Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems

August 2005

Reference Number: 2005-20-128

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.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

August 26, 2005

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

Pamela J Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems (Audit # 200420029)

This report presents the results of our review to evaluate the Internal Revenue Service's (IRS) process for incorporating computer security controls into modernization systems. Currently, the IRS has a unique opportunity during its systems modernization efforts to develop and integrate adequate security controls effectively and efficiently. Many of its core systems are being rebuilt under the Business Systems Modernization efforts. As such, security controls should be provided during the development phase[1] of the Enterprise Life Cycle (ELC)[2] and tested during the integration phase.[3]

We judgmentally selected and reviewed the e-Services, Internet Refund Fact of Filing, Modernized e-File, Custodial Accounting Project, and Customer Account Data Engine (CADE) modernization projects. Appendix V provides a description of these systems.

In summary, the Mission Assurance and Security Services (MA&SS) organization, the Business Systems Modernization Office (BSMO), and the PRIME contractor[4] are

[1] The development phase includes the analysis, design, acquisition, modification, construction, and testing of the components of a business solution. This phase also includes routine planned maintenance of applications.

[2] The ELC establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduce the risks of system development and ensures alignment with the overall business strategy. All IRS personnel and contractors involved in the modernization effort are required to follow the ELC. See Appendix IV for additional details about the ELC.

[3] The integration phase includes the integration, testing, piloting, and acceptance of a release. Application and technical infrastructure components are tested to determine if they interact properly.

[4] The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies brought together to assist with the IRS' efforts to modernize its computer systems and related information technology.

responsible for incorporating and developing security controls into modernization systems and their coordination is critical to effectively carry out these responsibilities. The MA&SS organization is responsible for establishing security standards for all systems and testing the security controls for new systems. It has a directorate specifically dedicated to ensuring appropriate security controls are developed, tested, and implemented for modernization systems. The BSMO is primarily responsible for ensuring security controls are considered, developed, and integrated in modernization systems. For the systems we reviewed, the BSMO contracted with the PRIME contractor to develop security controls in accordance with IRS standards.

The IRS did not adequately consider security controls in the development phase of the systems. We identified several inadequate security controls, many of which could have been addressed in the development phase of the systems. For example, several security configurations do not comply with IRS standards, audit trails are not useable for modernization systems, and disaster recovery plans are not adequate for the systems we reviewed. In addition, documentation required in the development phase provided only general or outdated descriptions of security requirements and controls.

Waiting until after implementation to address these weaknesses will most likely cost significantly more than if the issues were considered during the development of the systems. These inadequate security configurations could result in system exploitation by unauthorized individuals or personnel. In addition, the lack of disaster recovery planning in the development phase could unnecessarily prolong the recovery from a natural disaster or terrorist attack. Based on the conditions we identified, we believe the PRIME contractor primarily focused on delivering systems that would function but did not provide sufficient emphasis to ensure security controls had been developed for the systems. Additionally, the MA&SS organization was not sufficiently involved in the early development stages of the systems we reviewed. More involvement was needed to hold the PRIME contractor accountable and to encourage the PRIME contractor to develop security controls in compliance with IRS security standards when the systems were being developed.

During the integration phase of the ELC, applications must be tested with the technical infrastructure to ensure they interact effectively. The IRS' testing identified several security control weaknesses, but some were not corrected before implementation. For example, the IRS found operating system configurations and file permissions were inaccurate on all Microsoft Windows computers for two systems. Although the IRS considered this weakness to be a moderate risk, it did not take any action to correct the weakness prior to implementation. Testing tools used by the IRS were generally adequate, but the IRS could use additional free software to identify additional security control weaknesses, such as the lack of security patches, before implementing new systems.

To ensure security controls that meet IRS security standards are adequately considered during the development of new systems, we recommended the Chief Information Officer (CIO) provide oversight to ensure coordination between the BSMO and PRIME contractor. The CIO should revise the ELC to require disaster recovery planning in the development phase of the system life cycle and ensure the CADE audit trail data are retained and reviewed to detect unauthorized accesses. The Chief, MA&SS, should take the initiative to participate in the development of new systems and ensure security controls are built into the new systems. To improve testing, we recommended the Chief, MA&SS, use additional off-the-shelf security testing tools.

Management's Response: The CIO emphasized that the IRS considers security controls at all times, even when there are pressures to implement systems. Security design processes are shared with various internal stakeholders and required life cycle artifacts are thoroughly reviewed. Also, IRS integration, deployment, and operational processes have matured since the audit was conducted. For example, the IRS modified the PRIME contract to include updated security requirements and implemented processes to measure compliance with IRS security settings during testing.

The CIO agreed with four of our five recommendations. The CIO stated the ELC and the PRIME contract have been updated to ensure security controls comply with IRS standards and are considered in the development phase. The ELC will be revised to include disaster recovery planning in the development phase. The CIO agreed that the MA&SS organization should be included in the development phase of new projects. In addition, the ELC has been updated to ensure security deliverables are addressed throughout the life cycle. To enhance security testing, the IRS will review internal processes and determine if additional tools can better check systems controls. The CIO disagreed with our recommendation to retain and review audit trail information on the CADE and is not taking any action because the system cannot be accessed externally. The CIO also disagreed that the Security Audit and Analysis System (SAAS), which was procured to collect and review audit trail information for other modernization systems, was not operating. The CIO stated testing in September 2004 validated the SAAS was receiving and processing modernized system audit trail transactions. Management's complete response to the draft report is included as Appendix VI.

Office of Audit Comments: The IRS made several improvements during our review that should address our conclusions and improve the security of modernization systems. IRS updates to the ELC and changes to the PRIME contract are examples of these improvements. We continue to believe that audit trail information for the CADE should be retained and reviewed. The CADE contains tax information for over 1.3 million returns that could be accessed by some IRS employees for unauthorized purposes and potentially used for identity theft purposes. Accordingly, audit trail information must be maintained to comply with Department of the Treasury requirements. We do not intend to elevate our disagreement to the Department of the Treasury for resolution at this time. However, we do plan a comprehensive review to determine whether audit trails for modernization systems are being retained and reviewed. We will include the CADE and the SAAS in this follow-up review.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Background

The Internal Revenue Service (IRS) relies on approximately 350 computer systems to process tax information and account for over $2 trillion in revenue annually.[1] Security over these systems is critical to prevent hackers, disgruntled employees, and contractors from gaining unauthorized access to taxpayers' sensitive financial information or from disrupting computer operations.

The IRS has many security weaknesses in its computer systems that have been difficult and costly to correct. One explanation for these weaknesses is that security controls were not adequately considered during the development of the systems. Many of the IRS' legacy systems were developed before the IRS had implemented a rigorous system development methodology.

Security weaknesses are almost always more difficult and costly to correct after systems have been implemented. According to the National Institute of Standards and Technology (NIST), it costs 30 times as much to fix a defect once software is built as it does to identify controls needed during requirements gathering.[2] In another study, Gartner, Inc.[3] states if 50 percent of software vulnerabilities were removed prior to production for purchased and internally developed software, enterprise configuration management costs and incident response costs would be reduced by 75 percent each.[4]

The IRS has a unique opportunity during its systems modernization efforts to develop security controls more effectively and efficiently. Many of its core systems are being rebuilt under the Business Systems Modernization (BSM) efforts.

[1] *Financial Audit: IRS's Fiscal Years 2004 and 2003 Financial Statements* (GAO-05-103, dated November 2004) and the IRS' Inventory of Cyber Assets.

[2] *The Economic Impacts of Inadequate Infrastructure for Software Testing*, NIST, May 2002. The NIST, under the Department of Commerce, develops standards and guidelines for providing adequate information security for Federal Government operations and assets.

[3] Gartner, Inc. is a leading provider of research and analysis on the global information technology industry.

[4] *Require Vulnerability Testing During Software Development*, Gartner, Inc. research document, dated September 10, 2003.

To ensure modernization projects are developed in a disciplined manner, the IRS adopted its Enterprise Life Cycle (ELC).[5] The ELC processes are divided into six phases. Three of these phases (development, integration, and operations and support) are relevant to incorporating security controls into each system. We concentrated on the development and integration phases in this review.

We judgmentally selected and reviewed the e-Services, Internet Refund Fact of Filing (IRFOF), Modernized e-File (MeF), Custodial Accounting Project (CAP), and Customer Account Data Engine (CADE) modernization projects. Appendix V provides a description of the modernization systems we reviewed. We tested the security controls of each system and, if security weaknesses were identified, determined whether the security control weakness was considered in the development and integration phases of the system.

This review was performed at the Business Systems Modernization Office (BSMO) facilities in New Carrollton, Maryland; the Martinsburg Computing Center (MCC)[6] in Martinsburg, West Virginia; and the Austin Campus[7] in Austin, Texas, during the period March 2004 through May 2005. 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.

[5] The ELC establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduce the risks of system development and ensures alignment with the overall business strategy. All IRS personnel and contractors involved in the modernization effort are required to follow the ELC. Appendix IV provides an overview of the ELC.

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

[7] The campuses are the data processing arm of the IRS. They process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.

Security Controls Need to Be Addressed in the Development Phase

The Mission Assurance and Security Services (MA&SS) organization, the BSMO, and the PRIME contractor[8] are responsible for incorporating and developing security controls into modernization systems, and their coordination is critical to carry out these responsibilities. The MA&SS is responsible for establishing security standards for all systems. It has a directorate specifically dedicated to ensuring appropriate security controls are developed, tested, and implemented for modernization systems. The BSMO is primarily responsible for ensuring security controls are considered, developed, and integrated in modernization systems. For the systems we reviewed, the BSMO contracted with the PRIME contractor to develop security controls in accordance with IRS standards.

We identified several security control weaknesses in the modernization systems we reviewed, many of which could have been addressed in the development phase of the systems. For example, audit trails for modernization systems are not functioning and disaster recovery plans are not adequate for the systems we reviewed. In addition, available documentation indicated a lack of emphasis on security controls as it provided only general or outdated descriptions of security requirements and controls. Waiting until systems are implemented to address security controls will most likely cost significantly more than if security controls had been considered during the development of the systems.

For the five systems, we concluded the PRIME contractor focused on developing systems that would function, but did not provide sufficient emphasis on the identification and development of security controls. In addition, the MA&SS organization was not sufficiently involved during the early development stages of the systems. More involvement was needed to hold the PRIME contractor accountable and to encourage the contractor to develop adequate security controls when the systems were being developed.

[8] The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies brought together to assist with the IRS' efforts to modernize its computer systems and related information technology.

In January 2005, the IRS began taking over the role of systems integrator from the PRIME contractor due to reductions in funding by Congress for the BSM program and concerns about the adequacy of the PRIME contractor's performance. The BSMO will now be responsible for program-level activities such as risk management and requirements management. Contractors will continue to be used to deliver projects and provide support services.

Security configurations needed to deter unauthorized activity did not always comply with IRS standards

Several security configurations in the modernization systems did not comply with IRS standards. In each case, the configurations should have been addressed in the development phase of the systems. These inadequate configurations could result in system security exploitation, unauthorized access to taxpayer data, and disruption of computer operations by unauthorized personnel. Some of the configurations identified are readily exploitable, while others require specialized knowledge of the application installed.

Additionally, we noted two instances in which IRS guidance needs to be improved to increase security. If developers had followed the guidance provided by the IRS in these two instances, authentication controls would have been jeopardized, increasing the opportunities for an unauthorized person to gain access to the systems. Due to the sensitive nature of the security weaknesses identified, we are not disclosing the weaknesses in this report. However, we provided IRS management with detailed information of these security weaknesses.

Audit trails needed to detect unauthorized activity are not operating on modernization systems

The Department of the Treasury requires automated information systems and networks which process, store, or transmit sensitive information maintain an audit trail of user security-relevant events. In addition, the audit trail security feature should be properly implemented and protected from modification. The NIST and the Government Accountability Office also provide guidelines for agencies to comply with Federal information systems security requirements.

Although we did not specifically evaluate audit trail controls for the systems in our sample, we noted in a prior review[9] that a system designed to collect audit trail data from certain modernization systems (including the e-Services, IRFOF, and MeF projects in our sample) was not functioning as intended. Audit trail data were being stored, but users could not query the information due to software performance and functionality problems. The IRS accepted the system from the PRIME contractor even though it was aware that the system was not functioning. We were advised by BSMO management during this review that this audit trail system is still not functioning.

The CADE has its own audit trail. The CADE, which is eventually expected to replace the IRS' existing Master File processing systems,[10] was first released in July 2004. As of April 27, 2005, it had processed 1.3 million Form 1040 EZ[11] returns. The audit trail for the CADE is being collected, but it is destroyed after 1-2 days without being reviewed. We were advised by the CADE systems programmer that no IRS manager or employee had expressed a need to review CADE audit trail data, thus it was not being retained. Audit trail information should be reviewed frequently to protect against abuse and to identify abnormal activity by users.

The lack of audit trail functionality on these four modernization systems prevents management from identifying and investigating potential unauthorized accesses to the systems. We cannot comment on the audit trail capabilities of the CAP because it was cancelled before being released.

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

[10] Master File processing systems contain taxpayer account and return data for individuals, businesses, and employer retirement plans.

[11] Form 1040EZ is the Income Tax Return for Single and Joint Filers With No Dependents. The initial release of the CADE will not process Forms 1040EZ for joint filers.

<u>Disaster Recovery Planning was not considered during the development phase of the systems</u>

The modernization systems we reviewed will reside on computers at the MCC. The strategy for disaster recovery at the MCC is to mirror all modernization applications at the Tennessee Computing Center (TCC) in Memphis, Tennessee. We noted the following concerns.

- The MCC Disaster Recovery Plan addresses the IRFOF system but does not contain steps to fully restore the system in the event of a severe disaster. The Disaster Recovery Plan does not address the other two production systems (e-Services and the MeF.) The Disaster Recovery Plan for the CADE adequately addressed disaster recovery requirements but these requirements were not tested prior to implementation.[12]

- Currently, the TCC cannot support full restoration of the modernization systems in the event of a disaster. The IRS is designing a Disaster Recovery Plan for those modernization systems currently being developed, including the e-Services and the MeF. The Plan will contain steps for building and recovering systems and is scheduled to be completed within 2 years.

- IRS guidance requires each site to store a complete copy of the Disaster Recovery Plan in both magnetic media and hard copy at the off premises storage facility for that site. Disaster recovery documents for four of the five modernization systems were not stored off-site. These documents are necessary to provide instructions to employees in the event of a disaster.

- Training was not provided for personnel with disaster recovery responsibilities. According to the Disaster Recovery Training Coordinator for systems at the MCC, the Disaster Recovery Team is

[12] *To Ensure the Customer Account Data Engine's Success, Prescribed Management Practices Need to Be Followed* (Reference Number 2005-20-005, dated November 2004).

comprised of system administrators who are considered technical experts and, thus, do not need training. The NIST requires disaster recovery personnel to be trained to the extent that they are able to execute their respective recovery procedures without aid of the recovery plan.

The lack of disaster recovery planning for modernization systems could unnecessarily delay the recovery from a natural disaster or terrorist attack. The ELC does not require a detailed Disaster Recovery Plan for any of the phases of the system life cycle. In lieu of a detailed Disaster Recovery Plan, the ELC does require a contingency plan that lacks the specific information needed to restore systems in the event of a disaster.

Available documentation indicated security controls were not addressed sufficiently during the development phase

The PRIME contractor is required to prepare several reports for each system including the Systems Requirements Report, Security Risk Assessment, Security Plan, Technical Model View, Physical Technology Model View, and the Version Description Document (VDD). Collectively, these reports should document the risks and security controls relevant to each system so the BSMO, the PRIME contractor, and the MA&SS organization have a common understanding of how the system will be developed and implemented.

We found several reports and plans that contained either general or outdated security requirements. For example, one report stated requirements would be conducted in accordance with the methodology described in an Internal Revenue Manual section that has been outdated since January 2002.

The VDD, in particular, should contain the steps needed to configure and develop the business and security applications needed for the system to operate. However, the VDDs used to build the systems did not include the security controls needed to eliminate the weaknesses we identified.

Recommendations

To ensure security controls that comply with IRS standards are considered in the development phase of modernization systems, the Chief Information Officer (CIO) should:

1. Provide oversight to ensure coordination between the BSMO and its contractors. Under the new operating model, the BSMO should retain the overall responsibility for ensuring security controls are provided in the development phase of new projects. This responsibility will require the BSMO to ensure it is properly drafting roles and responsibilities to adequately consider security controls during the development phase of the ELC.

Management's Response: The CIO has designated the Director, Infrastructure Modernization Program Office, to provide oversight and ensure coordination between the BSMO and contractors. The CIO stated that, although adequate controls during the design and development phase are reflected in the new ELC, additional improvements can be implemented. In addition, the PRIME contract has been updated to reflect updated security standards and requirements.

2. Revise the ELC to require disaster recovery planning in the development phase of the system life cycle. A complete Disaster Recovery Plan should be required that addresses all modernization systems. During development, computer capacity and business resumption requirements should be gathered and considered.

Management's Response: The Deputy Associate CIO of Business Integration will include language in the ELC regarding disaster recovery planning in the development phase of the system life cycle. In addition, corrective actions have been provided as part of the Disaster Recovery Material Weakness Plan to develop disaster recovery plans for all major systems supporting the IRS' most critical business processes and to update resource requirements for disaster recovery capabilities for major systems.

3. Ensure audit trail data captured for the CADE is retained and reviewed to detect unauthorized accesses.

Management's Response: The CIO disagreed with this recommendation. The log and audit files used by the CADE system programmers are established for recovery and diagnostic purposes and do not capture data related to unauthorized access. Currently, the CADE has no support for external data inquiry.

Office of Audit Comment: We continue to believe that audit trail information for the CADE should be retained and reviewed. The CADE contains tax information for over 1.3 million returns that could be accessed by some IRS employees for unauthorized purposes and potentially used for identity theft purposes. Accordingly, audit trail information must be maintained to comply with Department of the Treasury requirements.

The Chief, MA&SS, should:

4. Ensure the MA&SS organization is included and participates in the development phase of new systems and ensure security controls are built into the systems.

Management's Response: The CIO agreed that the MA&SS organization should participate in the development of new systems. In addition, the recent update to the ELC ensures security deliverables, checkpoints, and milestone exit certification requirements are addressed throughout the life cycle. The ELC updates will ensure security controls are built into the systems.

Modernization Systems' Security Testing Could Be Improved

During the integration phase of the ELC, systems must be tested to ensure security controls are adequate and they interact effectively with the technical infrastructure. This is a critical integration phase checkpoint because it is the last opportunity to identify security control weaknesses before implementation. The MA&SS organization is responsible for conducting security testing and identifying security weaknesses on new systems.

The IRS' security testing identified several security weaknesses but not all identified weaknesses were corrected. For example, the IRS' security testing of the modernization systems we reviewed identified incorrect registry and file permissions on all Microsoft Windows computers for two systems. Although the IRS considered this weakness to be a moderate risk, it accepted the risks and did not correct the weakness prior to implementation. Based on the circumstances at the time, the decision to implement without correcting the weakness may have been appropriate. However, addressing the weakness earlier in development would have precluded the IRS from having to accept the associated risks and from potentially incurring additional costs to correct it after implementation.

The IRS' testing process could also be enhanced. The IRS limited its testing tools to two products which were developed to test for compliance with IRS standards. The IRS believes its testing methodology adequately addresses security. While we agree the tools used by the IRS are effective, additional security vulnerabilities could be identified using additional cost-effective tools. For example, one free off-the-shelf program evaluates Microsoft Windows workstations for security vulnerabilities. Using this program, we found over 63 percent of the IRS' Microsoft Windows workstations systems were missing at least 1 critical security patch. The SANS Top 20 Internet Security Vulnerabilities[13] list recommends several additional security testing tools to assist organizations in identifying vulnerabilities.

Furthermore, the IRS' security tests could have been conducted more efficiently. For example, test commands for mainframe computers were entered manually into the system to gather data. Manual entry of commands is a very time-consuming process and, given the size of the modernization security database, inefficient and ineffective. The modernization mainframe computers already have software installed that could be used to generate test reports more efficiently.

[13] The SANS Top 20 Internet Security Vulnerabilities, dated October 8, 2004. The SysAdmin, Audit, Network, Security (SANS) Institute was established in 1989 as a cooperative research and education organization. It develops and maintains research documents about various aspects of information security.

Recommendation

To address the testing of security controls for modernization systems in the integration phase, the Chief, MA&SS, should:

5. Enhance the Security Test and Evaluation process to include the use of additional off-the-shelf security testing tools to identify security vulnerabilities. More efficient tools that are already available to the IRS for generating test reports should also be used.

Management's Response: The Deputy Director of Certification, Testing, Evaluation, and Assessment will review the IRS' internal process and determine if additional tools can be used to better check systems controls.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of our review was to evaluate the Internal Revenue Service's (IRS) process for incorporating computer security controls into modernization systems. To accomplish this objective, we:

I. Judgmentally selected a sample of three modernization projects that had been implemented (the Internet Refund Fact of Filing,[1] e-Services,[2] and Modernized e-File[3]) and two projects being developed (the Customer Account Data Engine[4] and the Custodial Accounting Project[5]). Currently, there are over 21 modernization projects consisting of business projects, infrastructure projects, and data projects. We used a judgmental sample because we were not planning to project the audit results. For the three implemented systems, we used software tools to evaluate operating system security settings for the systems at the Martinsburg Computing Center (MCC). We recorded any security weaknesses found in these systems.

A. Obtained and reviewed the most recent Security Test and Evaluation plans and reports and Rational Database Security tests.

B. Compared security vulnerabilities identified by the IRS and our audit team and conducted further research to determine whether the problem occurred before or after security testing was conducted.

II. If a security vulnerability identified in Step I occurred prior to testing, determined why the vulnerability was not reduced or corrected during the design phase.

A. Obtained and reviewed the Systems Requirements Report, Security Risk Assessment, Security Plan, Technical Model View, Physical Technology Model View, and the Version Description Document for the three implemented modernization systems we selected to evaluate the adequacy of the information provided.

[1] A web-based application that provides Form 1040-series taxpayers with refund status via the Internet. The Form 1040-series involves individual taxpayers.

[2] A suite of web-based products that will allow tax professionals and taxpayers to conduct business with the IRS electronically.

[3] Provides taxpayers the option to electronically file a U.S. Corporation Income Tax Return (Form 1120), U.S. Income Tax Return for an S Corporation (Form 1120S), U.S. Income Tax Return for Certain Political Organizations (Form 1120-POL), Return of Organization Exempt From Income Tax (Form 990), Short Form Return of Organization Exempt From Income Tax (Form 990-EZ), and Application for Extension of Time To File an Exempt Organization Return (Form 8868) through the Internet.

[4] An online modernization data infrastructure that will house the authoritative taxpayer account and return data.

[5] A single, integrated data repository of taxpayer account information, integrated with the general ledger and accessible for management analysis and reporting. The IRS cancelled this project in January 2005.

B. Determined whether the same vulnerabilities existed in the two projects being developed by reviewing applicable documentation and executing tests conducted in Step I.

III. Determined whether audit trails were functioning for the modernization systems we reviewed.

A. Followed up on a prior Treasury Inspector General for Tax Administration audit report[6] to determine whether actions had been taken to provide audit trail data for modernization systems, including the e-Services, Modernized e-File, and Internet Refund Fact of Filing projects.

B. Interviewed MCC officials regarding the availability and use of audit trail data for the Customer Account Data Engine system.

IV. Determined whether the modernization systems had adequate contingency plans.

A. Evaluated the adequacy of available Disaster Recovery Plans for each system in our sample.

B. Ascertained whether disaster recovery training had been provided to responsible officials.

C. Determined whether disaster recovery plans were maintained off-site.

D. Determined whether disaster recovery requirements were included in the Enterprise Life Cycle.

V. Evaluated the effectiveness of IRS security testing. For vulnerabilities identified by the IRS, we determined whether the problems were corrected, waived, or neglected.

A. Reviewed the IRS' processes and controls over security testing.

B. Evaluated the testing methodology for the three implemented modernization systems to determine whether the testing was adequate.

C. Reviewed the tests to determine whether information was correctly recorded and tested.

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

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Program)
Stephen Mullins, Director
Thomas Polsfoot, Audit Manager
Cari Fogle, Senior Auditor
Myron Gulley, Senior Auditor
Michael Howard, Senior Auditor
Jimmie Johnson, Senior Auditor
Jacqueline Nguyen, Senior Auditor
Midori Ohno, Senior Auditor
Larry Reimer, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Associate Chief Information Officer, Business Systems Modernization OS:CIO:B
Associate Chief Information Officer, Information Technology Services OS:CIO:I
Director, Enterprise Operations OS:CIO:I:EO
Acting Director, Regulatory Compliance OS:MA:RC
Acting Director, Strategy, Program Management, and Personnel Security OS:MA:SP
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Management Controls OS:CFO:AR:M
Audit Liaisons:
    Chief Information Officer OS:CIO
    Chief, Mission Assurance and Security Services OS:MA

Appendix IV

Enterprise Life Cycle Overview

The Enterprise Life Cycle (ELC) defines the processes, products, techniques, roles, responsibilities, policies, procedures, and standards associated with planning, executing, and managing business change. It includes redesign of business processes; transformation of the organization; and development, integration, deployment, and maintenance of the related information technology applications and infrastructure. Its immediate focus is the Internal Revenue Service (IRS) Business Systems Modernization (BSM) program. Both the IRS and its contractors must follow the ELC in developing/acquiring business solutions for modernization projects.

Life-Cycle Processes

The life-cycle processes of the ELC are divided into six phases, as described below:

- **Vision and Strategy** - This phase establishes the overall direction and priorities for business change for the enterprise. It also identifies and prioritizes the business or system areas for further analysis.
- **Architecture** - This phase establishes the concept/vision, requirements, and design for a particular business area or target system. It also defines the releases for the business area or system.
- **Development -** This phase includes the analysis, design, acquisition, modification, construction, and testing of the components of a business solution. This phase also includes routine planned maintenance of applications.
- **Integration** - This phase includes the integration, testing, piloting, and acceptance of a release. In this phase, the integration team brings together individual work packages of solution components developed or acquired separately during the Development phase. Application and technical infrastructure components are tested to determine if they interact properly. If appropriate, the team conducts a pilot to ensure all elements of the business solution work together.
- **Deployment** - This phase includes preparation of a release for deployment and actual deployment of the release to the deployment sites. During this phase, the deployment team puts the solution release into operation at target sites.
- **Operations and Support** - This phase addresses the ongoing operations and support of the system. It begins after the business processes and system(s) have been installed and have begun performing business functions. It encompasses all of the operations and support processes necessary to deliver the services associated with managing all or part of a computing environment.

The Operations and Support phase includes the scheduled activities, such as planned maintenance, systems backup, and production output, as well as the nonscheduled activities, such as problem resolution and service request delivery, including emergency unplanned maintenance of applications. It also includes the support processes required to keep the system up and running at the contractually specified level.

Management Processes

Besides the life-cycle processes, the ELC also addresses the various management areas at the process level. The management areas include:

- **IRS Governance and Investment Decision Management** - This area is responsible for managing the overall direction of the IRS, determining where to invest, and managing the investments over time.
- **Program Management and Project Management** - This area is responsible for organizing, planning, directing, and controlling the activities within the program and its subordinate projects to achieve the objectives of the program and deliver the expected business results.
- **Architectural Engineering/Development Coordination** - This area is responsible for managing the technical aspects of coordination across projects and disciplines, such as managing interfaces, controlling architectural changes, ensuring architectural compliance, maintaining standards, and resolving issues.
- **Management Support Processes** - This area includes common management processes, such as quality management and configuration management that operate across multiple levels of management.

Milestones

The ELC establishes a set of repeatable processes and a system of milestones, checkpoints, and reviews that reduce the risks of system development, accelerate the delivery of business solutions, and ensure alignment with the overall business strategy. The ELC defines a series of milestones in the life-cycle processes. Milestones provide for “go/no-go” decision points in the project and are sometimes associated with funding approval to proceed. They occur at natural breaks in the process where there is new information regarding costs, benefits, and risks and where executive authority is necessary for next phase expenditures.

There are five milestones during the project life cycle:

- **Milestone 1 - Business Vision and Case for Action.** In the activities leading up to Milestone 1, executive leadership identifies the direction and priorities for IRS business change. These guide which business areas and system development projects are funded for further analysis. The primary decision at Milestone 1 is to select BSM projects based on both the enterprise-level Vision and Strategy and the enterprise architecture.

- **Milestone 2 - Business Systems Concept and Preliminary Business Case.** The activities leading up to Milestone 2 establish the project concept, including requirements and design elements, as a solution for a specific business area or business system. A preliminary business case is also produced. The primary decision at Milestone 2 is to approve the solution/system concept and associated plans for a modernization initiative and to authorize funding for that solution.
- **Milestone 3 - Business Systems Design and Baseline Business Case.** In the activities leading up to Milestone 3, the major components of the business solution are analyzed and designed. A baseline business case is also produced. The primary decision at Milestone 3 is to accept the logical system design and associated plans and to authorize funding for development, test, and (if chosen) pilot of that solution.
- **Milestone 4 - Business Systems Development and Enterprise Deployment Decision.** In the activities leading up to Milestone 4, the business solution is built. The Milestone 4 activities are separated by two checkpoints. Activities leading up to Milestone 4A involve further requirements definition, production of the system’s physical design, and determination of the applicability of fixed-price contracting to complete system development and deployment. To achieve Milestone 4B, the system is integrated with other business systems and tested, piloted (usually), and prepared for deployment. The primary decision at Milestone 4B is to authorize the release for enterprise-wide deployment and commit the necessary resources.
- **Milestone 5 - Business Systems Deployment and Postdeployment Evaluation.** In the activities leading up to Milestone 5, the business solution is fully deployed, including delivery of training on use and maintenance. The primary decision at Milestone 5 is to authorize the release of performance-based compensation based on actual, measured performance of the business system.

Appendix V

Description of Modernization Projects Reviewed

e-Services - The e-Services is a suite of web-based products that will allow tax professionals and taxpayers to do business with the IRS electronically.

The Internet Refund Fact of Filing (IRFOF) – The IRFOF is a web-based application that provides Form 1040-series taxpayers with refund status via the Internet. The Form 1040 series involves individual taxpayers.

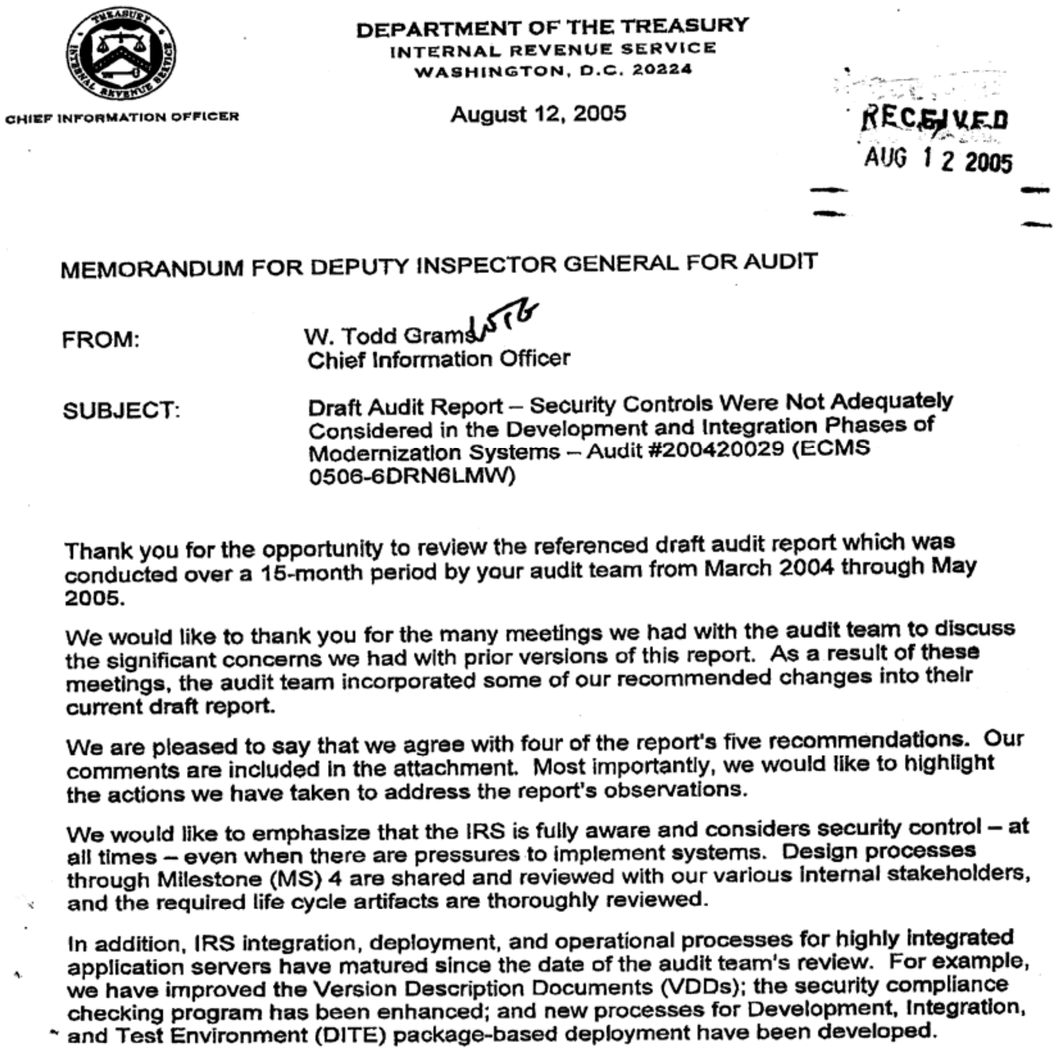
Modernized e-File (MeF) - The MeF provides taxpayers the option to electronically file a U.S. Corporation Income Tax Return (Form 1120), U.S. Income Tax Return for an S Corporation (Form 1120S), U.S. Income Tax Return for Certain Political Organizations (Form 1120-POL), Return of Organization Exempt From Income Tax (Form 990), Short Form Return of Organization Exempt From Income Tax (Form 990-EZ), and Application for Extension of Time To File an Exempt Organization Return (Form 8868) through the Internet.

The Custodial Accounting Project (CAP) - The CAP will be a single, integrated data repository of taxpayer account information, integrated with the general ledger and accessible for management analysis and reporting. The IRS cancelled this project in January 2005.

The Customer Account Data Engine (CADE) - The CADE is an online modernization data infrastructure that will house the authoritative taxpayer account and return.

Appendix VI

Management's Response to the Draft Report



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

CHIEF INFORMATION OFFICER

August 12, 2005

RECEIVED
AUG 12 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: W. Todd Grams
Chief Information Officer

SUBJECT: Draft Audit Report – Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems – Audit #200420029 (ECMS 0506-6DRN6LMW)

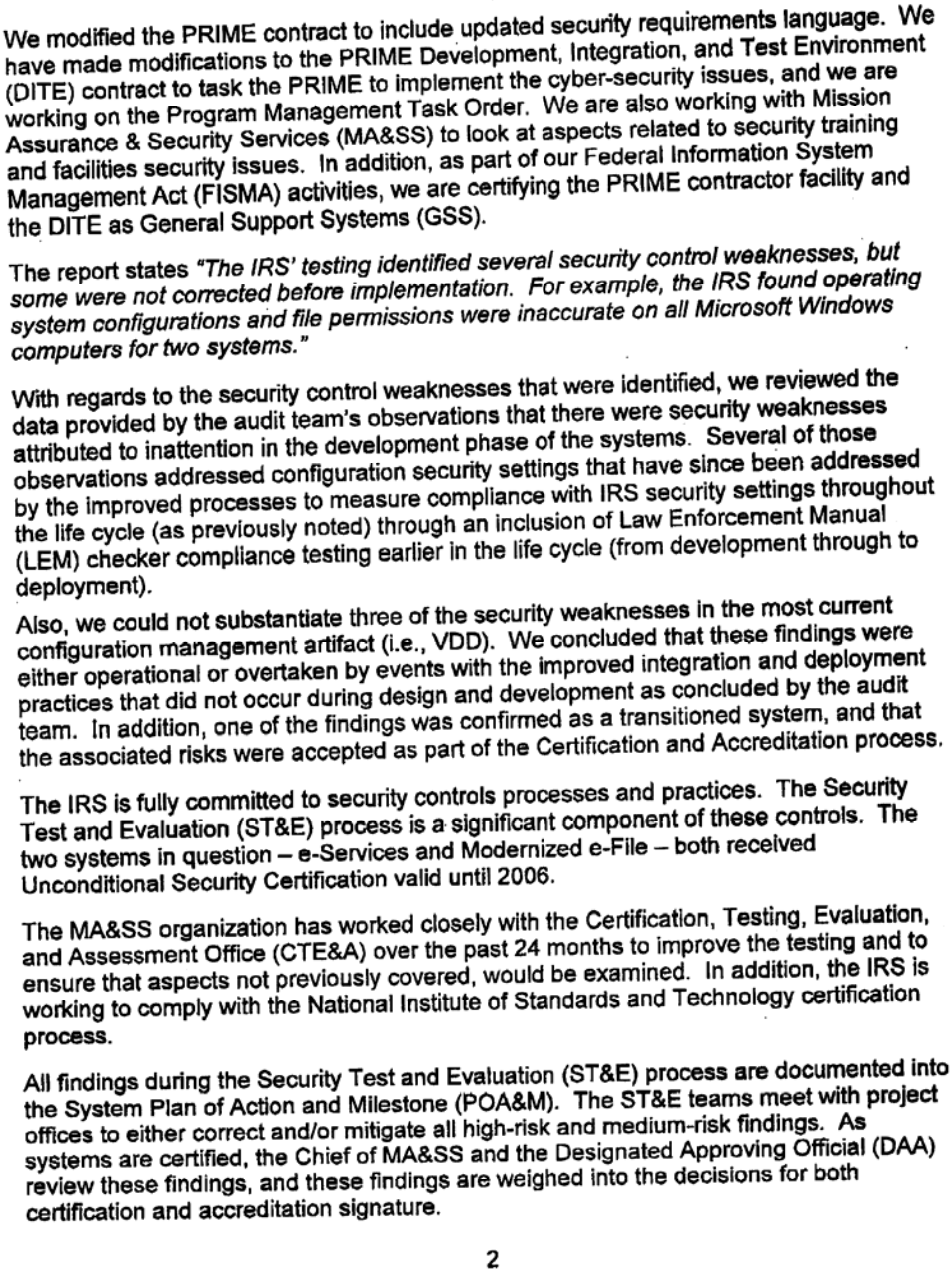
Thank you for the opportunity to review the referenced draft audit report which was conducted over a 15-month period by your audit team from March 2004 through May 2005.

We would like to thank you for the many meetings we had with the audit team to discuss the significant concerns we had with prior versions of this report. As a result of these meetings, the audit team incorporated some of our recommended changes into their current draft report.

We are pleased to say that we agree with four of the report's five recommendations. Our comments are included in the attachment. Most importantly, we would like to highlight the actions we have taken to address the report's observations.

We would like to emphasize that the IRS is fully aware and considers security control – at all times – even when there are pressures to implement systems. Design processes through Milestone (MS) 4 are shared and reviewed with our various internal stakeholders, and the required life cycle artifacts are thoroughly reviewed.

In addition, IRS integration, deployment, and operational processes for highly integrated application servers have matured since the date of the audit team's review. For example, we have improved the Version Description Documents (VDDs); the security compliance checking program has been enhanced; and new processes for Development, Integration, and Test Environment (DITE) package-based deployment have been developed.



We modified the PRIME contract to include updated security requirements language. We have made modifications to the PRIME Development, Integration, and Test Environment (DITE) contract to task the PRIME to implement the cyber-security issues, and we are working on the Program Management Task Order. We are also working with Mission Assurance & Security Services (MA&SS) to look at aspects related to security training and facilities security issues. In addition, as part of our Federal Information System Management Act (FISMA) activities, we are certifying the PRIME contractor facility and the DITE as General Support Systems (GSS).

The report states *"The IRS' testing identified several security control weaknesses, but some were not corrected before implementation. For example, the IRS found operating system configurations and file permissions were inaccurate on all Microsoft Windows computers for two systems."*

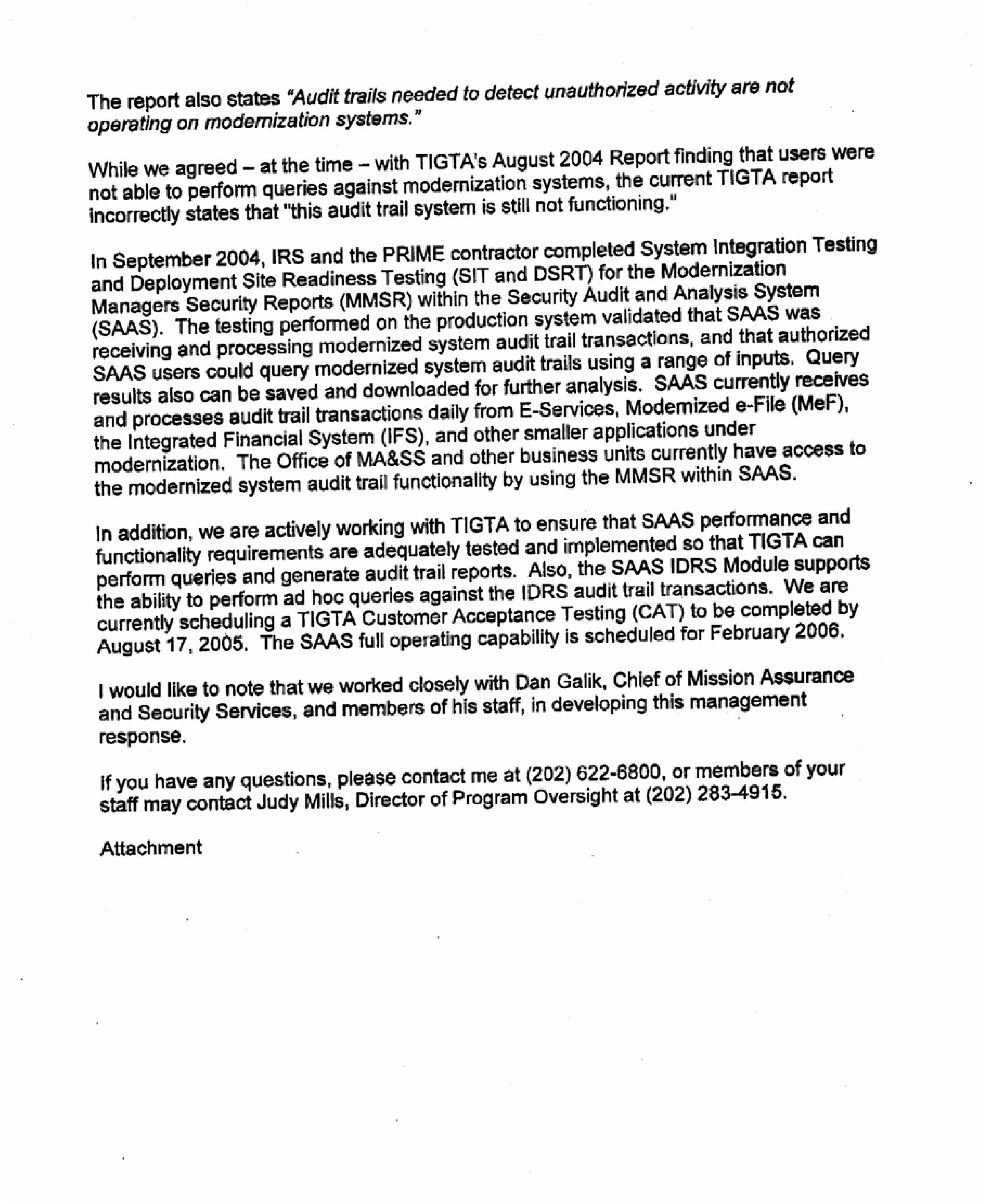
With regards to the security control weaknesses that were identified, we reviewed the data provided by the audit team's observations that there were security weaknesses attributed to inattention in the development phase of the systems. Several of those observations addressed configuration security settings that have since been addressed by the improved processes to measure compliance with IRS security settings throughout the life cycle (as previously noted) through an inclusion of Law Enforcement Manual (LEM) checker compliance testing earlier in the life cycle (from development through to deployment).

Also, we could not substantiate three of the security weaknesses in the most current configuration management artifact (i.e., VDD). We concluded that these findings were either operational or overtaken by events with the improved integration and deployment practices that did not occur during design and development as concluded by the audit team. In addition, one of the findings was confirmed as a transitioned system, and that the associated risks were accepted as part of the Certification and Accreditation process.

The IRS is fully committed to security controls processes and practices. The Security Test and Evaluation (ST&E) process is a significant component of these controls. The two systems in question – e-Services and Modernized e-File – both received Unconditional Security Certification valid until 2006.

The MA&SS organization has worked closely with the Certification, Testing, Evaluation, and Assessment Office (CTE&A) over the past 24 months to improve the testing and to ensure that aspects not previously covered, would be examined. In addition, the IRS is working to comply with the National Institute of Standards and Technology certification process.

All findings during the Security Test and Evaluation (ST&E) process are documented into the System Plan of Action and Milestone (POA&M). The ST&E teams meet with project offices to either correct and/or mitigate all high-risk and medium-risk findings. As systems are certified, the Chief of MA&SS and the Designated Approving Official (DAA) review these findings, and these findings are weighed into the decisions for both certification and accreditation signature.



The report also states *"Audit trails needed to detect unauthorized activity are not operating on modernization systems."*

While we agreed – at the time – with TIGTA's August 2004 Report finding that users were not able to perform queries against modernization systems, the current TIGTA report incorrectly states that "this audit trail system is still not functioning."

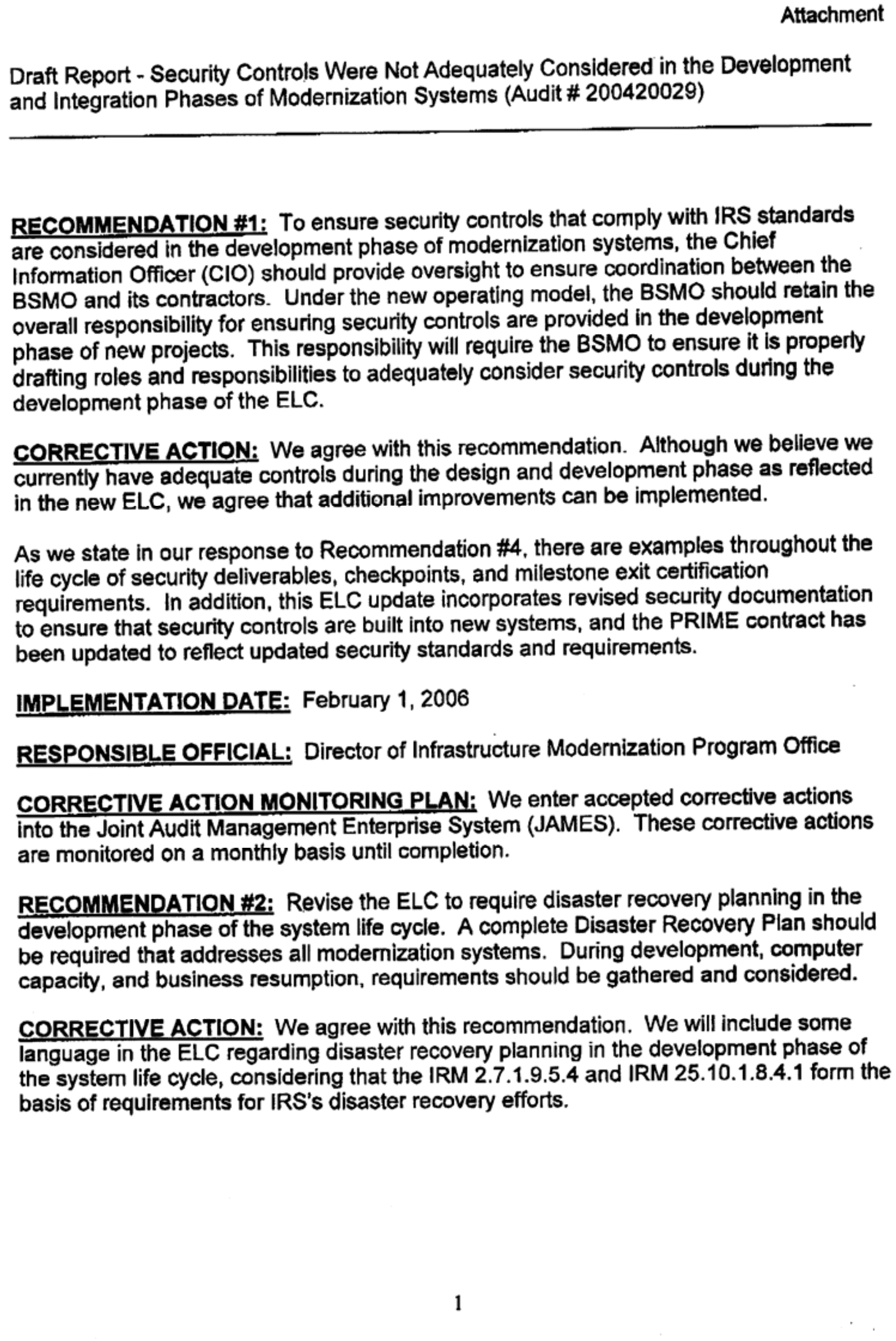
In September 2004, IRS and the PRIME contractor completed System Integration Testing and Deployment Site Readiness Testing (SIT and DSRT) for the Modernization Managers Security Reports (MMSR) within the Security Audit and Analysis System (SAAS). The testing performed on the production system validated that SAAS was receiving and processing modernized system audit trail transactions, and that authorized SAAS users could query modernized system audit trails using a range of inputs. Query results also can be saved and downloaded for further analysis. SAAS currently receives and processes audit trail transactions daily from E-Services, Modernized e-File (MeF), the Integrated Financial System (IFS), and other smaller applications under modernization. The Office of MA&SS and other business units currently have access to the modernized system audit trail functionality by using the MMSR within SAAS.

In addition, we are actively working with TIGTA to ensure that SAAS performance and functionality requirements are adequately tested and implemented so that TIGTA can perform queries and generate audit trail reports. Also, the SAAS IDRS Module supports the ability to perform ad hoc queries against the IDRS audit trail transactions. We are currently scheduling a TIGTA Customer Acceptance Testing (CAT) to be completed by August 17, 2005. The SAAS full operating capability is scheduled for February 2006.

I would like to note that we worked closely with Dan Galik, Chief of Mission Assurance and Security Services, and members of his staff, in developing this management response.

If you have any questions, please contact me at (202) 622-6800, or members of your staff may contact Judy Mills, Director of Program Oversight at (202) 283-4915.

Attachment



Attachment

Draft Report - Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems (Audit # 200420029)

RECOMMENDATION #1: To ensure security controls that comply with IRS standards are considered in the development phase of modernization systems, the Chief Information Officer (CIO) should provide oversight to ensure coordination between the BSMO and its contractors. Under the new operating model, the BSMO should retain the overall responsibility for ensuring security controls are provided in the development phase of new projects. This responsibility will require the BSMO to ensure it is properly drafting roles and responsibilities to adequately consider security controls during the development phase of the ELC.

CORRECTIVE ACTION: We agree with this recommendation. Although we believe we currently have adequate controls during the design and development phase as reflected in the new ELC, we agree that additional improvements can be implemented.

As we state in our response to Recommendation #4, there are examples throughout the life cycle of security deliverables, checkpoints, and milestone exit certification requirements. In addition, this ELC update incorporates revised security documentation to ensure that security controls are built into new systems, and the PRIME contract has been updated to reflect updated security standards and requirements.

IMPLEMENTATION DATE: February 1, 2006

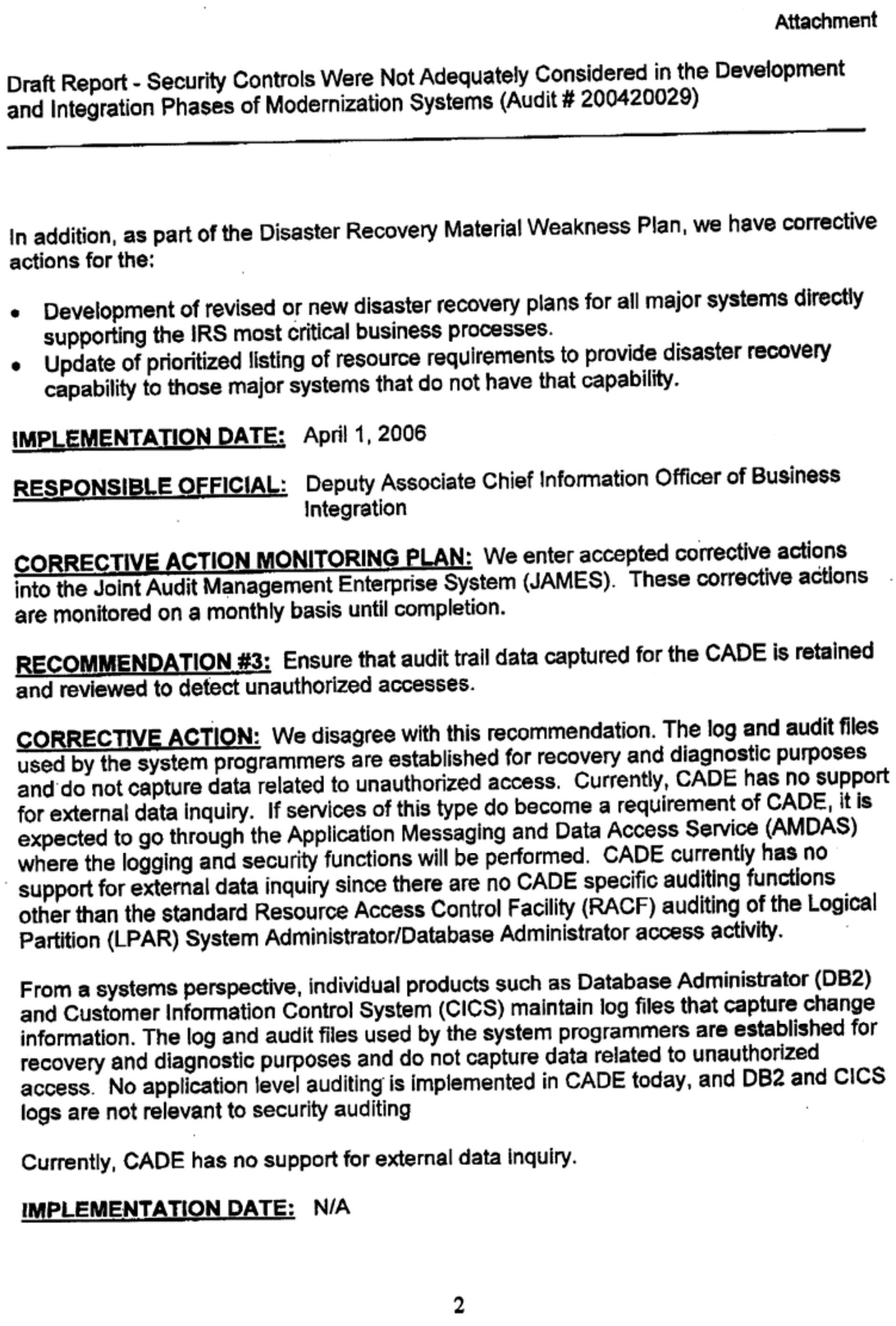
RESPONSIBLE OFFICIAL: Director of Infrastructure Modernization Program Office

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #2: Revise the ELC to require disaster recovery planning in the development phase of the system life cycle. A complete Disaster Recovery Plan should be required that addresses all modernization systems. During development, computer capacity, and business resumption, requirements should be gathered and considered.

CORRECTIVE ACTION: We agree with this recommendation. We will include some language in the ELC regarding disaster recovery planning in the development phase of the system life cycle, considering that the IRM 2.7.1.9.5.4 and IRM 25.10.1.8.4.1 form the basis of requirements for IRS's disaster recovery efforts.

1



Attachment

Draft Report - Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems (Audit # 200420029)

In addition, as part of the Disaster Recovery Material Weakness Plan, we have corrective actions for the:

- Development of revised or new disaster recovery plans for all major systems directly supporting the IRS most critical business processes.
- Update of prioritized listing of resource requirements to provide disaster recovery capability to those major systems that do not have that capability.

IMPLEMENTATION DATE: April 1, 2006

RESPONSIBLE OFFICIAL: Deputy Associate Chief Information Officer of Business Integration

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #3: Ensure that audit trail data captured for the CADE is retained and reviewed to detect unauthorized accesses.

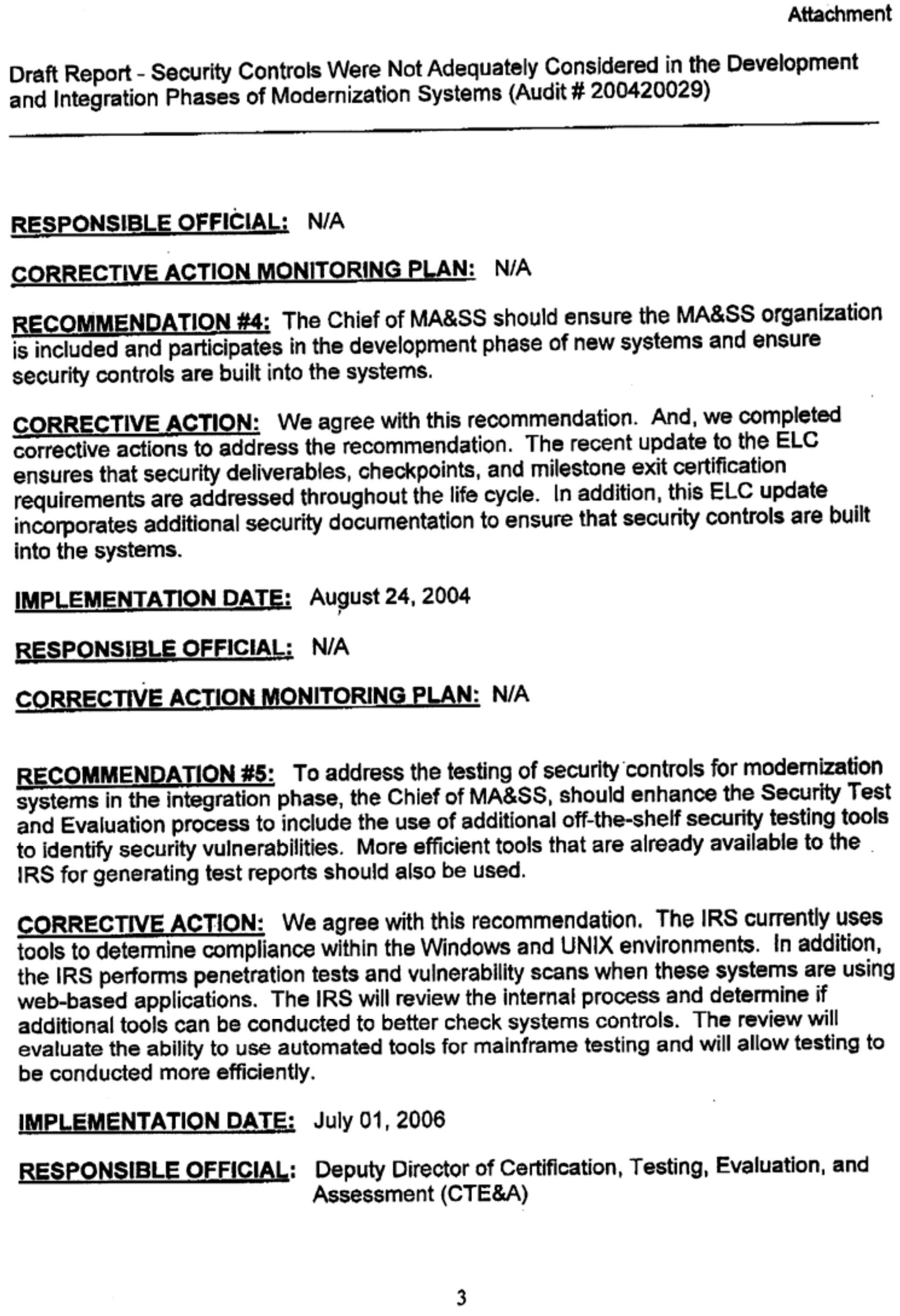
CORRECTIVE ACTION: We disagree with this recommendation. The log and audit files used by the system programmers are established for recovery and diagnostic purposes and do not capture data related to unauthorized access. Currently, CADE has no support for external data inquiry. If services of this type do become a requirement of CADE, it is expected to go through the Application Messaging and Data Access Service (AMDAS) where the logging and security functions will be performed. CADE currently has no support for external data inquiry since there are no CADE specific auditing functions other than the standard Resource Access Control Facility (RACF) auditing of the Logical Partition (LPAR) System Administrator/Database Administrator access activity.

From a systems perspective, individual products such as Database Administrator (DB2) and Customer Information Control System (CICS) maintain log files that capture change information. The log and audit files used by the system programmers are established for recovery and diagnostic purposes and do not capture data related to unauthorized access. No application level auditing is implemented in CADE today, and DB2 and CICS logs are not relevant to security auditing

Currently, CADE has no support for external data inquiry.

IMPLEMENTATION DATE: N/A

2



Attachment

Draft Report - Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems (Audit # 200420029)

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #4: The Chief of MA&SS should ensure the MA&SS organization is included and participates in the development phase of new systems and ensure security controls are built into the systems.

CORRECTIVE ACTION: We agree with this recommendation. And, we completed corrective actions to address the recommendation. The recent update to the ELC ensures that security deliverables, checkpoints, and milestone exit certification requirements are addressed throughout the life cycle. In addition, this ELC update incorporates additional security documentation to ensure that security controls are built into the systems.

IMPLEMENTATION DATE: August 24, 2004

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

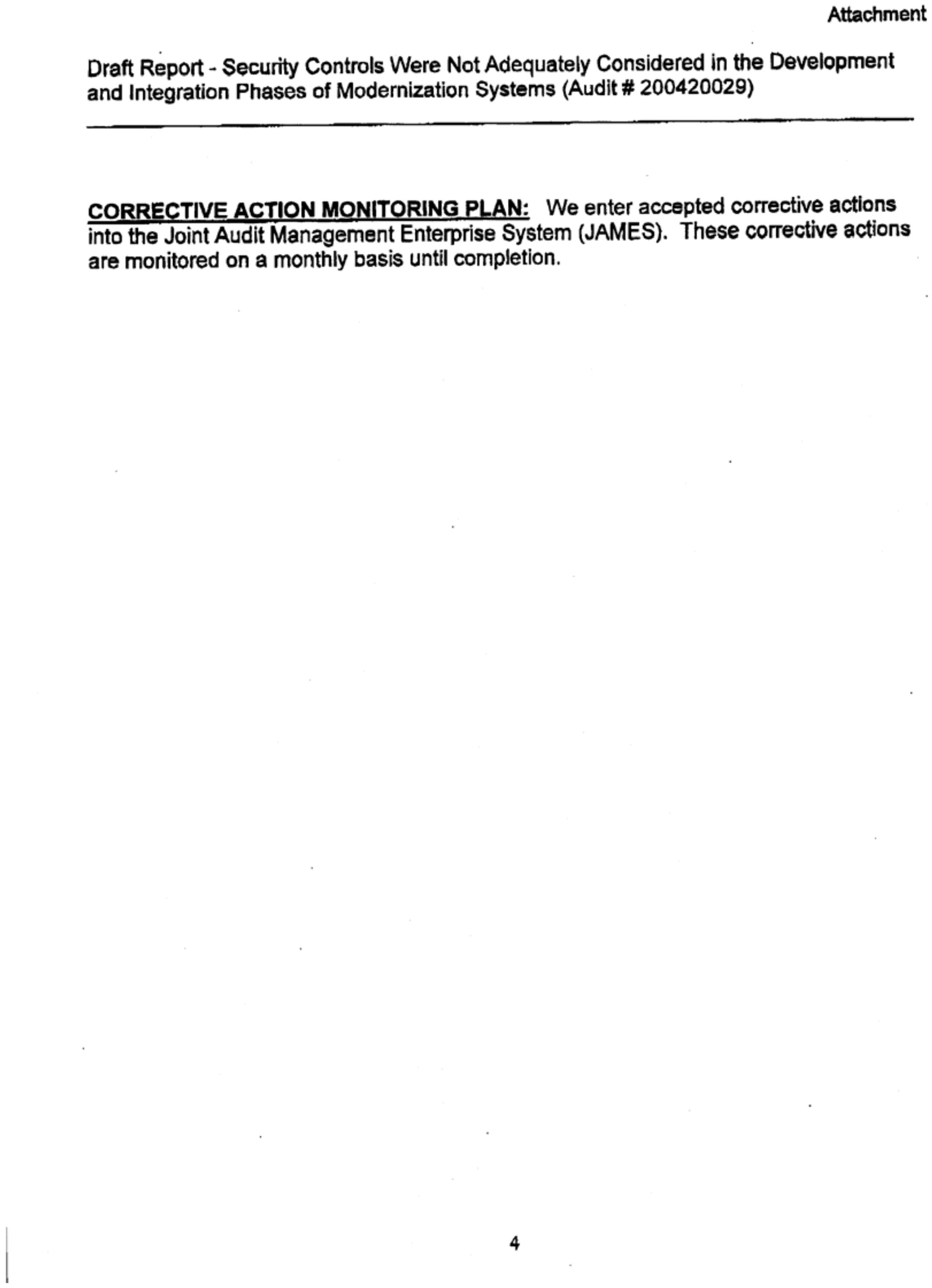
RECOMMENDATION #5: To address the testing of security controls for modernization systems in the integration phase, the Chief of MA&SS, should enhance the Security Test and Evaluation process to include the use of additional off-the-shelf security testing tools to identify security vulnerabilities. More efficient tools that are already available to the IRS for generating test reports should also be used.

CORRECTIVE ACTION: We agree with this recommendation. The IRS currently uses tools to determine compliance within the Windows and UNIX environments. In addition, the IRS performs penetration tests and vulnerability scans when these systems are using web-based applications. The IRS will review the internal process and determine if additional tools can be conducted to better check systems controls. The review will evaluate the ability to use automated tools for mainframe testing and will allow testing to be conducted more efficiently.

IMPLEMENTATION DATE: July 01, 2006

RESPONSIBLE OFFICIAL: Deputy Director of Certification, Testing, Evaluation, and Assessment (CTE&A)

3



Attachment

Draft Report - Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems (Audit # 200420029)

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.