The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

September 2004

Reference Number: 2004-20-131

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.

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 13, 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 - The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness (Audit # 200420004)

This report presents the results of our review of the effectiveness of the Internal Revenue Service's (IRS) actions to resolve vulnerabilities associated with its computer security material weakness. The IRS has segregated this material weakness into nine areas, one of which covers the monitoring of key networks and systems, commonly referred to as audit trails. 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 report is from one of five reviews conducted this fiscal year to meet the request.

In summary, the Department of the Treasury requires that computer systems and networks that process sensitive data maintain an audit trail of user events to detect unauthorized actions. The IRS has taken some key steps toward resolving the audit trails material weakness. Specifically, the Office of Mission Assurance has developed an enterprise-wide audit trail strategy to ensure reviews of audit trail information are conducted on a routine basis. In addition, it has developed overall standards for audit trails and coordinated with key Information Technology Service organizations to draft and implement procedures for reviewing audit trails of various operating system platforms.

The IRS carried out its strategy for addressing audit trail concerns on its mainframe and Windows-based computers. Actions were successful in resolving the audit trails material weaknesses on those operating systems. However, audit trails are not being run on the UNIX-based computers because software procured to help analyze the voluminous audit trail data still is not working as intended. Audit trails are usually large files that can be extremely difficult to analyze manually. The use of automated software to analyze these data is likely to be the difference between unused audit trail data and a robust program.

The IRS strategy to address audit trails did not include three issues we believe are critical. Specifically:

- Some UNIX servers cannot generate audit trails without impairment to the servers' performance. The IRS has acknowledged this deficiency but cannot resolve it until the applications on these servers have been migrated to another platform.
- Audit trails on applications have not been addressed. Audit trails are reviewed on very few applications in the IRS, with the most notable being the Integrated Data Retrieval System (IDRS)[1] application.
- The IRS' modernized system to collect and generate useful audit trail reports was not working as intended. While the Security Audit and Analysis System (SAAS) was collecting and storing audit trail data, it did not have adequate functionality and software performance to support any queries. Also, operating procedures for this System have not been developed.

Overall, the IRS' strategy to address audit trails was aimed at the root causes that have plagued the IRS for years (not having computer capacity, automated reporting software needed to help analyze the vast amount of audit trail information, accountability and staffing to carry out audit trail review responsibilities, and sufficient guidelines to assist in conducting audit trail reviews). While significant progress has been made in implementing this strategy, problems still exist. Additional effort is needed to ensure audit trails are run and monitored on the UNIX-based computers, existing applications, and modernized applications before the audit trails material weakness area is downgraded.

We recommended the Chief, Mission Assurance, continue reporting audit trails as part of the computer security material weakness until audit trails are routinely reviewed for UNIX-based computers, a reasonable approach is developed and implemented for reviewing audit trails of applications in addition to the operating systems, and audit trails are functioning for the modernized applications and operating systems. We also recommended the Chief Information Officer (CIO) continue with updating and implementing the audit trail solution for UNIX-based computers, ensure audit trails are being regularly generated and reviewed, and coordinate with the Office of Mission Assurance to develop and implement a reasonable approach for reviewing audit trails on major applications.

[1] The Integrated Data Retrieval System enables employees to have instantaneous visual access to certain taxpayer accounts. The system can be used to research accounts, enter transactions or collection information, or generate notices and other documents.

Management's Response: The Chief, Mission Assurance, partially concurred with our recommendations, specifically that the IRS will continue to ensure effective implementation of its security program for all computing platforms, including conducting audit trails on UNIX servers. However, the Chief, Mission Assurance, disagreed that the IRS should continue to report audit trails as part of the computer security material weakness and believes the IRS has completed sufficient corrective actions to downgrade this area to a significant control deficiency. The Chief, Mission Assurance, also disagreed that not having application audit trails and deficiencies on the SAAS should be included in the audit trail material weakness area.

The CIO agreed with our recommendations and has directed the Enterprise Operations Services office to enhance, test, and install the audit trail solution on UNIX-based servers. After installation, the Enterprise Operations Services office will ensure audit trails are regularly generated and reviewed. In addition, the CIO will work with the Chief, Mission Assurance, and other business units to address reviewing audit trails on major applications. In the interim, the IRS has issued specific requirements for application-level auditing, will work with Modernization projects to ensure audit requirements are built into applications, and will determine if application auditing can be implemented when applications undergo system recertification. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment: We strongly believe that audit trails should remain part of the computer security material weakness. Audit trail deficiencies in the UNIX environment affect a significant portion of the IRS' computer infrastructure. Based on the Office of Mission Assurance's inventory of all IRS systems, as of February 2004, 19 (33 percent) of 58 Major Applications and Applications of Interest[2] operate on a UNIX platform, which means that employees' activities on those systems are not being monitored for inappropriate access and use. The Chief, Mission Assurance, agreed to provide enhanced auditing and monitoring of the UNIX servers that cannot generate audit trails, but he did not provide specific corrective actions. The impact of not having audit trails for these UNIX servers is noteworthy because 11 (19 percent) of the 58 Major Applications and Applications of Interest operate on these types of UNIX servers, which totals over 700 servers throughout the IRS.

In addition, we contend that application audit trails are critical for monitoring user activity and should be considered when determining the materiality of computer security weakness areas. As stated in this report, the IRS has taken great strides on maintaining and reviewing audit trails over its IDRS application. Just as critical are the numerous other applications that contain sensitive taxpayer data. Likewise, we believe the audit trail system for modernized systems should be included in the audit trail material weakness area. While our review on the SAAS was not originally planned as

[2] The IRS has defined Major Applications as applications that require special attention to security because of the severe adverse effect that compromise of those applications would have on the IRS mission, tax administration functions, and/or employee welfare. In addition, Applications of Interests are defined as applications that do not possess the level of interest, size, or scope of Major Applications but require additional levels of control because, based on business functionality, level of exposure and third-party interest, compromise would significantly degrade the IRS mission and tax administration operations.

part of our material weakness reviews, the review of audit trails for modernized systems is at least as critical as reviews of legacy systems.

Accordingly, we intend to elevate our disagreement to the Department of the Treasury for resolution. The Deputy Commissioner for Operations Support is responsible for ensuring the IRS Commissioner submits a written reply to the Assistant Secretary for Management and Chief Financial Officer of the Department of the Treasury within 30 calendar days of the final report issuance date. This reply should explain the IRS' reasons for disagreement with the recommendations contained in this audit report. The IRS Commissioner will provide a copy of the reply to the TIGTA. Resolution shall be made within a maximum of 6 months after issuance of a final TIGTA audit report, in accordance with Office of Management and Budget Circular A-50.

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

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 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."[2] The Office of Management and Budget monitors progress on resolving these weaknesses.

In October 2002, the Internal Revenue Service (IRS) combined five security material weaknesses[3] that were mostly based on facility types into one material weakness on computer security. This was done to address computer security from an enterprise-wide approach and better align the weakness areas with the new organizational structure. The IRS further segregated the computer security material weakness into nine areas,[4] one of which covers the monitoring of key networks and systems, commonly referred to as audit trails. The IRS' goal was to effectively monitor key networks and systems to identify unauthorized activities and inappropriate system configurations.

[1] 31 U.S.C. §§ 1105, 1113, 3512 (2000). Legislation requiring Federal Government agencies to establish and maintain adequate internal control systems.

[2] Memorandum from the Secretary, Department of the Treasury, dated March 19, 2002, entitled, "Action Plan for Material Weakness Resolution and Audit Follow-up."

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

[4] The computer security material weakness consists of (1) network access controls, (2) key computer applications and system access controls, (3) configuration of software, (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.

Audit trails are historical records of user activity and application processes. They are often needed to perform diagnostic troubleshooting on system operational problems. Audit trails are also needed to detect unauthorized intrusions and provide the documented evidence needed for incident response and subsequent prosecution efforts.

The IRS has a long history of either not running audit trails or not reviewing them to detect unauthorized activity. Most recently, the Government Accountability Office (formerly the General Accounting Office) reported in May 2003 that the IRS did not have effective audit trail controls and did not routinely monitor key systems to identify unauthorized activities and inappropriate system configurations.[5]

In March 2002, we reported the IRS did not routinely review audit trails for its sensitive systems except the Integrated Data Retrieval System (IDRS).[6] The IRS did not have (1) automated reporting software needed to help analyze the vast amount of audit trail information, (2) accountability and staffing to carry out audit trail review responsibilities, (3) sufficient computer capacity to run audit trails, and (4) sufficient guidelines to assist in conducting audit trail reviews.[7]

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

This audit was conducted in the Office of Mission Assurance in the IRS Headquarters in New Carrollton, Maryland; the Martinsburg, West Virginia,

[5] *Information Security: Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks* (GAO-03-44, dated May 2003).
[6] The IDRS enables employees in the field offices and campuses to have instantaneous visual access to certain taxpayer accounts. The system can be used to research accounts, enter transactions or collection information, or generate notices and other documents.
[7] *User Activity on Most Sensitive Computer Systems Is Not Monitored* (Reference Number 2002-20-075, dated March 2002).

and Memphis, Tennessee, Computing Centers;[8] and the Brookhaven, New York, and Memphis, Tennessee, Campuses[9] during the period August 2003 through April 2004. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Significant Progress Has Been Made in Implementing the Internal Revenue Service Audit Trail Strategy

The IRS Office of Mission Assurance developed an enterprise-wide audit trail strategy to ensure audit trail information is reviewed on a routine basis. Actions included:

- Developing audit trail standards and procedures based on National Institute of Standards and Technology (NIST) guidelines.[10]
- Coordinating with IRS organizations to develop and implement audit trail procedures for specific operating system platforms used within the IRS.
- Validating that audit trail procedures are functioning for operating systems environments.

The IRS has made significant progress toward completing its strategy for addressing audit trail weaknesses. The Office of Mission Assurance developed overall standards for audit trails and coordinated with key Information Technology Service organizations to draft and implement procedures on the various operating systems used within the IRS.

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

[9] IRS campuses are comprised of the Submission Processing, Accounts Management, and Compliance Services functions, which receive, process, and archive paper and electronic tax and information returns; issue taxpayer notices; process refunds; answer taxpayers' tax law/account inquires through telephone, correspondence, fax, and email; adjust taxpayer accounts; conduct correspondence examinations; and provide taxpayers with post-filing services related to Collection and Examination function cases.

[10] The NIST develops standards and guidelines for providing adequate information security for Federal Government operations and assets.

To better organize its approach on addressing audit trail concerns, the IRS categorized its computer system operating environments into the following three tiers:

- Tier 1 systems, which are relatively few in number, are mainframe computers that handle a high volume of critical operational data.
- Tier 2 systems, which number in the hundreds, are UNIX-based minicomputer servers that provide specialized services.
- Tier 3 systems, which number in the thousands, are Windows-based computer servers that run major IRS business unit applications and support the computing infrastructure.

The IRS carried out its plans for addressing Tiers 1 and 3. These actions were successful in resolving the audit trail material weaknesses on those operating systems. However, significant issues still exist for Tier 2 systems.

Controls over audit trail information on a Tier 1 mainframe system had minor problems, which were addressed soon after we identified them

In general, we found Tier 1 mainframe systems generated audit trail information that was collected and reported weekly to security staff at various locations. The security staff reviewed the reports and forwarded information on security violations to the appropriate managers for further review. The extent of review of the security violations varied.

However, we identified two areas of concern related to audit trails on one Tier 1 mainframe system: audit trail reports did not capture key information, and audit trail reports were not reviewed. When notified of our concerns, the IRS took steps to address these issues.

The audit trail reports for the Tier 1 Security and Communications System (SACS),[11] which is operated out of both the Martinsburg and Tennessee Computing Centers,

[11] The SACS provides security, communications, and terminal management for thousands of IDRS and Corporate Files On-Line user terminals.

did not capture all of the information required by IRS standards, specifically whether a computer command issued by a user was a success or failure. NIST guidelines for Federal Government agencies direct that system-level audit trails should capture the functions performed once a user is logged on (e.g., the applications the user tried, successfully or unsuccessfully, to access).

Audit trails did not capture the success or failure of attempted accesses for the SACS because the programming was not written to capture this information. Significant effort would be required to recode the SACS to capture success or failure for the audit trail. IRS officials did not believe recoding would be worth the effort. Instead, they have developed alternative procedures that will be adequate, if properly implemented.

The procedures require SACS security administrators to search files for commands used to alter files or resources on the system. When a SACS security administrator identifies such commands, a violation report that contains all instances of the use of such commands will be sent to the user's manager. The manager must review the violation report, explain the use of the sensitive commands, and sign and return the violation report to the SACS security administrator.

Our second concern involved inadequate reviews of audit trail reports. The security administrator at one location was not aware that some of the audit trail reports existed and, therefore, was not running or reviewing them. This occurred due to insufficient communication between the site Security Office and the National Headquarters Technical Systems Software Division, which was responsible for producing the audit trail reports. However, after this omission was identified during our audit, the security administrator located the additional audit trail reports and established a review process.

While the SACS mainframe computers do not have a significant amount of taxpayer data, they do support other key functions. For example, if unanticipated or unauthorized user actions shut down the SACS, the IDRS application would be unavailable to IRS employees. The

IDRS application is critical to the IRS' customer service effort and to many other IRS functions.

Audit trail procedures for the Tier 2 environment have not been fully implemented

To address past concerns over not having automated auditing tools for analyzing audit trails, the IRS identified an audit product that was compatible with the UNIX version running on most Tier 2 servers. This software product, eTrust® Access Control and Audit (commonly called eTrust®), was to produce audit reports that are compliant with IRS audit requirements.

During our site visits, we found 184 (74 percent) of 250 Tier 2 UNIX servers did not have eTrust® software installed. Generally, audit trails were captured but not reviewed. Even for computers on which eTrust® software was installed, security specialists and system administrators were either not reviewing audit trail information or not performing a complete review that complies with IRS guidance. Employees advised us that eTrust® software produced data that were too voluminous and difficult to comprehend. The eTrust® software does not currently provide a feature to help analyze the data. Consequently, employees who were not familiar with audit trail review procedures were not reviewing the audit trail data.

During the deployment of eTrust® software, the IRS also found that the software did not interact properly with some existing applications and that it required more computer capacity than expected. As a result, eTrust® software is not providing adequate audit trail reports for the consolidated Tier 2 UNIX servers. The IRS has been working with the software vendor, who is optimistic that all of the technical issues can be resolved.

Audit trails are usually large files that can be extremely difficult to analyze manually. The use of automated software to analyze the data is likely to be the difference between unused audit trail data and a robust program. Until eTrust® software has been installed on all Tier 2 consolidated UNIX servers and employees perform required audit trail reviews, audit trails will continue to be a control weakness.

Tier 3 audit trail controls are working as intended

IRS oversight of Tier 3 audit trails has improved with installation and use of Aelita® software, an automated tool similar to eTrust® that collects audit trail information from Windows servers and generates reports for review. We interviewed employees responsible for reviewing 450 Tier 3 servers from 5 locations and found the Aelita® software was working as intended. Generally, employees were generating, maintaining, and reviewing audit trails.

We identified 27 (6 percent) of 450 servers that did not have Aelita® software installed. Most of these servers were nonproduction servers. When we raised this issue, security specialists stated that the Aelita® software was not supposed to be installed on nonproduction servers. Officials in the Office of Mission Assurance subsequently reevaluated that decision and directed that Aelita® software be installed on all nonproduction servers.

The Internal Revenue Service Strategy Did Not Address All Significant Audit Trail Weaknesses

Although the IRS has substantially implemented its audit trail strategy, except for Tier 2 systems, critical issues have not been addressed. We believe these issues are significant and should be addressed before the audit trails material weakness area is downgraded.

Some UNIX servers cannot generate audit trails without impairing the servers' performance

Approximately 700 UNIX servers supporting the Integrated Collection System (ICS)[12] application do not have the capacity to generate audit trails without significantly degrading performance. As a result, the ICS Project Office made the decision to not activate the audit trail capabilities of its servers.

The ICS is a critical system for carrying out the IRS' collection programs and contains a significant amount of sensitive taxpayer data. The Office of Mission Assurance has emphasized its importance by categorizing it as a major application within the IRS.

[12] The ICS provides workload management, case assignment/tracking, inventory control, electronic mail, case analysis tools, and management information capabilities to support tax collection fieldwork.

The IRS has acknowledged that implementing audit trail logging cannot be consistently achieved on the older ICS UNIX servers, due to insufficient memory capacity and processing resources. The IRS expects to replace these computers in Fiscal Year 2005. Until the computers are replaced, the IRS will not be able to monitor for unauthorized accesses on these servers.

Audit trails on applications were not addressed in the IRS' material weakness efforts

To address the audit trails material weakness area, the IRS focused its efforts on operating system platforms. We acknowledge that this is a critical first step. However, the IRS has not recognized the need for audit trails at the application level for most of its systems.

Audit trails on an operating system can identify applications accessed by an individual, but they do not provide information on what the individual did after accessing the application. Currently, audit trails are being run and reviewed on very few applications in the IRS. The best example of this is the audit trail functionality of the IDRS.

The IRS has effective audit procedures in place to ensure audit trail reports for the IDRS are regularly reviewed to deter and detect unauthorized access or misuse of taxpayer data and accounts. IDRS audit trail reviews have consistently identified potential unauthorized access to taxpayer accounts in spite of the IRS' zero tolerance policy and awareness programs. For example, in its Semiannual Report to the Congress for the period April 1, 2003, through September 30, 2003, the TIGTA reported it had identified 233 potential IDRS security breaches that were referred to its field staff for further investigation.

The consistent identification of IDRS security breaches is a strong indication unauthorized accesses to taxpayer data may be occurring without detection on other systems that provide access to the same type of sensitive taxpayer data as the IDRS. It is certain the IRS and the TIGTA Office of Investigations will not detect such security breaches if the IRS continues to generate audit trails on only a few of its hundreds of sensitive computer systems.

NIST guidance states that, when an application is critical, it can be desirable to record who accessed the application along with certain details specific to each use. The decision about how much to log and how much to review should be a function of application or data sensitivity and should be decided by each functional manager or application owner with guidance from the system administrator and the computer security manager, weighing the costs and benefits of the logging.[13]

The Office of Mission Assurance indicated that addressing widespread computer security problems should start at a common ground, which, in this case, was the operating system level. We believe the IRS should also run and review application audit trails for the major applications, at a minimum.

The IRS' modernized system to collect and generate useful audit trail reports was not working as intended

The IRS and the PRIME contractor[14] developed the Security Audit and Analysis System (SAAS) to meet audit trail needs for modernized systems and the IDRS. Key information necessary to detect improper activities and to reconstruct events for potential criminal investigations was to be collected and stored in a central database warehouse from which users could generate reports and create custom queries.

However, the SAAS is not working as intended. As a result, IRS business units, the Office of Mission Assurance, and the TIGTA cannot use the SAAS to carry out their monitoring responsibilities.

In our review of audit trails for modernized systems,[15] we found that audit trail data are being stored, but the SAAS does not have adequate functionality and software

[13] NIST Special Publication 800-12, *Introduction to Computer Security*.

[14] The Computer Sciences Corporation serves as the PRIME contractor to design and develop modernization programs and projects for the IRS. The Business Systems Modernization Office within the IRS coordinates and oversees the work of the PRIME contractor.

[15] *The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning* (Reference Number 2004-20-135, dated August 2004).

performance to support queries of the data. In addition, operating procedures for the SAAS have not been developed. Consequently, even if the SAAS was functioning, users would not be able to conduct effective audit trail reviews.

Not having a functioning audit trail inhibits the IRS' ability to detect unauthorized activities on its modernized systems that have been implemented. Future applications that will provide the key tax administration functions in the modernized environment will rely solely on the SAAS to provide meaningful audit trail reports. The inability to detect unauthorized activities on these systems is a significant security risk that should be considered in deciding whether these systems should be accredited and implemented.

The deficiencies of the SAAS have been reported in another TIGTA report solely on that topic. As such, we are not making recommendations to address SAAS deficiencies in this report.

Overall, the IRS' strategy to address audit trails was aimed at the root causes that have plagued the IRS for years (inadequate computer capacity, automated reporting software needed to help analyze the vast amount of audit trail information, accountability and staffing to carry out audit trail review responsibilities, and sufficient guidelines to assist in conducting audit trail reviews). While significant progress has been made in implementing this strategy, problems still exist. Additional effort is needed to ensure audit trails are run and monitored on the Tier 2 computers, existing applications, and modernized applications before the audit trails material weakness area is downgraded.

Recommendations

The Chief, Mission Assurance, should keep the audit trails area as part of the computer security material weakness until:

1. The Tier 2 eTrust® audit trail software is operating effectively and security specialists are performing regular reviews of Tier 2 systems' audit trail data.

Management's Response: The Chief, Mission Assurance, partially concurred with our recommendation. While not all audit trail weaknesses have been corrected, the Chief, Mission Assurance, believes the IRS has completed sufficient corrective actions to downgrade this area to a significant control deficiency. The IRS agreed that it must continue to ensure effective implementation of its security program for all computing platforms, including the implementation of the eTrust® software on Tier 2 UNIX systems.

Office of Audit Comment: We strongly believe that audit trails should remain part of the computer security material weakness. Audit trail deficiencies in the Tier 2 UNIX environment affect a significant portion of the IRS' computer infrastructure. Based on the Office of Mission Assurance's inventory of all IRS systems, as of February 2004, 19 (33 percent) of 58 Major Applications and Applications of Interest[16] operate on a Tier 2 UNIX platform, which means that employees' activities on those systems are not being monitored for inappropriate access and use.

2. A reasonable approach is developed and implemented for reviewing audit trails over sensitive applications.

Management's Response: The Chief, Mission Assurance, partially concurred with our recommendation. The Chief, Mission Assurance, believes that the area of audit trails for applications is out of the scope of determining whether the audit trail area should be kept as a material weakness. However, in response to the issue of developing and implementing audit trail reviews over sensitive applications, the IRS is working with NIST guidance to define application-level auditing requirements. In the interim, the IRS has issued the specific requirements for

[16] The IRS has defined Major Applications as applications that require special attention to security because of the severe adverse effect that compromise of those applications would have on the IRS mission, tax administration functions, and/or employee welfare. In addition, Applications of Interest are defined as applications that do not possess the level of interest, size, or scope of Major Applications but require additional levels of control because, based on business functionality, level of exposure and third-party interest, compromise would significantly degrade the IRS mission and tax administration operations.

application-level auditing and has been working with Modernization projects to ensure audit requirements are built into applications during the development phases. In addition, when applications are identified for recertification, the IRS will determine if applications auditing can be implemented. If not, the project will be assessed to identify risks and to develop cost-effective risk mitigation strategies.

Office of Audit Comment: We disagree with the Chief, Mission Assurance, that application auditing is out of the scope of the material weakness definition. As part of this review, we determined whether the actions planned to resolve the specific vulnerabilities were sufficient to close the weakness. We contend that application audit trails are critical for monitoring user activity on specific applications and should be considered when determining the materiality of computer security weakness areas. As stated in this report, the IRS has taken great strides on maintaining and reviewing audit trails over its IDRS application. Just as critical are the numerous other applications that contain sensitive taxpayer data.

3. Critical applications are removed from Tier 2 unconsolidated UNIX servers or consolidated into a more secure environment.

Management's Response: The Chief, Mission Assurance, partially concurred with our recommendation. Because the IRS made a risk-based decision to continue to operate an older version of UNIX that cannot support audit trail functionality and has taken ancillary steps on audit trails in general, the IRS believes its efforts support reducing audit trail vulnerabilities to a significant control deficiency. Until these servers have been replaced, the IRS will continue to provide enhanced continuous monitoring of applications and systems residing on these servers.

Office of Audit Comment: We disagree with the Chief, Mission Assurance, that the IRS actions are sufficient to downgrade audit trails to a significant control deficiency. Because the IRS' response did not provide specific detail on what constitutes enhanced auditing and monitoring of these systems, we believe the operation of these servers represents serious security vulnerabilities since the IRS cannot monitor user activity on these servers.

The risk-based decision to operate vulnerable servers may have been justified since, for example, keeping the ICS application operational supports the collection of delinquent taxes. The acceptance of this risk does not preclude the IRS from being held responsible and accountable for ensuring security attributes are maintained on its systems. Based on the Office of Mission Assurance's inventory of all IRS systems, as of February 2004, approximately 11 (19 percent) of 58 Major Applications and Applications of Interest operate on the unconsolidated UNIX environment, which represents over 700 servers throughout the nation. Thus, we believe the audit trails should remain part of the computer security material weakness until this insecure environment no longer exists.

4. The SAAS is providing usable audit trail data for modernized applications.

Management's Response: The Chief, Mission Assurance, did not concur with this recommendation, stating that the issue and recommendation are new and unrelated to the scope and coverage of the original reported material weakness.

Office of Audit Comment: We disagree with the Chief, Mission Assurance, that the reporting of the audit trail system for modernized systems should not be part of our scope of work for the audit trail material weakness area. While our review on the SAAS was not originally planned as part of our material weakness reviews, the review of audit trails for modernized systems is at least as critical as reviews of legacy systems.

The Chief Information Officer should:

5. Direct the Director, Enterprise Operations, to continue with updating and implementing the Tier 2 eTrust® audit trail software on all applicable servers and ensure audit trails are being regularly generated and reviewed.

Management's Response: The Chief Information Officer agreed with our recommendation and the Enterprise Operations Services office has enhanced the eTrust® Access Control software to correct existing problems. The software will be tested and installed on all Tier 2 consolidated UNIX-based systems. After installation, the Enterprise

Operations Services office will ensure that eTrust® audit trails are regularly generated and reviewed.

6. Coordinate with the Office of Mission Assurance to develop and implement a reasonable approach for reviewing audit trails over major applications.

Management's Response: The Chief Information Officer agreed with our recommendation and will work with the Office of Mission Assurance and other business units to develop and implement a reasonable approach for reviewing audit trails over major applications.

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 vulnerabilities associated with its computer security material weakness. The IRS has segregated this material weakness into nine areas, one of which covers the monitoring of key networks and systems, commonly referred to as audit trails. The Department of the Treasury requested that the Treasury Inspector General for Tax Administration (TIGTA) provide an independent assessment on the effectiveness of the IRS' actions to address its computer security material weakness. This review, related to the monitoring of key networks and systems, is one of five reviews conducted this fiscal year to meet the request.

I. To determine whether the IRS identified the significant vulnerabilities that need to be corrected before closing the computer security material weakness, we:

  A. Interviewed Modernization and Information Technology Services (MITS) organization and Office of Mission Assurance staff.

  B. Reviewed relevant IRS and TIGTA documentation and reports on the IRS' approach to resolving the material weakness.

  C. Documented variations between IRS and TIGTA material weakness vulnerabilities.

II. To determine whether the actions planned to resolve the specific vulnerabilities were sufficient to close the weakness, we interviewed IRS staff, reviewed documentation, conducted site visits of IRS validations and corrective actions, and evaluated the actions. We made site visits to five locations: the IRS Headquarters in New Carrollton, Maryland; the Martinsburg, West Virginia, and Memphis, Tennessee, Computing Centers;[1] and the Brookhaven, New York, and Memphis, Tennessee, Campuses.[2] To increase audit efficiency and reduce the burden on IRS staff, we judgmentally selected sites that were important in the IRS validation effort and contained major computer facilities.

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

[2] IRS campuses are comprised of the Submission Processing, Accounts Management, and Compliance Services functions, which receive, process, and archive paper and electronic tax and information returns; issue taxpayer notices; process refunds; answer taxpayers' tax law/account inquires through telephone, correspondence, fax, and email; adjust taxpayer accounts; conduct correspondence examinations; and provide taxpayers with post-filing services related to Collection and Examination function cases.

III. To determine whether the planned actions taken to resolve the vulnerabilities have been fully implemented nationwide, we interviewed MITS organization and Office of Mission Assurance staff and conducted substantive onsite testing.

IV. To determine the effectiveness of IRS actions to resolve specific vulnerabilities, we:

A. Verified whether the audit trail feature was active on 4 mainframe, 250 UNIX, and 450 Windows network operating systems and on sensitive applications from the 5 locations visited.

B. Verified whether audit trails were maintained for operating systems and applications.

C. Verified whether audit trails were being reviewed with effective criteria to identify security incidents and what process was used when issues were identified.

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
Michelle Griffin, Senior Auditor
Myron Gulley, Senior Auditor
Michael Howard, Senior Auditor
Mary Jankowski, Senior Auditor
Louis Lee, Senior Auditor
Abraham Millado, Senior Auditor
Stasha Sue Smith, Senior Auditor
Esther Wilson, Senior Auditor

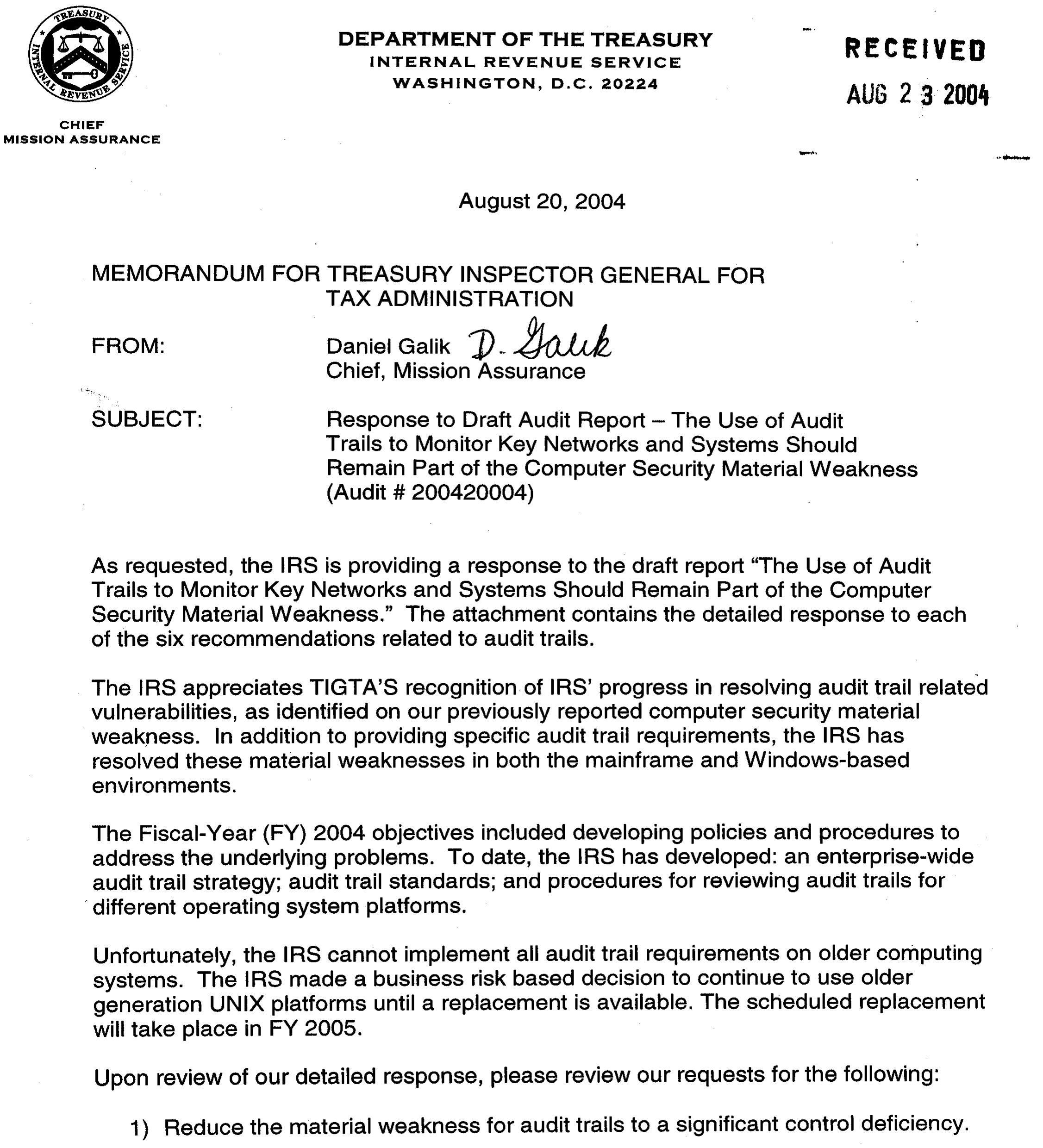
Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Director, Assurance Programs OS:MA:AP
Director, Modernization and Systems Security Engineering OS:MA:M
Director, Operational Assurance OS:MA:O
Associate Chief Information Officer, Information Technology Services OS:CIO:I
Director, Business Systems Development OS:CIO:I:B
Director, End User Equipment and Services OS:CIO:I:EU
Director, Enterprise Operations OS:CIO:I:EO
Director, Portfolio Management OS:CIO:R:PM
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

Appendix IV

Management's Response to the Draft Report



CHIEF
MISSION ASSURANCE

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

August 20, 2004

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR
TAX ADMINISTRATION

FROM: Daniel Galik D. Galik
Chief, Mission Assurance

SUBJECT: Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness (Audit # 200420004)

As requested, the IRS is providing a response to the draft report "The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness." The attachment contains the detailed response to each of the six recommendations related to audit trails.

The IRS appreciates TIGTA'S recognition of IRS' progress in resolving audit trail related vulnerabilities, as identified on our previously reported computer security material weakness. In addition to providing specific audit trail requirements, the IRS has resolved these material weaknesses in both the mainframe and Windows-based environments.

The Fiscal-Year (FY) 2004 objectives included developing policies and procedures to address the underlying problems. To date, the IRS has developed: an enterprise-wide audit trail strategy; audit trail standards; and procedures for reviewing audit trails for different operating system platforms.

Unfortunately, the IRS cannot implement all audit trail requirements on older computing systems. The IRS made a business risk based decision to continue to use older generation UNIX platforms until a replacement is available. The scheduled replacement will take place in FY 2005.

Upon review of our detailed response, please review our requests for the following:

1) Reduce the material weakness for audit trails to a significant control deficiency.

2) Review the need to keep a material weakness open, using the existing draft report.

3) Separate the new recommendations into a separate section to allow corrective actions related to this report to be monitored and closed. This is the approach GAO used in the audit report concerning the Disaster Recovery portion of the IRS material weakness action plan. This approach allowed for closure of completed action items and allowed a process to identify new issues, arising during the audit.

If you have any questions, please contact me at (202) 283-8910 or Rose Hernandez, Director, Certification Testing Evaluation, and Assessment at (202) 283-4500.

Attachment

Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

RECOMMENDATION # 1: The Chief, Mission Assurance, should keep the audit trails area as part of the computer security material weakness until: The Tier 2 eTrust audit trail software is operating effectively and security specialists are performing regular reviews of Tier 2 systems' audit trail data.

CORRECTIVE ACTION TO RECOMMENDATION #1:

We partially concur. The TIGTA draft report already concludes the IRS has successfully implemented corrective actions to address the material weakness, associated with audit trails. As such, the Computer Security Material Weakness should be downgraded to significant control deficiency.

While not all audit activity has been corrected, the IRS accomplishments substantiate removal of the audit trail area as part of the Material Weakness and the downgrade of this weakness to a significant control deficiency.

The IRS accomplishments include the following:

- Developed an enterprise-wide audit trail strategy;
- Developed audit trail standards, including procedures for reviewing audit trails for the different operating system platforms;
- Closed all audit trail issues for mainframe environments;
- Closed all audit trail issues for windows-based environments;
- Procured an automated tool to manage audit trails in the Windows environment and;
- Established a working group to address Windows auditing implementation issues.

The IRS agrees that we must continue to ensure effective implementation of our security program for all computing platforms, including the Tier 2 systems. With the implementation of eTrust, this will ensure the future success of audit of Tier 2 systems. In addition, the IRS will continue to enhance our review of all audit trails, as recommended.

IMPLEMENTATION DATE:

CLOSED (Note: eTrust action reported under recommendation #5)

RESPONSIBLE OFFICIAL:

Chief Mission Assurance

Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

CORRECTIVE ACTION MONITORING PLAN:
CLOSED (Note: eTrust action reported under recommendation#5)

Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

RECOMMENDATION # 2: The Chief, Mission Assurance, should keep the audit trails area as part of the computer security material weakness until: A reasonable approach is developed and implemented for reviewing audit trails over sensitive applications.

CORRECTIVE ACTION TO RECOMMENDATION #2:

We partially concur. This TIGTA issue/recommendation is outside of the scope of the draft report. As such, this should not be used in the determination to keep audit trails open as a material weakness.

Regarding application-level auditing, the IRS is working with NIST guidance to define application level auditing requirements. In 2004, the IRS issued the *Law Enforcement Manual (LEM) 25.10.8 Audit Security Standards* as interim guidance. This LEM contains specific requirements for application level auditing.

In addition, the IRS has been working with Modernization projects to ensure audit requirements are built into the application during the development of the applications to avoid the cost of retrofitting audit-related application security requirements.

As applications are identified for re-certification, the IRS will ensure these applications are reviewed to determine if application auditing can be implemented. If not, the project will be assessed to identify risks and will develop cost-effective, risk mitigation strategies.

IMPLEMENTATION DATE:

June 1, 2004

RESPONSIBLE OFFICIAL:

Chief Mission Assurance

CORRECTIVE ACTION MONITORING PLAN:

N/A

Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

RECOMMENDATION # 3: The Chief, Mission Assurance, should keep the audit trails area as part of the computer security material weakness until: Critical applications are removed from Tier 2 unconsolidated Unix servers or consolidated into a more secure environment

CORRECTIVE ACTION TO RECOMMENDATION #3:

We partially concur. TIGTA has already identified that the IRS UNIX systems are not capable of supporting audit trail reporting. The IRS has budgeted and planned for a FY 2005 replacement.

During this interim period, the IRS has made an, OMB/NIST approved, risk based decision to continue to use and to rely upon older generation UNIX platforms. The IRS should not be penalized, when it has used an approved decision-making process to make audit-related decisions.

The IRS has made the following significant accomplishments in regard to audit trails, during the past year:

- Developed an enterprise-wide audit trail strategy;
- Developed audit trail standards, including procedures for reviewing audit trails for the different operating system platforms;
- Agreed to provide enhanced auditing and monitoring of these systems and;
- Budgeted for a plan to replace the UNIX platforms, for Fiscal Year 2005.

The IRS efforts support reducing audit trails vulnerabilities to a significant control deficiency.

In addition, the IRS will continue to provide enhance continuous monitoring of these applications and servers until they have been replaced.

IMPLEMENTATION DATE:

The schedule for replacement of the old UNIX platforms will be completed by December 2005.

RESPONSIBLE OFFICIAL:

Chief Mission Assurance (Recommendation #3)
Chief Information Officer (UNIX platform replacement)

CORRECTIVE ACTION MONITORING PLAN:

Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

The IRS will identify additional steps and milestones for the audit trail issue to ensure that the significant control deficiency is monitored and tracked.

Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

RECOMMENDATION # 4: The Chief, Mission Assurance, should keep the audit trails area as part of the computer security material weakness until: The SAAS is providing usable audit trail data for modernized applications.

CORRECTIVE ACTION TO RECOMMENDATION #4:

The IRS does not concur with this recommendation. The TIGTA issue/recommendation is new and unrelated to the scope and coverage of the original IRS/Treasury reported material weakness.

As this relates to SAAS, TIGTA recently provided the IRS a draft report, entitled "The Audit Trails System for Detecting Improper Activities on Modernized Systems Is Not Functioning" (Audit #200420026). While there were recommendations made in this report, there was no indication that TIGTA viewed this as a material weakness.

IMPLEMENTATION DATE:

June 1, 2004

RESPONSIBLE OFFICIAL:

Chief Mission Assurance

CORRECTIVE ACTION MONITORING PLAN:

N/A

Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

RECOMMENDATION # 5a: The Chief Information Officer should:
Direct the Director, Enterprise Operations, to continue with updating and implementing the Tier 2 eTrust audit trail software on all applicable servers and ensure audit trails are being regularly generated and reviewed.

CORRECTIVE ACTION TO RECOMMENDATION #5a:

The eTrust Access Control software has been enhanced and will be installed by 01/01/05 on the consolidated Tier 2 servers at the Enterprise Computing Center and the Detroit Computing Center.

IMPLEMENTATION DATE:

January 1, 2005

RESPONSIBLE OFFICIAL:

Director, Enterprise Operations Services

CORRECTIVE ACTION MONITORING PLAN:

A schedule was developed and will be followed for installing and updating Tier 2 eTrust Access Control software by 01/01/05 on the consolidated servers at the Enterprise Computing Center and the.Detroit Computing Center.

Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

RECOMMENDATION # 5b: The Chief Information Officer should:
Direct the Director, Enterprise Operations, to continue with updating and implementing the Tier 2 eTrust audit trail software on all applicable servers and ensure audit trails are being regularly generated and reviewed.

CORRECTIVE ACTION TO RECOMMENDATION #5b:

The eTrust Audit software is being tested at the Enterprise Computing Center. After completion of the testing, the eTrust Audit solution will be installed on all Tier 2 Consolidation Solaris-based systems. All Tier2 eTrust installation will be completed by 01/01/05.

IMPLEMENTATION DATE:

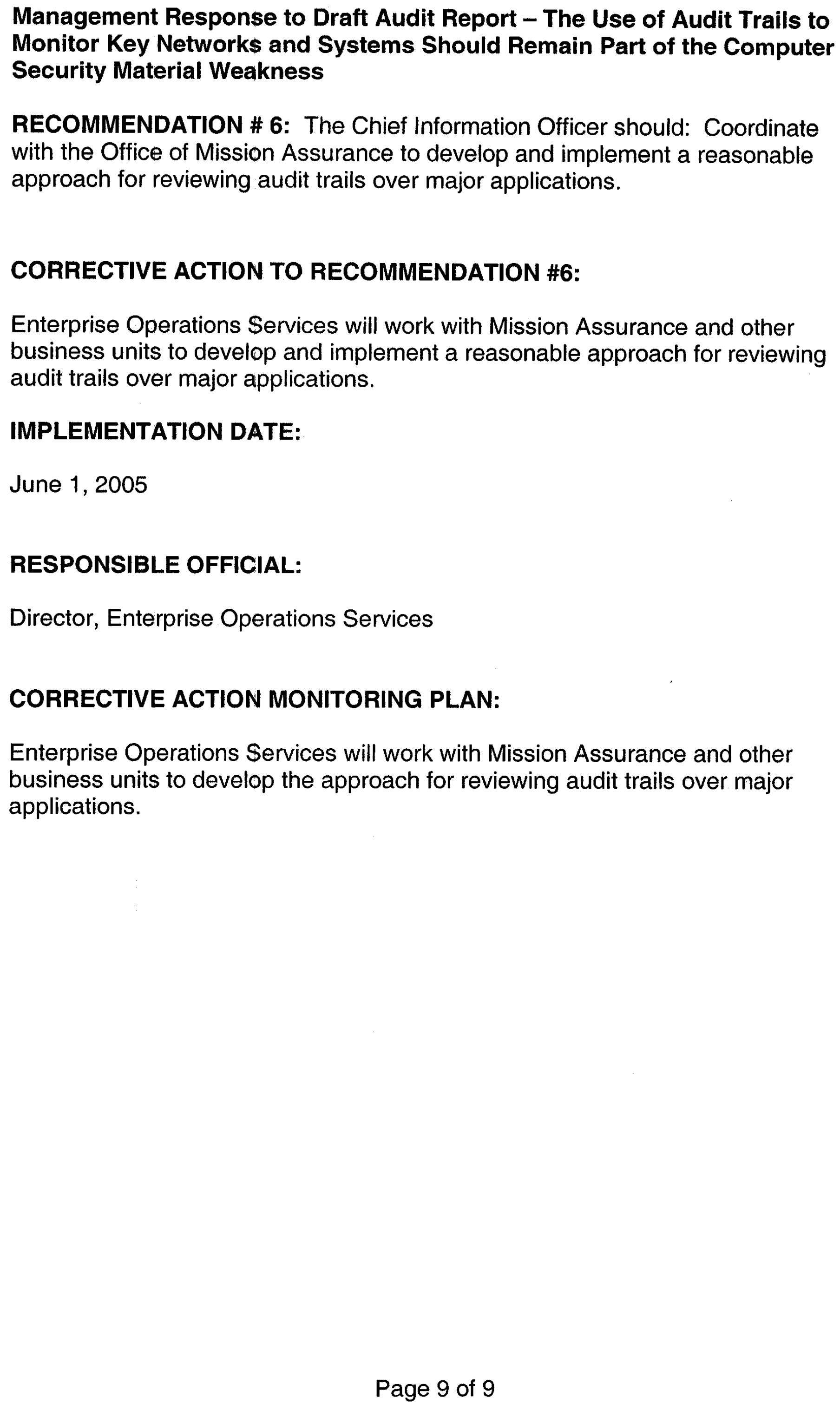
January 1, 2005

RESPONSIBLE OFFICIAL:

Director, Enterprise Operations Services

CORRECTIVE ACTION MONITORING PLAN:

Monthly updates on spreadsheets to monitor actions. The Tier2 installation schedule for the eTrust Audit Solution will be monitored during regular EOS meetings to ensure completion by 01/01/05. Once installed, EOS will ensure that eTrust Audit Trails are regularly generated and reviewed.



Management Response to Draft Audit Report – The Use of Audit Trails to Monitor Key Networks and Systems Should Remain Part of the Computer Security Material Weakness

RECOMMENDATION # 6: The Chief Information Officer should: Coordinate with the Office of Mission Assurance to develop and implement a reasonable approach for reviewing audit trails over major applications.

CORRECTIVE ACTION TO RECOMMENDATION #6:

Enterprise Operations Services will work with Mission Assurance and other business units to develop and implement a reasonable approach for reviewing audit trails over major applications.

IMPLEMENTATION DATE:

June 1, 2005

RESPONSIBLE OFFICIAL:

Director, Enterprise Operations Services

CORRECTIVE ACTION MONITORING PLAN:

Enterprise Operations Services will work with Mission Assurance and other business units to develop the approach for reviewing audit trails over major applications.