DATE:
Step One - Training – July 2004
Step Two – Evaluation – August 2004

RESPONSIBLE OFFICIAL:
Director, Assurance Programs

CORRECTIVE ACTION MONITORING PLAN:
Not applicable

RECOMMENDATION # 2: The Chief, Mission Assurance should: Ensure the current effort to identify security training needs will result in appropriate security training for employees with key security duties by:

- Identifying employees in all offices with key roles and responsibilities.
- Establishing Knowledge, Skills, and Abilities (KSA) standards for key personnel.
- Assessing the KSAs of key personnel.
- Allocating sufficient funds to ensure key personnel are recruited and trained.

CORRECTIVE ACTION TO RECOMMENDATION #2:

Mission Assurance concurs with the recommendation. Actions are either completed or are underway to address these issues. Specifically,

2a) During the October 2004 standup activities of the newly established Mission Assurance organization, key security personnel were identified. The roles and responsibilities of the key security personnel played an integral part in the standup.

2b) The skill sets needed for information technology professionals was assessed for MA who were formerly with the End User Equipment and Services' (EUES) Data Security organization of MITS. For those staff, IRS has applied the security curriculum to the Training and Education Resource Management System (TERMS) database and determined the course of studies for the various security specialties, linking particular courses to specific standardized position descriptions (SPDs). Ongoing reviews within the Data Security environment (at least quarterly) ensure the appropriateness of the applied curriculum. At least annually, the security managers review the applied curriculum for each of their employees.

2c) To assess the Knowledge, Skills, and Abilities (KSAs) of key personnel, Mission Assurance will issue a policy statement endorsing Training and Education Resource Management System (TERMS) and its successor as the formal repository for security training data and will extend its use throughout the remainder of Mission Assurance in the third quarter, April 2004.

2d) During the Mission Assurance standup; qualified key security personnel were moved into the organization. Until new processes can be developed, recruitment of new personnel will be severely limited. Funding for recruiting personnel must be found through savings in the current program. The training of key security personnel is addressed in our response to recommendation #1. No further action will be taken on this part of recommendation #2.

IMPLEMENTATION DATE:

2a) Completed – October 1, 2004
2b) September 30, 2004
2c) April 1, 2004
2d) December 31, 2004

RESPONSIBLE OFFICIAL:

2a) Director, Assurance Program
2b) Director, Assurance Program
2c) Director, Assurance Program
2d) Director, Assurance Program

CORRECTIVE ACTION MONITORING PLAN:

Mission Assurance will develop a tool to track training taken, training needed, and training costs for any business case development to justify funding by a business unit.