TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed to Ensure the Use of Modernization Applications Is Effectively Audited

September 29, 2006

Reference Number: 2006-20-177

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.

Phone Number | 202-927-7037
Email Address | Bonnie.Heald@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 29, 2006

MEMORANDUM FOR CHIEF INFORMATION OFFICER
CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed to Ensure the Use of Modernization Applications Is Effectively Audited
(Audit # 200620003)

This report presents the results of our review to determine whether the Internal Revenue Service's (IRS) modernized systems generate audit logs that are saved and analyzed to detect unauthorized accesses to modernization applications.

Impact on the Taxpayer

Audit trails[1] for the IRS' modernized systems are not being adequately collected, reviewed, or retained. Consequently, unauthorized access and theft of taxpayer records may be occurring without being detected, possibly resulting in theft of taxpayer identities. In addition, fraudulent transactions and intrusions on IRS systems used to administer tax laws could go undetected.

Synopsis

The IRS has two approaches for collecting audit trails for the computers supporting its Business Systems Modernization effort. Audit trails for the Customer Account Data Engine (CADE)[2] are stored internally. Audit trails for all other modernized systems are stored centrally and reviewed in the Security Audit and Analysis System (SAAS). Neither approach is working effectively.

[1] An audit trail is a chronological log of activities on a computer system.
[2] The CADE is the foundation for managing taxpayer accounts in the IRS' modernization effort.

The IRS is not monitoring audit trails on the CADE. While the CADE currently stores and processes only a small fraction of all taxpayer returns, its workload is expected to greatly increase in the next few years. This will place added importance on the IRS' ability to monitor accesses to the sensitive taxpayer records stored in the CADE. We believe CADE transactions are not reviewed because only a limited number of users have permission to access the system. However, these users have powerful access privileges, which could enable them to steal taxpayer information and take action to disrupt computer operations with little chance of detection.

The SAAS audit trails of user and system activities on modernized systems are not being adequately monitored. User activity audit trails on modernized systems are not being reviewed by the IRS business units and the Treasury Inspector General for Tax Administration (TIGTA) for two reasons. First, while audit trail data are being collected by the SAAS, the data are not accurate, reliable, and complete. We reviewed over 3 million audit trail records and found 48 percent of the places for data required by IRS policy were missing data or contained inaccurate information. Second, even if the SAAS audit trails were usable, reports and functions for reviewing them are not yet available, making it unlikely SAAS users could identify inappropriate activity on modernized systems.

System activity audit trails are not being adequately reviewed by the Computer Security Incident Response Center,[3] to identify security-related events. These audit trails have not been delivered timely and have not been completed sufficiently.

The underlying reason why audit trails on the SAAS are not adequately reviewed is the inadequacy of SAAS system requirements, which are used to identify the System's features and capabilities. Although the IRS accepted the SAAS in Fiscal Year 2002, the system requirements are still inadequate because much of the SAAS development effort to date has been focused on replacement of the Audit Trail Lead Analysis System.[4] This replacement has been a TIGTA and IRS priority because the System is aging. However, until all SAAS users emphasize the need to review audit trail data on modernized systems, sufficient priority will not be given to the development of SAAS audit trails.

Our results indicate the problems with the SAAS we reported[5] in August 2004 have not been adequately addressed, despite claims by the IRS that the SAAS has been functioning. In April 2005, the IRS responded to questions from the Senate Appropriations Committee that the "SAAS is effectively managing audit trail data for modernization systems." We again reported[6]

[3] This Center was designed to ensure the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify, contain, and eradicate cyber threats targeting IRS computers and data.
[4] This is an IRS system that aids the TIGTA in researching unauthorized access of taxpayer data by IRS employees.
[5] *The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning* (Reference Number 2004-20-135, dated August 2004).
[6] *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernized Systems* (Reference Number 2005-20-128, dated August 2005).

problems with the SAAS in August 2005. In its response to that report, the IRS disagreed with our conclusion that audit trails for IRS modernized systems were not functioning. IRS management explained the SAAS receives and processes audit trail transactions daily from several modernization applications and the data could be accessed through queries or reports.

Recommendations

We recommended the Chief, Mission Assurance and Security Services (MA&SS), establish a review process for CADE audit trails and ensure they are retained. For the SAAS, the Chief Information Officer should modify modernized system audit trails to comply with SAAS standards and capture information needed by user organizations. In addition, the Chief, MA&SS, should reassess the user and system requirements for the SAAS, including the control weaknesses identified in this report, and ensure the requirements are assigned a completion date. Once this is complete, SAAS procedures and processes should be reevaluated to ensure the new SAAS requirements are incorporated.

Response

The IRS agreed with our findings and recommendations. The MA&SS organization will establish an enterprise process for reviewing the audit trails of all IRS legacy (current) and modernized applications and systems, including CADE audit trails. In addition, it will establish, in conjunction with the Chief Information Officer, a viable retention policy for CADE audit trails that is consistent with established IRS policies. For the SAAS, the MA&SS organization will reassess the requirements for SAAS audit trails, including identifying all user requirements and the resulting SAAS system requirements needed to achieve them. The IRS will provide a Project Plan that includes development of change requests for modification of modernized applications to provide audit trail data to, and in the correct format for, the SAAS based on the reassessed SAAS requirements. The Plan will include expected implementation dates for each modernization application and will be based on funding and resource availability. Once SAAS requirements are reassessed, the MA&SS organization will establish procedures to ensure audit trails are properly reviewed and will assign staff to monitor failed audit trail records. Management's complete response to the draft report is included as Appendix V.

Office of Audit Comment

The IRS provided an implementation date of October 2008 for its corrective action addressing our recommendation to modify modernized system audit trails to comply with SAAS standards and capture information needed by user organizations. We recognize the difficult task the IRS faces in modifying modernized system audit trails to provide usable information, given their current state. However, this implementation date will leave the IRS without usable audit trails

for more than 2 years. With this response, the IRS is accepting the risk that unauthorized access to taxpayer information on modernized systems may occur and not be detected.

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 ..... Page 1

Results of Review ..... Page 4

Customer Account Data Engine Audit Trails Are Not Being Adequately Monitored ..... Page 4

Recommendations 1 and 2: ..... Page 5

Security Audit and Analysis System Audit Trails Are Not Being Adequately Monitored ..... Page 6

Recommendation 3: ..... Page 10

Recommendations 4 and 5: ..... Page 11

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 13

Appendix II – Major Contributors to This Report ..... Page 15

Appendix III – Report Distribution List ..... Page 16

Appendix IV – Additional Information on the Security Audit and Analysis System Audit Trail ..... Page 17

Appendix V – Management's Response to the Draft Report ..... Page 21

Abbreviations

CADE	Customer Account Data Engine
CSIRC	Computer Security Incident Response Center
IDRS	Integrated Data Retrieval System
I-EIN	Internet Employer Identification Number
IFS	Integrated Financial System
IRFOF	Internet Refund/Fact of Filing
IRS	Internal Revenue Service
MA&SS	Mission Assurance and Security Services
MeF	Modernized e-File
SAAS	Security Audit and Analysis System
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized accesses and inspections of taxpayer records

Background

Internal Revenue Service (IRS) procedures state that each of the IRS' computer systems is required to collect and maintain adequate audit trail information and that this information is to be timely reviewed. An audit trail is defined as a chronological record of system activities that allows for the reconstruction, review, and examination of a transaction from inception to final results. Audit trails can also be used to diagnose computer problems because they capture all user and system activities associated with a transaction and provide documentation that identifies what has been done.

An audit trail is a chronological record of system activities that allows for the reconstruction, review, and examination of a transaction.

The National Institute of Standards and Technology[1] states that audit trails can provide a means to help accomplish several security-related objectives, including:

- Individual accountability – Enables managers to identify and provide information about users suspected of improper modification of data (e.g., introducing errors into a database).
- Reconstruction of events – Assesses damage to a system by pinpointing how, when, and why normal operations ceased.
- Intrusion detection – Identifies attempts to penetrate a system and gain unauthorized access.
- Problem analysis – Provides online tools to help identify problems other than intrusions as they occur.[2]

For the IRS, audit trails on modernized systems are also needed to detect unauthorized access attempts, successful accesses of its most critical information, and attacks on its systems. In particular, audit trails are used to identify willful unauthorized accesses and inspections of taxpayer records (UNAX). Identifying UNAX violations became more important with the passage of the Taxpayer Browsing Protection Act of 1997,[3] which states the willful unauthorized access or inspection of taxpayer records is a crime punishable upon conviction by fines, prison terms, and termination of employment.

[1] The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
[2] The National Institute of Standards and Technology Information Technology Laboratory Computer Security Bulletin published in March 1997.
[3] 26 U.S.C.A. §§ 7213, 7213A, 7431 (West Supp. 2003).

In addition to identifying UNAX violations, audit trails can be used to identify whether IRS financial information and transactions have been compromised. Such compromise could result in corruption of financial data and limit the IRS' ability to conduct business. Compromise of financial information could also result in fraudulent transactions, such as unauthorized payments.

However, none of these events can be detected if audit trails have not been designed to capture key information and are not retained for a sufficient period of time. Also, management must have a formal process for reviewing audit trail reports to effectively respond to system events.

The IRS has two approaches for collecting audit trails for the computers supporting its Business Systems Modernization effort. For the Customer Account Data Engine (CADE), audit trails are stored internally in the system's database. The CADE is the foundation for managing taxpayer accounts in the IRS' Business Systems Modernization effort and will eventually house taxpayer accounts and tax return data for more than 135 million individual and business taxpayers. The CADE will incrementally replace the existing IRS Master File.[4] The current release of the CADE processes selected data for over 1.4 million single filers with no dependents who filed an Income Tax Return for Single Filers and Joint Filers With No Dependents (Form 1040EZ) in Calendar Year 2005.

Audit trails for all other modernized systems are centralized in the Security Audit and Analysis System (SAAS). See Appendix IV for a list of these systems. The SAAS was initially built by the IRS' PRIME contractor as part of the Business Systems Modernization effort and was accepted by the IRS in 2002. The SAAS is designed to gather user and system audit trail information from these systems and store this information in a central database that should be accessed and used by the following customers:

- Managers from the IRS business units, who should review user audit trails for questionable activities of their employees on IRS modernized systems, by reviewing the transactions from those systems. Potential UNAX violations and fraudulent transactions are forwarded to the Treasury Inspector General for Tax Administration (TIGTA) for investigation.
- TIGTA investigators, who are responsible for detecting and investigating UNAX violations in accordance with the Taxpayer Browsing Protection Act of 1997. The TIGTA uses various techniques to analyze audit trail data to identify potential UNAX violations.
- The Computer Security Incident Response Center (CSIRC)[5], which should review system audit trail data generated by operating systems, databases, and applications of

[4] The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
[5] The CSIRC was designed to ensure the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify, contain, and eradicate cyber threats targeting IRS computers and data.

modernized systems to detect and respond to computer security incidents targeting the IRS' enterprise information technology assets.

This review was performed in the Mission Assurance and Security Services (MA&SS) organization and the Modernization and Information Technology Services organization, at the Enterprise Computing Center – Martinsburg,[6] in Kearneysville, West Virginia, and in the MA&SS organization in Lanham, Maryland, during the period October 2005 through March 2006. 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.

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

Results of Review

The IRS is not adequately collecting, reviewing, or retaining audit trail data from its modernized systems. Without adequate processes in these areas, unauthorized accesses or security intrusions could be occurring without being detected.

Customer Account Data Engine Audit Trails Are Not Being Adequately Monitored

The IRS is properly monitoring audit trails to identify attempts by unauthorized persons to access the CADE, and any security violations noted are sent to appropriate management officials for review and certification. However, once a user is authorized to access the CADE, his or her actions are not monitored. The lack of monitoring provides no assurance that an authorized user is accessing CADE data for official business purposes only.

While the CADE currently stores and processes only a small fraction of all taxpayer returns, its workload is expected to greatly increase in the next few years, as shown in Table 1. This growth places added importance on the IRS' ability to monitor accesses to the sensitive taxpayer records stored in the CADE. If the IRS cannot review audit trail information for the current volume of returns, its ability to adequately and effectively review audit trails will diminish when the volume increases in future years.

Table 1: Estimated Number of Returns to Be Processed by the CADE

Year	Estimated Number of Returns	Year	Estimated Number of Returns
2005	1,423,417 (Actual)	2009	70 million
2006	4 million	2010	90 million
2007	33 million	2011	100 million
2008	50 million	2012	135 million

Source: Customer Relationship Management Executive Steering Committee, approved October 18, 2005.

The IRS has not emphasized the need to monitor audit trails on the CADE because it is updated primarily through input of data from other IRS systems. Consequently, only a limited number of users have direct access to the CADE application. The CADE is currently accessible by only 39 persons including IRS computer personnel, contractors, and TIGTA personnel. However, these users have powerful access privileges that could enable them to steal taxpayer information with little chance of detection. By not reviewing user transactions in the CADE's audit trails, the IRS cannot be assured that security violations are not occurring.

Also, CADE audit trails are not being sufficiently retained. Currently, audit trails are retained for 30 calendar days, a retention period based on available storage space. In comparison, SAAS audit trail data are required to be retained for 6 years.

We previously identified the CADE audit trail review and retention issues in our August 2005 report,[7] but at that time, CADE audit trails were retained for only 1 to 2 calendar days and were not being reviewed. We recommended CADE audit trail data be retained and reviewed to detect unauthorized accesses. The IRS disagreed with this recommendation, stating that log and audit files used by CADE system programmers are established for recovery and diagnostic purposes and do not capture data related to unauthorized access. In response, we commented that we continue to believe audit trail information for the CADE should be retained and reviewed. The CADE contains tax information for over 1.4 million returns that could be accessed by some IRS employees for unauthorized purposes, potentially resulting in identity thefts. Therefore, audit trail information must be maintained to comply with Department of the Treasury requirements.

Recommendations

Recommendation 1: To ensure CADE audit trails are reviewed, the Chief, MA&SS, should establish a review process for CADE audit trails. Such a process will aid in current reviews and position the IRS to perform future reviews when the amount of taxpayer information residing in the CADE is significantly larger.

> ***Management's Response:*** IRS management agreed with this recommendation. The MA&SS organization will establish an enterprise process for reviewing the audit trails of all IRS legacy (current) and modernized applications and systems, including CADE audit trails.

Recommendation 2: To ensure CADE audit trails are sufficiently retained, the Chief, MA&SS, and the Chief Information Officer should establish a viable retention policy for CADE audit trails, mirroring, where possible, that of other systems with taxpayer information.

> ***Management's Response:*** IRS management agreed with this recommendation. The MA&SS organization, in conjunction with the Chief Information Officer, will establish a viable retention policy for CADE audit trails that is consistent with established IRS policies governing records management and retention standards for systems with taxpayer information.

[7] *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernized Systems* (Reference Number 2005-20-128, dated August 2005).

Security Audit and Analysis System Audit Trails Are Not Being Adequately Monitored

The three primary users of the SAAS (the IRS business units, TIGTA, and CSIRC) are performing either no reviews or limited reviews of user and system activity on modernized systems, as recorded in the systems' audit trails. As a result, possible UNAX violations, other inappropriate accesses, or security intrusions may be occurring without being identified.

An underlying reason for the lack of reviews is inadequate requirements for the SAAS, which are used to identify features and capabilities for the System. SAAS requirements have not been adequately identified because much of the SAAS development effort to date has been focused on replacement of the Audit Trail Lead Analysis System, which is currently used by the TIGTA to identify potential UNAX violations on the Integrated Data Retrieval System (IDRS).[8] The replacement of the Audit Trail Lead Analysis System has been a TIGTA and IRS priority because the System is aging. Until all SAAS users emphasize the need to review modernized system audit trails, sufficient priority will not be given to the development of SAAS audit trails.

Our results indicate the problems with the SAAS we reported[9] in August 2004 have not been adequately addressed despite claims by the IRS that the SAAS has been functioning. In April 2005, the IRS responded to questions from the Senate Appropriations Committee that the "SAAS is effectively managing audit trail data for modernization systems." In August 2005, we again reported[10] problems with the SAAS. In their response to that report, IRS management disagreed with our conclusion that audit trails for IRS modernized systems were not functioning. IRS management explained the SAAS receives and processes audit trail transactions daily from several modernization applications and the data could be accessed through queries or reports.

IRS business units and the TIGTA are not reviewing user activity on modernized systems

The IRS business units and the TIGTA are not reviewing SAAS user audit trails, which document a user's actions on modernized systems. Specifically:

- IRS business unit managers are not reviewing employee transactions on modernized systems through the SAAS. The MA&SS organization is currently reviewing user activity for one application to identify employees' accesses to their own and other employees' information. The MA&SS organization is planning to train business unit

[8] The IDRS is the IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records.
[9] *The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning* (Reference Number 2004-20-135, dated August 2004).
[10] *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernized Systems* (Reference Number 2005-20-128, dated August 2005).

employees to conduct these reviews using the SAAS and eventually to transition these reviews to all IRS functions. However, no timetable for the transition has been established. Transactions by employees on the other systems, as well as those initiated by users accessing systems through the IRS.gov web site, are not being reviewed.

- The TIGTA is unable to review modernized systems for possible UNAX violations. Currently, the TIGTA only reviews IDRS audit trails to identify UNAX violations, using the Audit Trail Lead Analysis System.

At present, the only audit trails available for IRS business unit managers and the TIGTA to review are those for IRS employee transactions. In October 2005, the IRS ceased adding transactions by nonemployees to the SAAS, such as those for tax filers and users of the IRS.gov web site, to address an immediate problem of insufficient data storage and to improve the performance of the System. These transactions are now stored in separate files in the SAAS. MA&SS organization personnel informed us this was justified because the TIGTA and IRS business units had not provided any requirements to review these data. In addition, these transactions can be made available to the business units and the TIGTA once requirements are identified to review the transactions.

Reviews of user activity are not occurring because a large amount of audit trail data in the SAAS is not usable. In addition, reporting features that would aid users in reviewing these data are not adequate.

User activity data are not reliable, complete, and accurate

The audit trails collected by the SAAS do not comply with the IRS' audit trail requirements. The data collected have significant integrity issues, rendering much of the data unreliable, inaccurate, incomplete, and, therefore, unusable. For a record in an audit trail to be useful, certain data must be complete and valid. These data include who initiated the transaction, when the transaction occurred, where it occurred, and whether the transaction succeeded or failed.

We reviewed over 3 million SAAS audit trail records of modernized systems for November 2005 and identified over 24 million possible entries[11] for data required by IRS policies. Of these, we determined that 48 percent were missing data or contained inaccurate information. In particular, we found blank entries, incomplete entries with partial numbers or text, and unexpected data such as numbers where text is expected. In addition to the required entries, the SAAS audit trail can store descriptive information about a transaction, which is useful in the search for UNAX violations. We determined that, while the SAAS audit trail record has 15 places for these descriptive entries, only 1 of the available places contained useful information. In addition to inadequate data entries, we identified over 80,200 potentially missing audit trail records and over 3,400 corrupted audit trail records. Appendix IV presents additional details on this issue.

[11] Each audit trail record has eight entries, or places, for data required by IRS policies.

Due to these data integrity issues, the MA&SS organization has not engaged IRS business units to review employee activity on modernized systems. The data integrity issues are a result of inaccurate and incomplete data being sent to the SAAS by modernized systems and insufficient controls in place to ensure the audit trail data brought into the SAAS are complete and valid. Modernized systems send audit trail data to the SAAS, which then processes and tests the data for existence of selected information. However, the following problems with this process exist:

- Invalid, inconsistent, or incorrectly formatted data are sent from modernized systems. Many of the data integrity issues we identified can be attributed to specific modernized systems. In addition, IRS personnel informed us some modernization application projects did not adequately test the audit trail output their applications produced to verify that the applications were correctly generating audit trail records that met IRS requirements.
- No tests are conducted to ensure audit trail entries are appropriate and accounted for. The SAAS currently tests incoming audit records to ensure six types of data, such as username and taxpayer identifier, exist in an audit trail record and the fields are not blank. However, there are no SAAS requirements to test the appropriateness of audit trail entries or to ensure all audit records are accounted for.
- Failed integrity test records are not reviewed. Failed integrity test results are not recorded in the SAAS audit trail; instead, they are recorded in a Failed Audit table. For November 2005, over 620,000 records failed SAAS validity tests. This represents 16 percent of all audit trail records sent to the SAAS for November 2005. Based on our discussions with IRS security personnel, the Failed Audit table is not reviewed. Currently, there are no SAAS requirements to provide users with features to review failed audit records.

During our audit, the MA&SS organization submitted a change request for the modernized system audit trails to be revised to properly recognize user actions as well as comply with standard formats and content. The primary focus of the request was to address inconsistencies in how modernized systems record transaction events and the payload, or transaction content, portion of the audit trail record. These changes were requested to be completed by June 2006.

In August 2005, we reported[12] the IRS did not adequately consider security controls in the development phase of modernized systems. Several inadequate security controls were identified, many of which could have been addressed in the development phase of the systems. Given the lack of robust integrity tests and the inadequacy of audit trail data being sent to the SAAS, it is apparent sufficient emphasis was not placed on audit trails during the development and in certification testing of modernized systems.

[12] *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernized Systems* (Reference Number 2005-20-128, dated August 2005).

Report features are not adequate for the business units and the TIGTA

Even if the modernized audit trails were reliable, it is unlikely that users of the SAAS would be able to review them because SAAS features needed to review these data are not yet available. The SAAS is designed to be both the replacement for the Audit Trail Lead Analysis System and the central repository for modernized IRS systems' audit trails. The SAAS is intended to enable IRS business unit, TIGTA, and CSIRC users to generate reports and search audit trail records to detect unauthorized activities and security intrusions on modernized systems. In addition, IRS managers will be able to certify they have reviewed modernized audit trail reports for their employees, to identify accesses and violations. These reports and functions are specified in the SAAS requirements used to develop the System. Similar features are also available on the IDRS On-Line Reports Services application, which aids IRS managers in identifying UNAX and other violations on the IDRS.

However, SAAS reports and certification features have not yet been implemented. Currently, users can search audit trail records only through user-created queries. While report features are included in the current System requirements, they have not been implemented and do not have completion dates assigned. This occurred in part because IRS business units have historically placed little emphasis on reviewing audit trail data. For example, a recent TIGTA report[13] found that business unit managers were not reviewing audit trail data to detect inappropriate activity of their employees on the IDRS.

The CSIRC does not have sufficient data with which to identify intrusions on modernized systems

We also determined the CSIRC is performing limited reviews of system audit trails to identify security intrusions on modernized systems. System audit trails document the system activities, including those taken during an attack or intrusion into the system. The CSIRC is performing some reviews of modernized system audit trails. However, these reviews are limited because audit trail files needed by the CSIRC are not being sent or sent timely to the SAAS. Procedures require that these files be sent daily from all modernized systems, excluding mainframe computers, to a central server (the Log File Collector) for forwarding to the SAAS. In addition, the files sent are not required to be retained for a sufficient period of time. These deficiencies are a result of insufficient SAAS requirements. Specifically:

- Files are not being sent timely. While audit trail files from Microsoft Windows-based modernized system servers generally are sent as required, files from servers running the Sun Solaris operating system are not. Of the 26 Solaris-based modernized system servers, 5 sent their files daily, 18 sent their files weekly, and 3 did not send their files at all. While SAAS system requirements include creation of reports to identify systems that

[13] *Increased Managerial Attention Is Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses* (Reference Number 2006-20-111, dated July 2006).

failed to send data as required, this functionality has not been implemented and no completion dates have been assigned.

- Consolidated audit trail files are not sent. For Solaris-based computers, two sets of audit trail files can be created. One set contains eight individual files that record different system events. The other set records all events in one consolidated file and can potentially record more system event information. While CSIRC users would like to review information contained in the consolidated audit trail files, these audit trails are not forwarded from the Log File Collector to the SAAS for inclusion in the SAAS audit trail. We reviewed the Log File Collector on December 5, 2005, and identified approximately 214 gigabytes of consolidated audit trails covering a 2-week period. These files are not sent to the SAAS because CSIRC personnel and SAAS contractors are not considered security personnel by the IRS and, therefore, are not permitted access to the necessary command to convert the files to a format readable by the SAAS. In addition, SAAS requirements do not specify that the consolidated audit trail files need to be available for inclusion in the SAAS.
- Audit trail files are not sufficiently retained. After audit trail files sent from modernized systems are received by the SAAS, they are kept for 1 year. Because only selected data from these files are incorporated into the SAAS, it is important for the IRS to retain the files in the event additional research on system activity needs to be performed. The CSIRC requires the SAAS to retain data sent from modernization systems for 6 years, but the requirement does not specify what type of data should be retained. The requirements used to develop the SAAS include only the data stored in the SAAS and not the audit trail files providing the data. During our review, the IRS established an informal policy to store audit trail files for 6 years, but no documentation formalizing this policy was available.

Recommendations

To ensure the SAAS can better meet the needs of its customers and audit trail data reported are reliable, accurate, and complete, the Chief, MA&SS, should:

Recommendation 3: Reassess the requirements for SAAS audit trails, including identifying all user requirements and the resulting SAAS system requirements needed to achieve them. Once the reassessment is complete, requirements should be assigned completion dates. The reassessment process must include the following requirements:

- Additional validity tests to ensure audit trail data received are reliable and accurate.
- Controls to ensure all audit trail records are uniquely identifiable, and completeness tests to ensure all audit records are accounted for.
- Reports and queries to aid in the analysis of audit trail records that failed validity tests.

- Functionality for review and certification of employee access to taxpayer information, similar to the functions available through the IDRS On-Line Reports Services application.
- Consolidated Solaris audit files that are available for inclusion in the SAAS audit trail. To do this, technical issues preventing these files from being incorporated into the SAAS need to be resolved. Until the issues are resolved, these files should be retained.
- Retention period for source audit trail files sent from modernized systems to ensure files are kept for a necessary length of time.

Management's Response: IRS management agreed with this recommendation. The MA&SS organization will reassess the requirements for SAAS audit trails, including identifying all user requirements and the resulting SAAS system requirements needed to achieve them.

To ensure modernized systems send reliable, accurate, and complete audit trail information to the SAAS, the Chief Information Officer should:

Recommendation 4: Modify modernized system audit trails to comply with SAAS standards, ensuring data collected are valid and arranged in the proper format. This process should include the solicitation of input from user organizations, such as the IRS business units, TIGTA, and CSIRC, to identify their audit trail data needs.

Management's Response: IRS management agreed with this recommendation. The IRS will provide a Project Plan that includes development of change requests for modification of modernization applications to provide audit trail data to, and in the correct format for, the SAAS based on requirements identified in the corrective action for Recommendation 3. The Plan will include expected implementation dates for each modernization application and will be based on funding and resource availability. The IRS plans to make incremental changes as requirements are developed.

Office of Audit Comment: The IRS provided an implementation date of October 2008 for its corrective action to this recommendation. We recognize the difficult task the IRS faces in modifying modernized system audit trails to provide usable information, given their current state. However, this implementation date will leave the IRS without usable audit trails for more than 2 years. With this response, the IRS is accepting the risk that unauthorized access to taxpayer information on modernized systems may occur and not be detected.

To ensure new SAAS requirements are included in IRS procedures, the Chief, MA&SS, should:

Recommendation 5: After completion of the requirements reassessment, reevaluate SAAS procedures and processes to ensure the new SAAS requirements are incorporated and responsibilities for reviewing modernization audit trails are adequately defined. These

procedures should include reviews for audit trail records that failed validity tests and transactions by tax filers and registered users.

Management's Response: IRS management agreed with this recommendation. Once SAAS requirements are reassessed, the MA&SS organization will establish procedures to ensure audit trails are properly reviewed and assign staff to monitor failed audit trail records.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS' modernized systems generate audit logs that are saved and analyzed to detect unauthorized accesses to modernization applications. To accomplish this objective, we:

I. Determined whether adequate information was being captured in modernization application audit trails.

- A. Reviewed policies and procedures specifying system information required to be captured for audit trail purposes.
- B. Identified the modernization application audit trails that were processed through the SAAS.
- C. Determined whether modernization applications were generating required audit trail records by obtaining from the SAAS an extract of audit trail records for November 2005, which totaled over 3.6 million records, and reviewing audit trail settings for the CADE. Our analysis of these records identified that 48 percent of the required entries were not usable. We also determined that the CADE audit trail settings were appropriate.
- D. Assessed the impact of missing audit trail elements on the IRS' ability to detect, identify, and substantiate unauthorized accesses of modernization applications.
- E. Determined why modernization application audit trails do not capture required data elements.

II. Determined whether audit trails were being retained for required time periods.

- A. Reviewed policies and procedures regarding audit trails to identify storage requirements for audit trail data, including required retention periods.
- B. Determined whether modernization applications were retaining audit trail records for required time periods by analyzing audit trail settings and interviewing SAAS and CADE system and database administrators.
- C. Assessed the impact of absent audit trail records on the IRS' ability to detect, identify, and substantiate unauthorized accesses of modernization applications.
- D. Determined why modernization application audit trails are not retained for required time periods.

III. Determined whether audit trails were being analyzed to detect unauthorized access and other violations.

A. Reviewed policies and procedures regarding audit trails to identify monitoring and reporting requirements for audit trail data.

B. Determined whether user activity on modernization applications was being adequately monitored by reviewing current reports generated from the SAAS.

C. Assessed the impact of inadequate monitoring of audit trails on the IRS' ability to detect, identify, and substantiate unauthorized accesses of modernization applications.

D. Determined why modernization application audit trail monitoring was not occurring. This step included analysis of computer records from SAAS servers for November and December 2005 to determine whether audit trail files were being sent timely to the SAAS. This step included reviewing the records for all modernized systems sending data to the SAAS, in particular those running the Microsoft Windows or Sun Solaris operating systems. Our analysis identified that Microsoft Windows-based modernized system servers generally sent data as required. However, of the 26 Solaris-based modernized system servers, 5 sent their files daily, 18 sent their files weekly, and 3 did not send their files at all.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Kent Sagara, Acting Director
Gerald Horn, Audit Manager
Marybeth Schumann, Audit Manager
Michael Howard, Lead Auditor
David Brown, Senior Auditor
Myron Gulley, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Chief Information Officer OS:CIO
Deputy Chief, Mission Assurance and Security Services OS:MA
Associate Chief Information Officer, Enterprise Operations OS:CIO:EO
Associate Chief Information Officer, Enterprise Services OS:CIO:ES
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Deputy Commissioner for Operations Support OS
- Chief, Mission Assurance and Security Services OS:MA
- Director, Program Oversight Office OS:CIO:SM:PO

Appendix IV

Additional Information on the Security Audit and Analysis System Audit Trail

This appendix provides additional information on audit trail integrity issues for specific modernization applications. The SAAS collects audit trail information from most modernization applications, including:

- Modernized e-File (MeF): The MeF system modernizes the IRS' existing electronic filing system and provides an Internet-based electronic filing application that taxpayers can use to file IRS forms.
- e-Services: The e-Services system provides several third-party tools and data collection processes to enhance taxpayer interaction with the IRS.
- Integrated Financial System (IFS): The IFS is the new IRS financial and cost accounting system.
- Internet Refund/Fact of Filing (IRFOF): The IRFOF system, also known as "Where's My Refund" on the IRS.gov web site, allows IRS customers to retrieve their refund status as well as fact of filing information.
- Internet Employer Identification Number (I-EIN): The I-EIN system allows the general public to apply for an Employer Identification Number over the Internet and receive the number at the same time.

The data presented are based on reviewed SAAS data from November 2005, specifically from the SAAS audit trail table (MODTRANS) and two additional SAAS audit trail files for users registered through the IRS.gov web site (REGUSER) and tax filers (TAXFIL). We identified issues with required and descriptive audit trail records as well as missing audit records.

Required audit trail entries

We reviewed over 3 million SAAS audit trail records of modernized systems for November 2005 and determined 48 percent of the data entries required by IRS policy contained missing or inaccurate information. For each modernization application we reviewed, Table 1 lists the audit trail requirements specified in the Internal Revenue Manual and the percentage of the entries in the SAAS fields meeting these requirements that were unusable.

Table 1: Percentage of Unusable Required Entries in the SAAS Audit Trail

Audit Trail Requirement	Field Name	MeF	e-Services	IFS	IRFOF	I-EIN	Other	SAAS Totals
Date and time of the event	TIMESTAMP	0.0%	0.5%	0.0%	0.0%	0.0%	0.0%	0.3%
The unique identifier initiating an action	USERID	0.0%	8.4%	0.0%	100.0%	100.0%	0.0%	28.0%
Type of event	EVENTID	7.0%	48.0%	0.0%	100.0%	0.0%	0.0%	46.6%
Origin of the request for identification/authentication events	SRCADDR	6.2%	34.0%	83.1%	100.0%	0.0%	0.0%	50.8%
Subject of event, action taken	VARDATA	29.9%	49.4%	100.0%	0.0%	100.0%	0.0%	51.5%
Identity of user creating the event	USERID	0.0%	8.4%	0.0%	100.0%	100.0%	0.0%	28.0%
Role of user, when creating the event	None	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Success or failure of the event	ERRORMSG	100.0%	100.0%	0.0%	100.0%	0.0%	100.0%	78.9%
Totals		**30.4%**	**43.6%**	**35.4%**	**75.0%**	**50.0%**	**25.0%**	**48.0%**

Source: TIGTA analysis of SAAS audit trail data for November 2005.

Although we reviewed three SAAS audit trail files, the MODTRANS table is the primary audit trail table in the SAAS. Table 2 presents the results of our assessment of the data integrity for the MODTRANS table and displays only those records collected from that table. Currently, the MODTRANS table includes audit trail records of IRS employees; therefore, Table 2 lists only those modernized systems accessed by IRS employees.

Table 2: Percentage of Unusable Required Entries in the MODTRANS Table

Audit Trail Requirement	Field Name	MeF	e-Services	IFS	Other	Totals
Date and time of the event	TIMESTAMP	0.0%	0.0%	0.0%	0.0%	0.0%
The unique identifier initiating an action	USERID	0.0%	0.0%	0.0%	0.0%	0.0%
Type of event	EVENTID	7.1%	41.3%	0.0%	0.0%	28.7%
Origin of the request for identification/authentication events	SRCADDR	6.3%	37.6%	83.1%	0.0%	50.9%
Subject of event, action taken	VARDATA	30.6%	44.7%	100.0%	0.0%	61.1%
Identity of user creating the event	USERID	0.0%	0.0%	0.0%	0.0%	0.0%
Role of user, when creating the event	None	100.0%	100.0%	100.0%	100.0%	100.0%
Success or failure of the event	ERRORMSG	100.0%	100.0%	0.0%	100.0%	70.0%
Totals		**30.5%**	**40.5%**	**35.4%**	**25.0%**	**38.9%**

Source: TIGTA analysis of SAAS audit trail data for November 2005.

Because audit trail records from the other two tables, TAXFIL and REGUSER, are also important, Table 3 displays percentages of unusable audit trail records collected from these two tables. Table 3 lists only those modernized systems accessed by tax filers and registered users.

Table 3: Percentage of Unusable Required Entries in the TAXFIL and REGUSER Tables

Audit Trail Requirement	Field Name	MeF	e-Services	IRFOF	I-EIN	Totals
Date and time of the event	TIMESTAMP	0.0%	1.1%	0.0%	0.0%	0.6%
The unique identifier initiating an action	USERID	0.0%	20.0%	100.0%	100.0%	57.5%
Type of event	EVENTID	0.0%	57.3%	100.0%	0.0%	65.6%
Origin of the request for identification/authentication events	SRCADDR	0.0%	29.2%	100.0%	0.0%	50.6%
Subject of event, action taken	VARDATA	0.0%	55.9%	0.0%	100.0%	41.4%
Identity of user creating the event	USERID	0.0%	20.0%	100.0%	100.0%	57.5%
Role of user, when creating the event	None	100.0%	100.0%	100.0%	100.0%	100.0%
Success or failure of the event	ERRORMSG	100.0%	100.0%	100.0%	0.0%	88.3%
Totals		**25.0%**	**47.9%**	**75.0%**	**50.0%**	**57.6%**

Source: TIGTA analysis of SAAS audit trail data for November 2005.

Descriptive audit trail entries

In addition to the required entries, the SAAS audit trail can store descriptive information about a transaction, which is useful in the search for UNAX violations. The SAAS audit trail record has 15 places for these descriptive entries, which are listed in Table 4.

Table 4: MODTRANS Fields Providing Additional Details on User Transactions

Fields Detailing User Transactions	
DOLLARAMT	NAMECTRL
TAXFILERTIN	MFTCODE
TAXPERIOD	FILESRCCD
TAXFILFILESRC	CASESTATCD
TAXFILERINTYPE	CAMPUSCODE
REASONCODE	CAMPUSACCESS
PLANNUMBER	DLN
OUTPUTCODE	

Source: TIGTA analysis of SAAS audit trail data for November 2005.

Of these 15 fields, only the following include any information:

- DOLLARAMT: This field should include the dollar amount of a transaction. However, this field contains no actual dollar amounts.

- TAXFILERTIN: This field includes the Taxpayer Identification Number used in a transaction.

Table 5 lists the percentage of unusable TAXFILERTIN entries in the SAAS audit trail for those modernized systems using the TAXFILERTIN field. Those systems not included in audit trail records of one or more SAAS tables are labeled as not applicable (N/A).

Table 5: Percentage of Unusable TAXFILERTIN Entries in the SAAS Audit Trail

SAAS Audit Trail Table	MeF	e-Services	IRFOF	I-EIN	SAAS Totals
MODTRANS	100.0%	0.6%	N/A	N/A	1.5%
REGUSER	100.0%	6.0%	N/A	N/A	6.0%
TAXFIL	N/A	4.0%	2.0%	0.0%	2.0%
SAAS Totals	100.0%	8.3%	2.0%	0.0%	2.8%

Source: TIGTA analysis of SAAS audit trail data for November 2005.

Missing audit trail entries

Our analysis of SAAS audit trail records also identified thousands of missing audit trail records. Each SAAS audit trail record contains a unique, sequential identification number, which can be used to ensure all records are accounted for. We identified over 80,200 missing identification numbers, indicating the records associated with these numbers may be missing or are not identifiable from the SAAS. We identified over 3,400 corrupted audit records for which the identification number was overwritten or not in its proper place. Therefore, approximately 3,400 of the over 80,200 missing records may be in the SAAS but not identifiable due to the record corruption. However, there may be more missing records because not all audit trail records contained a unique identification number. Table 6 presents the applications for which these identification numbers were unusable.

Table 6: Percentage of Unusable Audit Trail Identification Numbers in the SAAS Audit Trail

Application	Percentage of Unusable or Missing Audit Trail Identification Numbers
MeF	32.2%
e-Services	42.1%
IFS	0.0%
IRFOF	100.0%
I-EIN	0.0%
Other	0.0%
SAAS Total	43.0%

Source: TIGTA analysis of SAAS audit trail data for November 2005.

Appendix V

Management's Response to the Draft Report

RECEIVED
SEP 25 2006

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

CHIEF
MISSION ASSURANCE AND SECURITY SERVICES

September 22, 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Response to Draft Audit Report – Improvements Are Needed to Ensure That Use of Modernization Applications Is Effectively Audited (Audit #200620003)

Thank you for the opportunity to review the subject draft audit report, dated September 7, 2006. The IRS acknowledges its challenges in the area of Audit Trails and is rigorously addressing our deficiencies. The Operational Information Technology Security Council has tasked the Audit Trails Working Group to provide an enterprise solution that aligns with the strategies outlined in our Computer Security Material Weakness Plan, as well as the proposed improvements to the Security Audit and Analysis System (SAAS).

The SAAS is the cornerstone of our automated audit trail systems, and currently SAAS provides taxpayer systems audit trail data and reports to personnel in the TIGTA Office of Investigations, the Computer Security Incident and Response Center (CSIRC), and some business units with plans to include them all. We are improving the quality of data sent to SAAS by our Modernized systems, as recommended in your report, and through a partnership with our PRIME contactor we have developed a SAAS Improvement Plan, broken into a set of nine discrete Work Segments. We are pleased the report recognizes the SAAS improvements efforts that are currently underway, and we appreciate your focused recommendations for additional improvements.

We concur with all five report recommendations that address a review process of audit trails in the Customer Account Data Engine (CADE), a retention policy for audit trails in CADE, re-assessing the requirements for SAAS audit trails, modifying modernized audit trails to comply with SAAS standards, and re-evaluating SAAS procedures and processes.

In conjunction with the Chief Information Officer, we are working to implement corrective actions to resolve the reported deficiencies. Attached is a detailed response outlining our corrective action plans for each report recommendation. We appreciate your continued support and valuable oversight assistance. If you have any questions, please contact me at (202) 622-8910, or Devon Bryan, Director, Information Technology Security, at (202) 283-7271.

Attachment

Management response to Draft Audit Report – Improvements Are Needed to Ensure That Use of Modernization Applications Is Effectively Audited (Audit # 200620003)

RECOMMENDATION #1:

To ensure Customer Account Data Engine (CADE) audit trails are reviewed, the Chief, Mission Assurance and Security Services, should establish a review process for CADE audit trails. Such a process will not only aid in current reviews, but also position the IRS to perform future reviews when the amount of taxpayer information residing in the CADE is significantly larger.

CORRECTIVE ACTION TO RECOMMENDATION #1:

Mission Assurance and Security Services' Information Technology Security Directorate will establish an enterprise process for reviewing the audit trails of all IRS legacy and modernized applications and systems, including CADE audit trails.

IMPLEMENTATION DATE:

October 15, 2007

RESPONSIBLE OFFICIAL:

Director, Information Technology Security, Mission Assurance and Security Services, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:

Implementation will be monitored through monthly Program Reviews conducted by the Director, Information Technology Security, Mission Assurance and Security Services.

1

Management response to Draft Audit Report – Improvements Are Needed to Ensure That Use of Modernization Applications Is Effectively Audited (Audit # 200620003)

RECOMMENDATION #2:

To ensure Customer Account Data Engine (CADE) audit trails are sufficiently retained, the Chief, Mission Assurance and Security Services, and the Acting Chief Information Officer should establish a viable retention policy for CADE audit trails, mirroring, where possible, that of other systems with taxpayer information.

CORRECTIVE ACTION TO RECOMMENDATION #2:

Mission Assurance and Security Services' Information Technology Security Directorate, in conjunction with the Chief Information Office, will establish a viable retention policy for CADE audit trails that is consistent with established IRS policies governing, records management and retention standards for systems with taxpayer information.

IMPLEMENTATION DATE:

July 15, 2007

RESPONSIBLE OFFICIAL:

Director, Information Technology Security, Mission Assurance and Security Services, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:

Implementation will be monitored through monthly Program Reviews conducted by the Director, Information Technology Security, Mission Assurance and Security Services.

2

Management response to Draft Audit Report – Improvements Are Needed to Ensure That Use of Modernization Applications Is Effectively Audited (Audit # 200620003)

RECOMMENDATION #3:

To ensure the Security Audit and Analysis System (SAAS) can better meet the needs of its customers and audit trail data reported are reliable, accurate, and complete, the Chief, Mission Assurance and Security Services, should re-assess the requirements for SAAS audit trails, including identifying all user requirements and the resulting SAAS system requirements needed to achieve them. Once the re-assessment is complete, requirements should then be assigned a release milestone to provide a timetable for completion. The re-assessment process must include requirements to addresses the following controls:

- Additional validity tests to ensure audit trail data received are reliable and accurate.
- Controls to ensure all audit trail records are uniquely identifiable and completeness tests to ensure all audit records are accounted for.
- Reports and queries to aid in the analysis of audit trail records that failed validity tests.
- Functionality for review and certification of employee access to taxpayer information, similar to the functions available through the IDRS On-Line Reports Services application.
- Consolidated Solaris audit files to be available for inclusion in the SAAS audit trail. To do this, technical issues preventing these files from being incorporated into the SAAS need to the resolved. Until the issues are resolved, these files should be retained.
- Retention period for source audit trail files sent from modernized systems to ensure files are kept for a necessary length of time.

CORRECTIVE ACTION TO RECOMMENDATION #3:

Mission Assurance and Security Services' Information Technology Security Directorate will re-assess the requirements for SAAS audit trails, including identifying all user requirements and the resulting SAAS system requirements needed to achieve them.

IMPLEMENTATION DATE:

April 15, 2007

3

Management response to Draft Audit Report – Improvements Are Needed to Ensure That Use of Modernization Applications Is Effectively Audited (Audit # 200620003)

RESPONSIBLE OFFICIAL:

Director, Information Technology Security, Mission Assurance and Security Services, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:

Director, Information Technology Security, will develop a project plan that includes requirements identification, documentation and allocation to a release.

Management response to Draft Audit Report – Improvements Are Needed to Ensure That Use of Modernization Applications Is Effectively Audited (Audit # 200620003)

RECOMMENDATION #4:

To ensure modernized systems send reliable, accurate, and complete audit trail information to the Security Audit and Analysis System (SAAS), the Acting Chief Information Officer should modify modernized system audit trails to comply with SAAS standards, ensuring valid data are collected and arranged in the proper format. This process should include the solicitation of input from user organizations, such as IRS business units, the TIGTA, and the CSIRC, to identify their audit trail data needs.

CORRECTIVE ACTION TO RECOMMENDATION #4:

The IRS will provide a Project Plan that includes development of Change Requests for modification of Modernization's Applications to provide Audit Trail data to, and in the correct format for, SAAS based on requirements identified in the corrective action for Recommendation #3. The Project Plan will include expected implementation dates for each Modernization Application and will be based on funding and resource availability. The foundation of this Project Plan will be the incremental nature of the changes that IRS will begin implementing based on requirements which have already been documented and agreed to by Mission Assurance & Security Services, MITS and TIGTA. Additional improvements will continue to be made as additional audit trail requirements are developed and baselined. While IRS plans to make incremental changes as mentioned above, we cannot commit to completion of all actions until the final requirements are baselined in April 2007.

Modifying the modernized system audit trials is to be completed within 18 months following receipt of the final SAAS baselined requirements.

IMPLEMENTATION DATE:

October 15, 2008

5

Management response to Draft Audit Report – Improvements Are Needed to Ensure That Use of Modernization Applications Is Effectively Audited (Audit # 200620003)

RESPONSIBLE OFFICIAL:

Director, Infrastructure Architecture & Engineering, CIO, OS:CIO:ES:AE

CORRECTIVE ACTION MONITORING PLAN:

Monitoring will be conducted through the implementation plan and schedule.

Management response to Draft Audit Report – Improvements Are Needed to Ensure That Use of Modernization Applications Is Effectively Audited
(Audit # 200620003)

RECOMMENDATION #5:

To ensure the Security Audit and Analysis System (SAAS) can better meet the needs of its customers and audit trail data reported are reliable, accurate, and complete, the Chief, Mission Assurance and Security Services, should after completion of the requirements re-assessment, re-evaluate SAAS procedures and processes to ensure that new SAAS requirements are incorporated and responsibilities for reviewing modernization audit trails are adequately defined. These procedures should include reviews for audit trail records that failed validity tests and transactions by tax filers and registered users.

CORRECTIVE ACTION TO RECOMMENDATION #5

Once SAAS requirements are re-assessed, Mission Assurance and Security Services' (MA&SS) Information Technology Directorate will establish procedures to ensure that audit trails are properly reviewed. MA&SS' Information Technology Directorate will also assign staff to monitor failed audit trail records.

IMPLEMENTATION DATE:

April 15, 2008

RESPONSIBLE OFFICIAL:

Director, Information Technology Security, Mission Assurance and Security Services, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:

Implementation will be monitored through monthly Program Reviews conducted by the Director, Information Technology Security, Mission Assurance and Security Services.

7