The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning

August 2004

Reference Number: 2004-20-135

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 18, 2004

MEMORANDUM FOR CHIEF, MISSION ASSURANCE

Gordon C. Milbourn III

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

SUBJECT: Final Audit Report - The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning (Audit # 200420026)

This report represents the results of our review of the Internal Revenue Service's (IRS) audit trail system for modernized projects. The overall objective of this review was to assess the availability of audit trail data used to monitor computer activity on the IRS' modernized systems.

In summary, the Security Audit and Analysis System (SAAS) represents the IRS' solution for audit trail collection and review for both modernized computer systems and the Integrated Data Retrieval System.[1] The PRIME contractor[2] developed the SAAS as part of the IRS' modernization efforts. Conceptually, the SAAS is intended to gather audit trail information from IRS systems and store this information in a central database that IRS management, computer incident response team members, and Treasury Inspector General for Tax Administration (TIGTA) investigators could access. The SAAS is intended to enable these users to generate reports and create custom queries to detect unauthorized activities and facilitate the reconstruction of events if unauthorized activities occurred.

[1] The IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records.
[2] 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.

Currently, the SAAS contains audit trail information from the IRS' e-Services[3] and Internet Refund Fact of Filing[4] modernized applications. Additionally, it contains data from the Audit Trail Lead Analysis System used by the TIGTA to detect and investigate unauthorized accesses to taxpayer information (UNAX)[5] by IRS employees.

However, software performance and functionality problems with the SAAS have prevented users from accessing the SAAS data once it has been collected. In November 2002, the PRIME contractor delivered the SAAS to the IRS. The IRS was aware that the SAAS did not meet IRS requirements but formally accepted the system with the caveat that the system deficiencies were to be addressed. To date, the problems have not been fully resolved. The IRS should not have accepted the SAAS, knowing that the system did not meet all the software performance and functionality requirements of its users.

As a result, the ability to detect improper activity on IRS computer systems has been diminished. Specifically:

- IRS business units cannot use the SAAS for identifying questionable activities on modernized applications.
- The IRS' Computer Security Incident Response Center cannot use the SAAS for identifying unauthorized intrusions.
- The TIGTA cannot use the SAAS for identifying UNAX violations.

Business unit managers of modernized applications are primarily responsible for identifying questionable activities on their applications. However, operating procedures for reviewing SAAS data for modernized applications have not been developed. The Office of Mission Assurance, as the business leader of the SAAS, did not actively assist and facilitate requirements until January 2004. As a result, even if the SAAS were functioning as intended, the IRS would not be able to effectively review audit trail data.

Without a functioning audit trail process, the IRS' ability to detect unauthorized activities on its current modernized systems is lessened. Future modernization applications will rely solely on the audit trail functions provided through the SAAS. The inability to detect unauthorized activities is a significant security risk that should weigh heavily on whether future modernization applications should be accredited and implemented. Not having operating procedures, problems with software performance and functionality, and delays in addressing software problems collectively indicate that the IRS has not devoted sufficient attention to the review of audit trails.

---

[3] Provides electronic products and services for specific customer segments (e.g., application for preparer tax identification number and registration for electronic return originators).

[4] Provides refund status information to taxpayers with Internet access and guidance to the taxpayers about what steps to follow to resolve issues with their refunds.

[5] Unauthorized access and inspection of returns and return information as established in the Taxpayer Browsing Protection Act, 26 U.S.C.A. §§ 7213, 7213A, 7431 (West Supp. 2003).

We recommended that the Chief, Mission Assurance, ensure the SAAS performance and functionality requirements are adequately tested and implemented to perform query and report generation. Also, SAAS operational procedures (e.g., who will review audit trails, what information is needed, and for what purpose) should be fully developed and finalized so that business units can conduct audit trail reviews of system and user activities in modernized applications. In addition, periodic compliance reviews should be conducted to ensure business units carry out their roles and responsibilities to review audit trails, and alternatives should be developed for reviewing audit trails for modernized applications in the event the SAAS deficiencies cannot be corrected.

Management's Response: Management concurred with three of our recommendations and partially concurred with one recommendation. The Office of Mission Assurance will participate in testing the SAAS to help ensure that audit trail information is available and retrievable to detect unauthorized activities, provide operating procedures to help business owners analyze SAAS information, monitor compliance with operating procedures, and enhance its certification procedures for systems and applications to ensure that audit trail procedures are available.

Management partially agreed with our recommendation to develop alternatives for modernized applications audit trails in the event that SAAS deficiencies cannot be corrected. The IRS is committed to ensuring that the SAAS contains the necessary storage and processing capability to allow users to retrieve and analyze information. However, if necessary, the IRS will consider alternative approaches for identifying unauthorized access and intrusion detection for modernization applications that may not contain taxpayer information. Management's complete response to the draft report is included as Appendix V.

Office of Audit Comment: We are hopeful that the IRS meets its new goal for making the SAAS functional by October 2004. However, if delays persist, we would encourage the IRS to begin looking for alternatives to the SAAS. While we still believe our recommendation is worthwhile, we do not intend to elevate our disagreement concerning it to the Department of the Treasury for resolution.

Although the Chief, Mission Assurance, agreed with most of our recommendations, the response stated that the SAAS met all defined requirements and passed all tests. As we noted in the report, the IRS accepted the SAAS in November 2002, although it was aware that reports for detecting unauthorized access could not be generated in a production environment. Later in the response, the Chief, Mission Assurance, recognized that the SAAS is not expected to be functional until October 2004.

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

The Security Audit and Analysis System Was Accepted Although It Did Not Meet Performance Requirements ..... Page 2

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

Procedures for Reviewing Audit Trails on the Security Audit and Analysis System Have Not Been Developed ..... Page 6

Recommendations 3 and 4: ..... Page 7

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 8

Appendix II – Major Contributors to This Report ..... Page 9

Appendix III – Report Distribution List ..... Page 10

Appendix IV – Outcome Measures ..... Page 11

Appendix V – Management's Response to the Draft Report ..... Page 12

The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning

Background

Even the best controls designed to prevent improper computer activity can be circumvented with the proper expertise. Hackers, and particularly disgruntled employees and contractors who already have access to a system, may attempt to circumvent the Internal Revenue Service (IRS) controls to gain access to sensitive information or to vandalize computer data and processing. To help minimize these risks, Federal Government agencies are required to run and review audit trails routinely to detect improper activity.

The Department of the Treasury procedures require that audit trails be sufficient in detail to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected. These procedures also state that designated personnel must review audit trails at least weekly for systems that contain sensitive information. The IRS' procedures require that, at a minimum, audit trails must include sufficient information to establish what events occurred, when the events occurred, and who (or what) caused them.

Conceptually, the Security Audit and Analysis System (SAAS) was intended to meet the IRS' audit trail needs for both modernized computer systems and the Integrated Data Retrieval System (IDRS).[1] The SAAS was to collect key information necessary to detect improper activities and to reconstruct events for potential criminal investigations and store it in a central database warehouse so that authorized users could generate reports and create custom queries.

The PRIME contractor[2] developed the SAAS for the IRS. The intended users of the SAAS include:

- IRS management to review questionable activities on its systems.
- The IRS' Computer Security Incident Response Center (CSIRC) to detect and respond to computer security

[1] IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records.
[2] 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.

incidents targeting the IRS' enterprise information technology assets.

- The Treasury Inspector General for Tax Administration (TIGTA) to detect and investigate unauthorized accesses to taxpayer information (UNAX)[3] by IRS employees. Although the TIGTA is a user of the SAAS system, IRS management is primarily responsible for the review and analysis of audit trail information.

This review was performed in the Offices of the Chief Information Officer and the Chief, Mission Assurance, at the IRS National Headquarters and in New Carrollton, Maryland, during the period December 2003 through March 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.

The Security Audit and Analysis System Was Accepted Although It Did Not Meet Performance Requirements

In November 2002, the PRIME contractor delivered the SAAS to the IRS. The SAAS is collecting and storing audit trail information from some IRS applications into the database warehouse.

A number of these records are from the Audit Trail Lead Analysis System (ATLAS) that obtains and analyzes audit trail information from the IDRS. The SAAS also contains audit trail information from the IRS' e-Services[4] and Internet Refund Fact of Filing (IRFoF)[5] modernized applications and audit trails from various security devices (e.g., firewalls and intrusion detection systems). As of January 2004, the database warehouse contained an estimated 9 billion records.

[3] Unauthorized access and inspection of returns and return information as established in the Taxpayer Browsing Protection Act, 26 U.S.C.A. §§ 7213, 7213A, 7431 (West Supp. 2003).
[4] Provides electronic products and services for specific customer segments (e.g., application for preparer tax identification number and registration for electronic return originators).
[5] Provides refund status information to taxpayers with Internet access and guidance to the taxpayers about what steps to follow to resolve issues with their refunds.

However, none of the users can query the information and generate reports because of SAAS software performance and functionality problems. The IRS was aware that the SAAS did not meet IRS requirements but formally accepted the system with the caveat that the system deficiencies were to be addressed. Specifically, the IRS noted that the SAAS could not yet produce reports currently available in the ATLAS and that query response times would have to match the ATLAS response times. The IRS should not have accepted the SAAS, knowing that the system did not meet all the software performance and functionality requirements of its users.

The functionality and software performance problems of the SAAS prevent the IRS business units from using it for identifying questionable activities on modernized applications.[6] New applications such as e-Services and IRFoF are highly sensitive since the applications will allow taxpayers and practitioners access to tax account information. Without a review of audit trail data, suspicious activities could go undetected on these systems.

Future modernization applications will also rely on the audit trail functions provided through the SAAS. Not having an effective audit trail review process is a significant security weakness that should weigh heavily on whether to accredit future modernization applications. Examples of applications that will provide key tax administration processes in the future include the Customer Account Data Engine,[7] Custodial Accounting Project,[8] and the Integrated Financial System.[9]

In addition, the functionality and software problems of the SAAS prevent the CSIRC from using it for identifying

---

[6] The IRS has hundreds of legacy systems where little has been done in the past to identify suspicious activities by reviewing audit trail data. Audit trail data from these systems has not been provided to the SAAS, and the IRS has no plans to do so.

[7] Intended to provide an online modernized data infrastructure to house authoritative taxpayer account and return information.

[8] Intended to provide the IRS a data warehouse of detailed taxpayer account information used for analysis and financial reporting.

[9] Intended to integrate the majority of IRS' internal financial management processes to better budget, plan, track, report, and manage finances.

unauthorized intrusions. The CSIRC is responsible for identifying unauthorized intrusions into the IRS' computer system. Currently, it carries out this responsibility by reviewing audit trails from various systems and security devices.

To enhance its ability to detect unauthorized intrusions, the CSIRC had planned to store intrusion detection system logs from multiple locations on the SAAS. However, functionality and software performance problems prevent the CSIRC from querying the intrusion detection data on the SAAS.

The PRIME contractor was not aware of this problem until almost a year after it delivered the SAAS because the CSIRC had not submitted a help-desk ticket describing the problems in accessing the database warehouse. Apparently, the CSIRC had not been using the SAAS since the November 2002 system delivery date.

The SAAS software performance and functionality problems also prevent the TIGTA from using the SAAS for identifying UNAX violations. The ATLAS was developed to obtain and analyze audit trail information from the IRS' most used legacy system (IDRS) for updating and maintaining taxpayer accounts. The TIGTA's Office of Investigations (OI) is the primary user of the ATLAS and uses it to identify potential unauthorized accesses of taxpayer information by IRS employees. Once the SAAS became functional, the IRS had planned to discontinue its use of the ATLAS.

However, the ATLAS is aging and, in the interim, significant funds must be expended to keep the system operational until the SAAS can become functional. The IRS contracted for hardware maintenance support covering Fiscal Years 2004 through 2006 for the ATLAS totaling approximately $584,000. Additionally, the IRS has allocated 2 employees in its spending plans for Fiscal Years 2004 and 2005, representing approximately $400,000 in labor costs, to maintain the ATLAS (see Appendix IV for details on these costs). If the ATLAS fails, the TIGTA would lose its primary system for identifying unauthorized accesses by IRS employees. However, once the SAAS

becomes operational, the resources expended to maintain the ATLAS can be used to support other IRS initiatives.

Since the SAAS was accepted and deployed by the IRS, the TIGTA OI, with strong support from the Office of Mission Assurance, has continued to report its inability to use the SAAS. Numerous meetings have since been held with the PRIME contractor and the IRS to discuss this issue.

Recommendations

The Chief, Mission Assurance, should ensure:

1. The SAAS performance and functionality requirements are adequately tested and implemented so that the IRS and the TIGTA can perform queries and generate audit trail reports.

Management's Response: Management agreed with this recommendation. The IRS and the PRIME contractor have developed a schedule that includes requirements for testing and evaluating audit trail capabilities for the IDRS and modernized applications. Testing for modernized application audit trails is scheduled to begin in August 2004 and be completed by October 31, 2004. The Office of Mission Assurance will participate in the testing to help ensure that users can access and retrieve audit trail information.

2. Alternatives are developed for reviewing audit trails for modernized applications in the event the SAAS deficiencies cannot be corrected.

Management's Response: Management partially agreed with our recommendation. The IRS maintained it has conducted sufficient testing to accept that the current SAAS approach is an effective approach for supporting Security and Business Organization requirements for identifying unauthorized access and intrusion detection. However, if necessary, management will consider alternative approaches for reviewing modernized applications that do not contain taxpayer information. The IRS is ready to commit additional resources to ensure the success of the SAAS.

Office of Audit Comment: We are hopeful that the IRS meets its new goal for making the SAAS functional by

October 2004. However, if delays persist, we would encourage the IRS to begin looking for alternatives to the SAAS.

Procedures for Reviewing Audit Trails on the Security Audit and Analysis System Have Not Been Developed

To date, procedures for audit trail reviews using the SAAS have not been finalized beyond the general security policies, roles, and responsibilities. In addition, specific roles and responsibilities (i.e., who will use the application, for what information, and for what purpose) have not yet been established.

At the time the SAAS was deployed, the PRIME contractor advised the IRS that many of the procedures for using the SAAS were not clear. The transition plan provided by the PRIME contractor identified necessary steps the IRS needed to take.

One step called for the IRS to "review, revise/establish security processes, policies and procedures." The IRS responded, "… security policies are in place" and provided no more support for this effort. The PRIME contractor also indicated that the IRS' current policies and procedures did not provide the details necessary to adequately analyze audit trails.

The PRIME contractor also indicated that ownership responsibilities for SAAS functions such as collecting audit trail data, generating and reviewing security reports, and determining who should have access to the SAAS had not been defined.

Business unit managers of modernized applications are primarily responsible for identifying questionable activities on their applications. However, to ensure consistency and that security requirements are met, the Office of Mission Assurance (the business leader of the SAAS) should take an active role by facilitating requirements analysis and definition, and defining policy, roles, and responsibilities.

As a result of the delays in defining operating procedures, the IRS business units still will not be in a position to effectively review audit trails, even if the SAAS performance issues are fully resolved. During our review, in January 2004, the Office of Mission Assurance provided additional procedures for certain manager reports and

acknowledged that additional procedures for modernized applications still need to be defined.

Not having operating procedures, problems with software performance and functionality, and delays in addressing software problems collectively indicate that the IRS has not devoted sufficient attention to the review of audit trails. Consequently, improper activities on IRS modernized applications could go undetected.

Recommendations

The Chief, Mission Assurance, should ensure:

3. The SAAS operating procedures (e.g., who will review audit trails, what information is needed, and for what purpose) are fully developed and finalized so that business units can conduct effective and efficient audit trail reviews of modernized applications.

Management's Response: IRS management agreed with this recommendation. The Office of Mission Assurance is implementing a two-phased plan to provide business organizations and security personnel access to modernized applications audit trail data through the SAAS and will identify procedures in conjunction with business owners to help ensure that unauthorized activities are detected. The Office of Mission Assurance will also enhance its certification procedures for systems and applications to ensure that audit trail procedures are available.

4. Periodic compliance reviews are conducted once the SAAS is functional to ensure the CSIRC and business unit managers carry out their roles and responsibilities to review audit trails.

Management's Response: IRS management agreed with this recommendation. The Office of Mission Assurance will initiate compliance reviews on modernized applications within 120 days of their initial operating capability dates. According to current schedules, these reviews are scheduled to begin in March 2005.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the availability of audit trail data used to monitor computer activity on the Internal Revenue Service's (IRS) modernized systems. To accomplish the objective, we:

I. Determined whether the IRS had a system in place to monitor modernized systems and whether the system collected sufficient data.

   A. Reviewed and evaluated the IRS policies, procedures, and documentation, including documentation prepared by the PRIME contractor[1] applicable to the Security Audit and Analysis System (SAAS).[2]

   B. Identified information that should be captured in audit trails and determined if modernized systems currently in production were collecting the appropriate audit trail data.

   C. Determined whether any mitigating controls were in place for audit trails on modernized systems.

II. Determined whether audit trails were being monitored to detect improper activities by employees, contractors, and registered/unregistered users.

   A. Interviewed the SAAS project manager and planned users of the SAAS and identified user efforts to use the SAAS for its intended purposes.

   B. Determined whether modernized audit trails were being reviewed using the SAAS and whether any improper activity was identified using the system.

[1] 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.

[2] Conceptually, the SAAS was intended to meet the IRS' audit trail needs for both modernized computer systems and the Integrated Data Retrieval System (the IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer's account records).

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
Theodore W. Grolimund, Audit Manager
David J. Brown, Senior Auditor
Anthony D. Knox, Senior Auditor
Louis Lee, Senior Auditor
George L. Franklin, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Information Officer OS:CIO
Associate Chief Information Officer, Business Systems Modernization OS:CIO:B
Associate Chief Information Officer, Information Technology Services OS:CIO:I
Director, Internal Management Systems OS:CIO:I:B:IM
Acting 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, Mission Assurance OS:MA
- Associate Chief Information Officer, Business Systems Modernization OS:CIO:B
- Manager, Program Oversight and Coordination Office OS:CIO:R:PM

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to the Congress.

Type and Value of Outcome Measure:

- Funds Put to Better Use – Potential; $584,372 (see page 2).

Methodology Used to Measure the Reported Benefit:

During our review we noted that the Audit Lead Analysis System (ATLAS) was to be replaced by the Security Audit and Analysis System (SAAS). Since the SAAS is not functioning as intended, the Internal Revenue Service (IRS) has had to contract[1] for hardware maintenance support covering Fiscal Years 2004 through 2006 for the ATLAS.

ATLAS Hardware Maintenance Costs:

Fiscal Year 2004	$181,770
Fiscal Year 2005	$194,494
Fiscal Year 2006	$208,108
Total	$584,372

Once the SAAS becomes operational, the funds expended to maintain the ATLAS could be used to support other IRS initiatives.

Type and Value of Outcome Measure:

- Inefficient Use of Resources – Potential; $400,000 (see page 2).

Methodology Used to Measure the Reported Benefit:

During our review we noted that the ATLAS was to be replaced by the SAAS. Since the SAAS is not functioning as intended, the IRS has allocated 2 full-time equivalent (FTE)[2] employees ($200,000 in labor costs) in its spending plans for Fiscal Years 2004 and 2005 to continue the support of the ATLAS. This represents a total of $400,000 ($200,000 * 2) in labor costs for the 2 years. Once the SAAS becomes operational, the employee resources expended to maintain the ATLAS could potentially be used to support other IRS initiatives.

[1] Source: IRS Contract Number NK20188090.
[2] A measure of labor hours in which 1 FTE is equal to 8 hours multiplied by the number of compensable days in a particular fiscal year. For example, in Fiscal Year 2004, 1 FTE is equal to 2,096 staff hours.

Appendix V

Management's Response to the Draft Report

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

RECEIVED
AUG 06 2004

CHIEF
MISSION ASSURANCE

August 5, 2004

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: Daniel Galik Daniel Galik
Chief, Mission Assurance

SUBJECT: Response to Draft Audit Report – The Audit Trail System For Detecting Improper Activities on Modernized Systems Is Not Functioning (Audit # 200420026)

This is in response to the draft report entitled "The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning." We are attaching a detailed response to each of the four report recommendations addressing the Security Audit and Analysis System (SAAS). We concur with three of the recommendations and partially concur with the other.

However, we would like to provide further clarification to the following observation in your report which states "The IRS was aware that SAAS did not meet IRS requirements but formally accepted the system anyway with the caveat that the system deficiencies were to be addressed. To date, the problems have not been fully resolved. The IRS should not have accepted the SAAS, knowing that the system did not meet all the software performance and functionality requirements of its users." Specifically, SAAS was developed as a major component of the Infrastructure Shared Services modernized system to support IRS requirements to review audit trails and logs, and to detect unauthorized activities or intrusions on IRS applications and networks.

Moreover, SAAS passed PRIME Integration Test & Deployment Testing, System Acceptance Testing, and Security testing. The SAAS met all defined requirements and passed all tests. In addition, the IRS was aware that SAAS did not duplicate all of the functionality currently provided by ATLAS and to do so was inconsistent with the intended purpose of SAAS. The purpose of SAAS was to allow users to write their own queries against the data. Also, the Security Technology Infrastructure Release (including SAAS) was approved within the Business Systems Modernization governance process (which includes the SAAS business owner) with unconditional approval. In summary, SAAS met all defined user requirements as documented. The SAAS was tested to ensure all requirements were met.

We discussed with your audit team that the software performance and functionality problems were being addressed in the Development, Integration and Testing Environment at the time of this audit and at the request of the business owner. At the end of your audit, the corrections were being moved into production. The SAAS

performance issues have been corrected in the SAAS Test environment. The SAAS datamart solution corrects the performance problem. Improved SAAS performance was demonstrated in the SAAS Test environment. The solution is being promoted to the SAAS production environment for Customer Acceptance Testing.

Since 2003, IRS and PRIME have worked together to ensure the security requirements are properly addressed and have made significant progress in supporting reviews of the Integrated Data Retrieval System (IDRS) and in modernized application audit trails. IRS expects to have the three components of SAAS --IDRS audit trails, modernized application audit trails, and CSIRC audit logs functioning by October 2004.

We agree with your report recommendations # 1, 3, and 4 that state the Chief, Mission Assurance should ensure the SAAS performance and functionality requirements are adequately tested and implemented, SAAS operating procedures are fully developed and Mission Assurance should ensure periodic compliance reviews are conducted. These activities have been the responsibility of Mission Assurance and will continue until SAAS matures into a fully implemented application.

We partially agree with your report recommendation # 2 that states Mission Assurance should ensure that alternatives are developed for reviewing audit trails for modernized applications. We agree that IRS may need to consider alternative approaches for reviewing modernized applications that do not contain taxpayer information. However, IRS is committed to ensuring that SAAS supports both the business and security requirements for sensitive systems. This commitment is justified because of the extensive testing performed by IRS and Prime.

If you have any questions, please contact me at (202) 622-8910 or Richard A. Stone, Acting Deputy Director, Assurance Programs, at (202) 283-4806.

Attachment

Management response to Draft Audit Report –The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning (Audit # 200420026)

RECOMMENDATION # 1: The Chief, Mission Assurance, should ensure that the SAAS performance and functionality requirements are adequately tested and implemented so that the IRS and the TIGTA can perform queries and generate audit trail reports.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The IRS and Prime have developed a SAAS tasking schedule that includes requirements for testing and evaluating audit trail capabilities for IDRS and modernization applications. Mission Assurance will participate in the testing to help ensure that user requirements are successful for access to and retrieval of audit trail information to support business organization and security needs to detect unauthorized activities. Testing for modernized application audit trails is scheduled to begin in August 2004 with a proposed completion date of October 31, 2004.

IMPLEMENTATION DATE:

October 31, 2004

RESPONSIBLE OFFICIAL:

Associate CIO Business Systems Modernization (OS:CIO:B)

CORRECTIVE ACTION MONITORING PLAN:

Mission Assurance will monitor the results of testing activities and will have final sign-off to ensure that all testing meets security and business customer requirements.

Management response to Draft Audit Report – The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning (Audit # 200420026)

RECOMMENDATION # 2: The Chief, Mission Assurance, should ensure that alternatives are developed for reviewing audit trails for modernized applications in the event the SAAS deficiencies cannot be corrected.

CORRECTIVE ACTION TO RECOMMENDATION #2:

We partially concur. The IRS has conducted sufficient testing to accept that the current SAAS approach is an effective approach for supporting Security and Business Organization requirements for identifying unauthorized access and intrusion detection. If necessary, IRS will consider alternative approaches for modernization applications that may not contain taxpayer information. However, IRS is ready to commit additional resources to help ensure that SAAS contains the necessary storage and processing capability to effectively allow SAAS users to retrieve and analyze audit trail information.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance

CORRECTIVE ACTION MONITORING PLAN:

N/A

Management response to Draft Audit Report — The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning (Audit # 200420026)

RECOMMENDATION # 3: The Chief, Mission Assurance, should ensure that the SAAS operating procedures (e.g., who will review audit trails, what information is needed, and for what purpose) are fully developed and finalized so that business units can conduct effective and efficient audit trails and reviews of modernized applications.

CORRECTIVE ACTION TO RECOMMENDATION #3:

Mission Assurance has developed requirements to support SAAS users' ability to retrieve and analyze modernized application audit trails. Phase 1, will provide business organizations and security staffs access to modernized applications audit trails and is expected to be completed by September 2004. For Phase 2, as appropriate, additional requirements for enhanced access to SAAS modernized applications will be implemented by April 2005. Mission Assurance will identify operating procedures in conjunction with the business owners to help ensure that unauthorized activities are detected.

Mission Assurance and the Business organizations must identify internal staff who will be responsible for performing reviews, and for reporting any suspicious activities to TIGTA. Mission Assurance staff will assist in performing monitoring and oversight activities to help ensure that audit trail reviews are being performed and that potential unauthorized activity is reported to the appropriate investigative sources.

Mission Assurance also will enhance its certification process for systems/applications to help ensure that modernized application owners have identified procedures to detect potentially inappropriate activity that users can perform. Business organizations will be responsible for implementing procedures to detect and/or prevent such activities. To the extent that the audit trails can be used as a detection method, business organization reviewers should look for inappropriate activities.

IMPLEMENTATION DATE:

A) Phase 1 - September 30, 2004
B) Phase 2 – April 30, 2005

RESPONSIBLE OFFICIAL:

A) Chief, Mission Assurance (OS:MA)
B) Chief, Mission Assurance (OS:MA)

CORRECTIVE ACTION MONITORING PLAN:

Security and Privacy documentation for the modernized applications will be updated to ensure that all current and future application owners have included requirements for audit trails to be reviewed regularly in accordance with the importance of identifying unauthorized activities.

Management response to Draft Audit Report – The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning (Audit # 200420026)

RECOMMENDATION # 4: The Chief, Mission Assurance, should ensure that periodic compliance reviews are conducted once the SAAS is functional to ensure that CSIRC and business unit managers carry out their roles and responsibilities to review audit trails.

CORRECTIVE ACTION TO RECOMMENDATION #4:

Mission Assurance agrees that part of its responsibility is to perform periodic compliance reviews of business organizations whose users are accessing modernized applications with audit trail data included on SAAS. Such reviews will determine whether business organizations are properly adhering to requirements and procedures to appropriately review and analyze audit trail data in accordance with certification requirements.

Because CSIRC's role is to detect unauthorized intrusions, their activities focus on audit logs from various security devices rather than on modernized application audit trails. CSIRC does not review the modernized application audit trails, but has been working with Prime to help ensure that its staff has access to the Log File Collector that is accumulating firewall and system intrusion activities. Mission Assurance internal reviews will assess how effectively CSIRC can assess and use SAAS data in performing its mission.

Mission Assurance will initiate compliance reviews of modernized applications within 120 days of their initial operating capability dates. Based on current schedules these reviews are expected to begin by March 2005.

IMPLEMENTATION DATE:

March 31, 2005

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance (OS:MA)

CORRECTIVE ACTION MONITORING PLAN:

As modernization applications are certified and implemented, Mission Assurance will incorporate requirements for its staff to perform compliance reviews of these applications.