TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities

September 24, 2008

Reference Number: 2008-20-163

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number | 202-622-6500
Email Address | inquiries@tigta.treas.gov
Web Site | http://www.tigta.gov

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 24, 2008

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION
CHIEF INFORMATION OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities (Audit # 200720031)

This report presents the results of our review to determine whether appropriate security controls have been implemented in the Customer Account Data Engine (CADE) and the Account Management Services (AMS) systems. This review was part of the Information Systems Programs business unit's statutory requirements to annually review the adequacy and security of Internal Revenue Service (IRS) information technology.

Impact on the Taxpayer

The CADE will provide the foundation for managing all taxpayer accounts and will replace existing tax processing systems. When we started our review, the AMS was being designed to interface with the CADE. The AMS will provide faster and improved access by employees to taxpayer account data. Security weaknesses in controls over sensitive data protection, system access, monitoring of system access, and disaster recovery have continued to exist even though key phases of the CADE and the AMS have been deployed. As a result, the IRS is jeopardizing the confidentiality, integrity, and availability of an increasing volume of tax information for millions of taxpayers as application releases[1] are put into operation.

[1] A release is a specific edition of software.

Synopsis

The IRS has established appropriate system development policies and procedures that require security and privacy safeguards to be planned for and designed in the early phases of a system's development life. To ensure that projects progress satisfactorily toward implementation of all security and privacy requirements, the IRS implemented various evaluations that developmental projects must undergo prior to exiting the different milestones.[2] In addition, the IRS annually updates the security and privacy control requirements that all new and existing information systems must address to comply with current Federal Government-wide guidance. For new systems such as the CADE and the AMS, the goals of these requirements and evaluations are to ensure that 1) security has been considered and built into systems, and 2) no system is deployed with significant security vulnerabilities.

Despite these requirements, our review of available test documents provided by the IRS showed that both the CADE and the AMS were deployed with known security vulnerabilities relating to the protection of sensitive data, system access, monitoring of system access, and disaster recovery. These vulnerabilities increase the risks that 1) an unscrupulous person, with little chance of detection, could gain unauthorized access to the vast amount of taxpayer information the IRS processes, and 2) the systems could not be recovered effectively and efficiently during an emergency.

We believe that the IRS' processes for ensuring that security controls are implemented before systems are deployed failed because key organizations did not consider the known security vulnerabilities to be significant,[3] which affected vulnerability resolution and system deployment decisions. Specifically, the CADE and AMS project offices did not prevent and resolve known security vulnerabilities before deployment of the systems. The Customer Service Executive Steering Committee,[4] which has final milestone exit approval, 1) did not provide sufficient oversight to ensure that security controls were implemented, and 2) signed off unconditionally on CADE milestones despite the existence of weaknesses repeatedly reported to the Committee. Finally, the Cybersecurity organization recommended–and the system owners accepted–the risks

[2] Milestones provide for "go/no-go" decision points in a project and are sometimes associated with funding approval to proceed.

[3] We believe these security vulnerabilities to be significant because they affect the systems' abilities to 1) restrict access to only those individuals with a business need, 2) monitor activities for questionable transactions, 3) protect data from unauthorized disclosure, and 4) ensure continued operation of the systems. We also believe that the significance of these security vulnerabilities is heightened because the CADE and the AMS are critical modernized systems that will affect the future success of the IRS' computing environment. In addition, the National Institute of Standards and Technology specifies a minimum baseline of security controls that all Federal Government systems must address to ensure compliance with Federal security standards.

[4] The charter for this Committee shows that its primary objective is to ensure that project objectives are met, risks are managed appropriately, and the expenditure of enterprise resources is fiscally sound.

associated with these vulnerabilities by accrediting[5] the systems. We disagree with the system owners' acceptance of what we consider excessive risks for these security vulnerabilities, particularly the inabilities to successfully recover the systems and their data in the event of a disaster and to detect malicious security events and unauthorized accesses to taxpayer data.

Since 1997, the IRS has designated computer security as a material weakness.[6] In addition, the IRS continues to struggle with addressing security vulnerabilities on its modernized systems. We identified some of these same vulnerabilities in prior audit reports on the CADE and other modernization projects. The IRS agreed with most of our findings and responded that it would ensure that security control requirements were planned for early in the Enterprise Life Cycle[7] process, and it was committed to addressing its deficiencies in modernized systems. Until security control vulnerabilities are corrected, the IRS is jeopardizing the confidentiality, integrity, and availability of the massive volume of taxpayer data processed and stored by the CADE and the AMS.

Recommendations

We recommended that the Director, Business Modernization Office, and the Director, Customer Service, as the Co-Chairs of the Customer Service Executive Steering Committee, consider all security vulnerabilities–including those associated with general support systems–that affect the overall security of the CADE and the AMS before approving unconditional milestone exits. The CADE and AMS Project Managers should provide more emphasis on preventing and resolving security vulnerabilities identified during Enterprise Life Cycle processes.

The Wage and Investment Division Directors of the CADE and the AMS, in their roles as system owners, should approve interim authorities to operate when significant security control weaknesses exist in system environments. These interim authorities to operate should contain specific terms and conditions in accordance with IRS policy. The Associate Chief Information Officer, Cybersecurity, should 1) recommend interim authorities to operate when significant

[5] Accreditation is the official management decision given by the owner of an information system to authorize the operation of the system and to explicitly accept the risks.

[6] The Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. §§ 1105, 1113, 3512 (2000)) requires that each Federal Government agency conduct annual evaluations of its systems of internal accounting and administrative control and submit an annual statement on the status of the agency's system of management controls. As part of the evaluations, agency managers identify control areas that can be considered material weaknesses. The Department of the Treasury has defined a material weakness as, "shortcomings in operations or systems which, among other things, severely impair or threaten the organization's ability to accomplish its mission or to prepare timely, accurate financial statements or reports." Material weaknesses are reported outside the agency and thus receive additional oversight.

[7] A structured business systems development method that requires the preparation of specific work products during different phases of the development process.

security vulnerabilities exist in system environments, and 2) continue efforts to improve the accuracy and completeness of risk information in the security assessment reports by listing the general support system controls that are not yet implemented in the system environment and documenting concurrence by appropriate offices when reporting that vulnerabilities identified during milestone reviews have been corrected.

Response

The IRS agreed with our recommendations. It will continue to follow the governance process documented in the Customer Service Executive Steering Committee charter and consider all security vulnerabilities to ensure that best practices are in place for the successful delivery of project security and functionality. The IRS will continue to follow the existing Enterprise Life Cycle processes for identifying, confirming, and resolving security vulnerabilities at the requirements, design, development, and testing life cycle stages, with an increased emphasis in both preventing and resolving security vulnerabilities identified during the Enterprise Life Cycle processes. It will also strengthen its process for capturing and documenting all Executive Steering Committee meeting minutes.

The IRS will continue to follow existing policy to issue interim authorities to operate with appropriate timelines when significant control weaknesses exist in system environments. The Cybersecurity organization has modified the certification and accreditation process to include documented concurrence by the Information Technology Security Architecture and Engineering Office and/or the Office of Privacy, Information Protection, and Data Security when reporting in security assessment reports that vulnerabilities identified during milestone reviews have been corrected. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment

Although the IRS agreed with all of our recommendations, the related corrective actions for the first four recommendations are focused on continuing to follow existing processes or strengthening current processes. As stated in the report, we believe that the existing security vulnerabilities were not caused by process deficiencies. Instead, IRS offices did not carry out their responsibilities for ensuring that security weaknesses were corrected before deployment.

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

Abbreviations

AMS	Account Management Services
CADE	Customer Account Data Engine
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
PII	Personally identifiable information

Background

The Internal Revenue Service (IRS) stores sensitive financial and personal information for more than 130 million individual taxpayers who file annual Federal income tax returns. Each tax return contains personally identifiable information (PII), such as the filer's name, address, and Social Security Number. Because of the volume of data it maintains, the IRS is an attractive target for criminals intent on committing identity theft by stealing and using someone else's identity for their own financial gain. To address public concern about the proper storage of taxpayer data, the IRS is subject to certain security restrictions and requirements.

Like all Federal Government agencies, the IRS should protect its computer systems by implementing appropriate security controls to ensure the confidentiality, integrity, and availability of sensitive data, as recommended in National Institute of Standards and Technology (NIST)[1] Special Publication 800-53.[2] NIST Special Publication 800-53 specifies the minimum baseline of security controls that all Federal Government information systems must address, based on each system's security categorization level of high, moderate, or low. These security controls include system access, audit logging, and contingency planning.

In addition, the IRS is specifically required by Federal law to keep taxpayer data confidential and to prevent unauthorized disclosure or browsing of taxpayer records. Section 6103 of the Internal Revenue Code[3] prohibits the disclosure of tax returns and tax return information and requires that the storage of such information be secure and the access restricted to only those persons whose duties and responsibilities require access. The Taxpayer Browsing Protection Act of 1997[4] also provides criminal penalties and civil remedies to help ensure that tax returns and tax return information remain confidential. These requirements apply to all IRS computer systems that maintain sensitive data. For the IRS, two of its most important modernized systems are the Customer Account Data Engine (CADE) and the Account Management Services (AMS).

The CADE will provide the foundation for managing taxpayer accounts to achieve the IRS modernization vision. It consists of databases and related applications that will replace the IRS' existing Master File[5] processing system, which is the current primary repository of taxpayer

[1] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
[2] *Recommended Security Controls for Federal Information Systems*, Revision 1, published December 2006.
[3] 26 U.S.C. Section (§) 6103.
[4] 26 U.S.C.A. §§ 7213, 7213A, 7431 (West 2006).
[5] The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.

information. Initiated in September 1999, the CADE project had cost more than $490 million as of June 2007 and is scheduled to cost more than $1 billion to develop, operate, and maintain through Calendar Year 2012. The CADE is being incrementally developed over multiple releases[6] and will deploy two releases per year–a midyear release to cover new functionalities and a year-end release to cover tax law changes and maintenance.

In July 2004, the first release of the CADE began processing the simplest Income Tax Returns for Single and Joint Filers With No Dependents (Form 1040EZ). The second and third releases of the CADE added increased functionality, and future releases are scheduled to provide additional functionalities so that the CADE can eventually house the account information of more than 200 million individual and business taxpayers. From January 1 to April 22, 2008, the CADE posted 28.1 million tax returns (19.8 percent of the total 141.8 million filed) and issued 26.8 million refunds (28.8 percent of the total 93.2 million issued) totaling more than $41.7 billion (18.3 percent of the total $228.2 billion refunded). These results significantly surpass the 11.2 million returns posted by the CADE for all of Calendar Year 2007. In addition, the CADE was able to support timely issuance of payments to millions of taxpayers mandated by the Economic Stimulus Act of 2008[7] beginning after the height of the filing season[8] and with limited lead time for preparation.

The IRS is also developing the AMS system. When we started our review, the AMS was being designed to interface with the CADE, much like the Integrated Data Retrieval System[9] currently does with the Master File. During our review, the scope of the AMS was changed. The AMS will provide faster and improved access by employees to taxpayer account data, which will minimize taxpayer interaction and provide more timely responses to and resolution of taxpayer inquiries. Initiated in August 2006, the AMS project is scheduled to cost more than $700 million to develop, operate, and maintain through Calendar Year 2024. The first release of the AMS, deployed in October 2007, was limited to achieving address changes in the CADE environment. As of January 2008, 1,000 of 120,000 address change requests could be completed in the CADE environment in real time, while the others were changed in the Master File.

This review was performed at the office of the Chief Information Officer in New Carrollton, Maryland, during the period September 2007 through April 2008. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our

[6] A release is a specific edition of software.
[7] Pub. L. No. 110-185, 122 Stat. 613.
[8] The period from January through mid-April when most individual income tax returns are filed.
[9] IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer’s account records.

finding and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Internal Revenue Service Organizations and Oversight Groups Did Not Consider Known Security Vulnerabilities to Be Significant Enough to Either Resolve the Vulnerabilities or Deploy the Systems With Conditional Restrictions

The IRS has established appropriate system development policies and procedures that require security and privacy safeguards to be planned for and designed in the early phases of a system's development life cycle, called the Enterprise Life Cycle[10] at the IRS. To ensure that projects progress satisfactorily toward implementation of all security and privacy requirements, the IRS implemented various evaluations that developmental projects must undergo prior to exiting the different milestones[11] of the Enterprise Life Cycle. These evaluations include milestone reviews performed by the Office of Privacy, Information Protection, and Data Security (the Office of Privacy), the Information Technology Security Architecture and Engineering Office (the Security Engineering Office), and the Cybersecurity organization. In addition, the IRS annually updates the security and privacy control requirements that all new and existing information systems must address to comply with current NIST guidance. For new systems, the goals of these requirements and evaluations are to ensure that 1) security has been considered and built into systems, and 2) no system is deployed with significant security vulnerabilities.

Despite these requirements, our review of available test documents provided by the IRS showed that both the CADE and the AMS were deployed with known security vulnerabilities. The following security control vulnerabilities were identified by the Office of Privacy, the Security Engineering Office, and the Cybersecurity organization during testing of CADE Release 2.2, which was deployed in January 2007, and Release 3.1, which was deployed in August 2007:

- ***Security events and unauthorized access to taxpayer accounts by privileged CADE users were not captured***. Privileged users, such as system administrators, have the ability to access, modify, and delete information on a computer system. This security weakness means that any activities by a privileged user, such as illegal browsing, changes, or theft of taxpayer data, might go undetected.

[10] A structured business systems development method that requires preparation of specific work products during different phases of the development process.
[11] Provide for "go/no-go" decision points in a project and are sometimes associated with funding approval to proceed.

- ***Contractors could make changes to system configuration settings without notice, approval, or security checks***. Lack of configuration management restrictions increases the likelihood that an unauthorized user could gain access to the CADE and alter configuration settings to improperly manipulate taxpayer data.

- ***The CADE Disaster Recovery Plan and the Information Technology Contingency Plan had not been sufficiently tested***. Weaknesses in contingency planning and disaster recovery activities might hinder efforts to recover the CADE and its data in the event of a disaster.

- ***Backup tapes from the offsite storage facility were not tested at the original site or alternative site***. Backup tapes should be tested regularly to ensure that data are being stored correctly and that files can be restored without errors or lost data.

- ***Interconnection Security Agreements were not in place or did not contain complete and current interface information***. Failure to agree on the security and use of interconnection data among Federal Government agencies might compromise the confidentiality, accuracy, validity, and availability of CADE data.

- ***The CADE did not have the ability to identify and process all error codes***. Receipt of too many error codes at one time could overwhelm the CADE and bring the system to a halt.

- ***The CADE development staff did not test security features before releasing the application code***. If required security testing is not performed before the release of new updates to the CADE, any flaws in the application code could go undetected and threaten the confidentiality, availability, and integrity of the system data.

- ***Vulnerability scans of the mainframe computer on which the CADE resides identified one high-risk failure and several configurations that were not sufficient for protecting taxpayer data. These vulnerabilities were not corrected.*** Allowing these vulnerabilities to remain on the mainframe computer exposes the CADE to unnecessary risks.

- ***The CADE did not employ an application-specific vulnerability scanning tool***. If vulnerability scanning is not performed at the application level, known vulnerabilities might go undetected and expose the application to unnecessary risk for the confidentiality, availability, and integrity of the system data.

- ***The system did not automatically terminate a session after 15 minutes of inactivity***. An insufficient timeout mechanism allows a user to remain logged into a system for extended periods without re-authenticating his or her session, particularly if the user walks away from the computer without locking it. This situation increases the risk of an unauthorized user gaining undetected access to the application.

- ***Malicious code protection was not implemented***. The CADE might be vulnerable to malicious code attacks, such as computer viruses.
- ***PII data were transmitted in clear text within Computing Centers***.[12] Failure to protect the integrity of transmitted information could allow unauthorized viewing of information and exposes the IRS to unnecessary risks.
- ***CADE PII data backed up on tapes, disks, and compact discs, and data shared with external agencies, were not encrypted***. Failure to protect the integrity of stored or shared information could allow unauthorized access to the information and exposes the IRS to unnecessary risks.
- ***Unauthorized access to PII could occur in mainframe computer memory, disk space, and tapes because the data were not removed before the media were reused***. Failure to properly remove taxpayer data from system memory devices before reuse increases the risk of unauthorized access to PII.
- ***The CADE did not have adequate controls to ensure that only a minimal amount of PII required for the particular CADE release was collected, stored, transferred, and processed***. The CADE was not complying with Federal privacy laws[13] that require computer systems to collect no more information with respect to taxpayers and IRS employees than is necessary and relevant for tax administration and other legally mandated or authorized purposes.
- ***The CADE was using live data in more than 18 test environments for application development testing, but the system owner did not properly describe how the CADE will acquire, use, and dispose of the live data***. As a result, the risk of improper disclosure of PII was increased.

The following security control vulnerabilities were identified by the Security Engineering Office and the Cybersecurity organization during testing of AMS Release 1.1, which was deployed in October 2007:

- ***Auditing controls were not sufficient to identify security-related events and unauthorized access to taxpayer information***. Activities such as illegal browsing, changes, or theft of taxpayer files might go undetected.
- ***Procedures were not implemented for disabling inactive accounts***. Persons no longer needing access to carry out responsibilities and persons with a malicious intent could use the accounts to gain unauthorized access to the system.

[12] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.
[13] Privacy Act of 1974, 5 U.S.C. § 552a (2000).

- ***The system did not automatically terminate a session after 15 minutes of inactivity***. An insufficient timeout mechanism allows a user to remain logged into a system for extended periods without re-authenticating his or her session, particularly if the user walks away from the computer without locking it. This situation increases the risk that an unauthorized user might gain undetected access to the application.
- ***No alternate processing site had been established for the AMS***. In the event of an area-wide disruption or disaster, availability of the AMS could be affected.
- ***The application error log contained Taxpayer Identification Numbers, risking accidental or intentional disclosure***. Capturing Taxpayer Identification Numbers in an error log unnecessarily exposes the data to accidental or intentional disclosure, which might result in identity theft and other unlawful use of the data.
- ***The operating system hosting the AMS was determined to have only a 77.8 percent compliance rate with required security settings, including 5 high-risk failures***. Noncompliant configurations could leave the infrastructure as well as the application open to known and unknown security threats that could affect the confidentiality, integrity, and availability of the application and the PII it processes and stores.

Missing security controls in the CADE and the AMS relate mainly to the protection of sensitive data, system access, audit logging,[14] and disaster recovery. These security weaknesses increase the risks that 1) an unscrupulous person, with little chance of detection, could gain unauthorized access to the vast amount of taxpayer information the IRS processes, and 2) the systems could not be recovered effectively and efficiently during an emergency. Until security control vulnerabilities are corrected, the IRS is jeopardizing the confidentiality, integrity, and availability of the massive volume of taxpayer data processed and stored by the CADE and the AMS.

Management Action: Subsequent to our audit fieldwork, the IRS advised us that 11 of the 22 security vulnerabilities mentioned previously had been either corrected during subsequent releases or determined not to be vulnerabilities after deployment, and actions were being taken to address the remaining 11 security vulnerabilities. We plan to perform a followup review to evaluate the effectiveness of the IRS' corrective actions.

[14] An audit log is a chronological record of activities that allow for the reconstruction, review, and examination of a transaction from inception to final results. Audit logs can be used to detect unauthorized accesses to computer networks.

We believe these security vulnerabilities to be significant because they affect the systems' abilities to 1) restrict access to only those individuals with a business need, 2) monitor activities for questionable transactions, 3) protect data from unauthorized disclosure, and 4) ensure continued operation of the systems. We also believe that the significance of these security vulnerabilities is heightened because the CADE and the AMS are critical modernized systems that will affect the future success of the IRS' computing environment. In addition, the NIST specifies a minimum baseline of security controls that all Federal Government systems must address to ensure compliance with Federal security standards.

We identified two areas of concern regarding why these systems were deployed with significant security vulnerabilities. Specifically:

- The CADE and AMS project offices did not ensure that the security vulnerabilities were adequately prevented and resolved once they were identified, and the Customer Service Executive Steering Committee[15] approved milestone exits without giving adequate consideration to what we view as significant security vulnerabilities on the systems.
- The Cybersecurity organization recommended–and the CADE and the AMS system owners approved–that the systems be fully accredited[16] without giving adequate consideration to what we view as significant security vulnerabilities on the systems.

Prevention and resolution of security vulnerabilities were not given adequate consideration prior to deployment of the systems

NIST Special Publication 800-53 specifies the recommended security controls for all Federal Government information systems. The IRS mandated that any business unit developing an information system must ensure that the system project office for the development effort has adequate security engineering expertise to properly address the planning and implementation of the minimum security controls required for protection of the data residing on its systems. Because of the criticality of both the CADE and the AMS, the IRS established specific project offices for both systems. The project offices should ensure that security controls have been implemented and security vulnerabilities have been mitigated or resolved during the Enterprise Life Cycle and prior to deployment.

Throughout the Enterprise Life Cycle, the Customer Service Executive Steering Committee is responsible for final exit approval at each milestone. This Committee consists of 14 IRS executives from the Wage and Investment Division and the Modernization and Information

[15] The charter for the Customer Service Executive Steering Committee shows that its primary objective is to ensure that project objectives are met, risks are managed appropriately, and the expenditure of enterprise resources is fiscally sound.

[16] Accreditation is the official management decision given by the owner of an information system to authorize the operation of the system and to explicitly accept the risks.

Technology Services organization. It is co-chaired by an executive from this Division and organization. Governance by the Customer Service Executive Steering Committee includes 1) ensuring that projects adhere to accepted principles and practices of the Enterprise Life Cycle, and 2) resolving enterprise-wide issues for its projects, such as the CADE and the AMS.

The decision to approve a milestone exit is based on the recommendation from the Enterprise Life Cycle Program Management Office, which conducts milestone readiness reviews. When significant security or privacy concerns exist, a conditional milestone exit may be recommended. This type of exit generally requires that the condition be corrected prior to the next milestone exit. Otherwise, the Customer Service Executive Steering Committee will give an unconditional exit approval, and the system development proceeds to the next milestone effort.

Despite these requirements and key milestone decision points, we found that most of the security vulnerabilities discussed previously were identified repeatedly during CADE milestone reviews and were not corrected. Rather, they were carried over from milestone to milestone and even from release to release. The continued existence of these security vulnerabilities indicates that security controls were not sufficiently considered by the project office and built into the systems during the Development Phase of later releases.

In addition to not building in security controls during the Development Phase, the CADE project office did not resolve the security vulnerabilities previously discussed and, as a result, the CADE was deployed with these vulnerabilities. Seven of the 16 CADE security vulnerabilities were attributable to the project office and should have been addressed by the project office. The other nine CADE security vulnerabilities related to general support systems[17] or enterprise-wide deficiencies. The project office advised us that it was not responsible for addressing these security control weaknesses because the weaknesses were beyond its system boundaries and authority to address, and the project office assumed that the owners of the nine general support systems on which the CADE relies were responsible for implementing many of its required security and privacy controls.

Of the six security vulnerabilities on the AMS, the project office was responsible for two, which it should have addressed. The other four security vulnerabilities were related to general support systems or enterprise-wide deficiencies.

[17] A general support system is an interconnected set of information resources under the same direct management control that shares common functionality and normally includes hardware, software, data, applications, communications, and people.

NIST Special Publication 800-18, Revision 1,[18] specifies that if a system is defined as a major application,[19] such as the CADE and the AMS, and the application is run on a general support system, the major application owner is responsible for acceptance of risk and must ensure that the system security plan of the general support system provides adequate protection for the application and its data. In addition, more recent NIST draft guidance specifies that if the general support system or common controls do not provide the security controls required by the individual information system, the project office should take appropriate actions to supplement those controls as required for any protection deficits that result at the system level.

Regardless of who was responsible for implementing the various security controls, we believe that the Customer Service Executive Steering Committee was in the best position to ensure that all significant security vulnerabilities were resolved or mitigated prior to deployment. Unfortunately, for the security vulnerabilities mentioned previously, the Customer Service Executive Steering Committee did not 1) provide sufficient oversight to ensure that security controls were implemented, and 2) did not consider the security vulnerabilities significant enough to place conditional restrictions on the release or delay the systems' releases all together. As a result, it signed off unconditionally on CADE milestones despite the existence of repeatedly reported security weaknesses.

Of the security vulnerabilities discussed previously, we are most concerned about the lack of audit logs and disaster recovery capabilities in modernized systems. It might be understandable that older legacy systems cannot log transactions or comply with other current security and privacy requirements, such as disaster recovery capabilities, due to older computer equipment. However, the IRS should ensure that these requirements are included in modernized systems. According to the NIST,[20] any effort to install logging capabilities or other security controls after deployment of a system will likely cost significantly more than if the security capabilities had been successfully designed into the system during the system Development Phase.

We believe that the lack of attention to security controls during the Development Phase can be traced to other business requirements, filing season pressures, and deployment demands. These concerns have taken precedence over security concerns, and executive-level management was not adequately engaged in security needs and requirements. Consequently, the CADE reached rollout dates without security controls, and accreditation officials were put in the position of implementing a critical system with significant security flaws rather than delaying the deployment.

[18] *Guide for Developing Security Plans for Federal Information Systems*, published February 2006.
[19] An application is the use of information resources (information and information technology) to satisfy a specific set of user requirements. A major application contains, processes, stores, or transmits information critical to the agency's mission.
[20] *Security Considerations in the Information System Development Life Cycle* (NIST Special Publication 800-64 Revision 1, published June 2004).

The IRS continues to struggle with addressing security vulnerabilities on its modernized systems. We identified some of these same vulnerabilities in prior audit reports on the CADE and other modernization projects. Specifically, in 2005 we reported that the IRS was not adequately considering security controls early enough in the Development Phase of a system.[21] We identified several inadequate security controls that should have been addressed in the Development Phase, including security configurations, audit logs, and disaster recovery plans. In 2004 and 2006, we reported that audit logs for IRS modernized systems were not functioning.[22] The IRS agreed with most of our findings and responded that it would ensure that security control requirements were planned for early in the Enterprise Life Cycle process, and it was committed to addressing its deficiencies in audit logging on modernized systems.

The systems were accredited despite the existence of several known security vulnerabilities

The last step of the developmental process and the most critical key decision point prior to deployment of a system is the accreditation by the system owner. In making the decision to accredit information systems, the system owner essentially accepts the risk of the system and approves the deployment and operation of the system. The system owner can give the system an authority to operate, give an interim authority to operate for a period of time until significant deficiencies are corrected, or prevent the system from deploying. The system owner bases his or her accreditation decisions on several certification documents.

During the certification process, the Cybersecurity organization develops the test plan based on the system security plan, performs the testing of application-specific security controls, and provides the results in the security assessment report. The Cybersecurity organization also issues a certification memorandum that provides a summary of the certification results and a recommendation for the system owner to grant the authority to operate, grant interim authority to operate, or deny authority to operate.

Despite the presence of what we believe were significant unresolved security vulnerabilities on the systems, the system owners did not consider the security vulnerabilities to be significant enough to either give an interim authority to operate or delay deployment, and they gave authorities to operate for the CADE and the AMS. We disagree with the system owners' acceptance of what we consider excessive risks for these security vulnerabilities, particularly the inabilities to successfully recover the systems and their data in the event of a disaster and to detect malicious security events and unauthorized accesses to taxpayer data. The current

[21] *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems* (Reference Number 2005-20-128, dated August 2005).
[22] *The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning* (Reference Number 2004-20-135, dated August 2004) and *Improvements Are Needed to Ensure the Use of Modernization Applications Is Effectively Audited* (Reference Number 2006-20-177, dated September 29, 2006).

cyber-threat environment in the Federal Government dictates the need for any significant system to have these capabilities.

We believe that the CADE and the AMS should have been given interim authorities to operate due to what we view as significant security vulnerabilities present on the systems. Further, the CADE should not be approved to operate if the significant security vulnerabilities require extended remediation time. In making the accreditation, the CADE system owner considered only those controls for which the owner was directly responsible. However, the decision to accredit should not be made in isolation and should be made with regard to agency-wide business process considerations and the interconnections with other systems, such as the general support systems.

We also disagree with the CADE and the AMS certification memoranda issued by the Associate Chief Information Officer, Cybersecurity, which recommended that the system owners grant an authority to operate. While the certification memoranda mentioned the existence of security vulnerabilities on the systems, the memorandum for the earlier CADE Release 2.2 stated, "With your commitment to develop a plan to address and ultimately resolve all identified risks for the CADE application timely, I am recommending you grant an Authorization to Operate for the CADE application." The later CADE Release 3.1 had most of the same security vulnerabilities. We believe that the system owners relied heavily on the Cybersecurity organization's recommendation as well as the Customer Service Executive Steering Committee's exit approvals during the Enterprise Life Cycle.

The recommendations in the certification memoranda are based on security assessment reports. However, we found that the security assessment reports provided only summary-level security vulnerability information for general support systems and contained incomplete and erroneous security control implementation status. As a result, the system owners might not have known the full extent of the risks they were accepting when authorizing the CADE and the AMS to operate.

In addition, since 1997, the IRS has designated computer security as a material weakness,[23] which the IRS has segregated into nine separate vulnerability areas: 1) network access controls; 2) key computer applications and system access controls; 3) software configuration; 4) functional business, operating, and program units security roles and responsibilities; 5) segregation of duties between system and security administrators; 6) contingency planning and disaster recovery;

[23] The Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. §§ 1105, 1113, 3512 (2000)) requires that each Federal Government agency conduct annual evaluations of its systems of internal accounting and administrative control and submit an annual statement on the status of the agency's system of management controls. As part of the evaluations, agency managers identify control areas that can be considered material weaknesses. The Department of the Treasury has defined a material weakness as, "shortcomings in operations or systems which, among other things, severely impair or threaten the organization's ability to accomplish its mission or to prepare timely, accurate financial statements or reports." Material weaknesses are reported outside the agency and thus receive additional oversight.

7) monitoring of key networks and systems; 8) security training; and 9) certification and accreditation. While the IRS is working toward closing these areas, we believe that the existence of the computer security material weakness needs to be considered when making decisions on system deployments.

We also believe that the IRS goal to certify and accredit all of its systems adversely affected the agency's ability to objectively evaluate the security posture of its systems, especially for the CADE and the AMS. NIST Special Publication 800-37[24] specifically states that systems with interim authorities to operate cannot be considered accredited. As a result, the existence of systems with interim authorities to operate might affect the agency in the following ways:

- The E-Government section in the President's Management Agenda initiative pertains to the certification and accreditation of systems. Using the color-coded rating to determine success levels, the President's Management Agenda allows an agency to achieve the optimum "green" status only if the agency maintained 100 percent of its systems as certified and accredited.

- The Federal Information Security Management Act[25] includes an evaluative section on the agency's number of systems that have been certified and accredited. This percentage affects the agency's overall grade.

- The Office of Management and Budget requires completion of the Exhibit 300[26] to comply with the Clinger-Cohen Act of 1996.[27] Any operational system that has not been certified and accredited might not have its proposed budget approved for funding by the Office of Management and Budget.

Recommendations

Recommendation 1: The Director, Business Modernization Office, and the Director, Customer Service, serving as the Co-Chairs of the Customer Service Executive Steering Committee, should consider all security vulnerabilities–including those associated with general support systems–that affect the overall security of the CADE and the AMS before approving milestone exits. Equal emphasis should be placed on security and functionality.

[24] *Guide for the Security Certification and Accreditation of Federal Information Systems*, published May 2004.
[25] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[26] The Exhibit 300 is a detailed budget justification that information technology system owners must complete and submit annually to the Office of Management and Budget.
[27] (Federal Acquisition Reform Act of 1996) (Information Technology Management Reform Act of 1996), Pub. L. No. 104-106, 110 Stat. 642 (codified in scattered sections of 5 U.S.C., 5 U.S.C. app., 10 U.S.C., 15 U.S.C., 16 U.S.C., 18 U.S.C., 22 U.S.C., 28 U.S.C., 29 U.S.C., 31 U.S.C., 38 U.S.C., 40 U.S.C., 41 U.S.C., 42 U.S.C., 44 U.S.C., 49 U.S.C., 50 U.S.C.).

Management's Response: The IRS agreed with this recommendation. It will continue to follow the governance process documented in the Customer Service Executive Steering Committee charter and consider all security vulnerabilities to ensure that best practices are in place for the successful delivery of project security and functionality.

Recommendation 2: The CADE and AMS Project Managers should provide more emphasis on both preventing and resolving security vulnerabilities identified during Enterprise Life Cycle processes.

Management's Response: The IRS agreed with this recommendation. It will continue to follow the existing Enterprise Life Cycle processes for identifying, confirming, and resolving security vulnerabilities at the requirements, design, development, and testing life cycle stages, with an increased emphasis on both preventing and resolving security vulnerabilities identified during the Enterprise Life Cycle processes. The IRS will also strengthen its process for capturing and documenting all Executive Steering Committee meeting minutes.

Recommendation 3: The Wage and Investment Division Directors of the CADE and the AMS, in their roles as system owners, should approve interim authorities to operate when significant security control weaknesses exist in system environments. These interim authorities to operate should contain specific terms and conditions in accordance with IRS policy, including corrective actions to be taken by the information system owners and a required time period for completion of the corrective actions, before authorities to operate are granted.

Management's Response: The IRS agreed with this recommendation. It will continue to follow existing policy to issue interim authorities to operate with appropriate timelines when significant control weaknesses exist in system environments.

Recommendation 4: The Associate Chief Information Officer, Cybersecurity, should recommend interim authorities to operate when significant security vulnerabilities exist in system environments.

Management's Response: The IRS agreed with this recommendation. The Cybersecurity organization has been recommending interim authorities to operate when significant security vulnerabilities exist in system environments as a standard part of the IRS certification and accreditation process.

Recommendation 5: The Associate Chief Information Officer, Cybersecurity, should continue efforts to improve the accuracy and completeness of risk information in the security assessment reports by listing the general support system controls that are not yet implemented in the system environment and documenting concurrence by the Security Engineering Office and the Office of Privacy when reporting that vulnerabilities identified during milestone reviews have been corrected.

Management's Response: The IRS agreed with this recommendation. The Cybersecurity organization has modified the certification and accreditation process to include documented concurrence by the Security Engineering Office and/or the Office of Privacy when reporting in security assessment reports that vulnerabilities identified during milestone reviews have been corrected. The Cybersecurity organization will update its standard operating procedures to incorporate these process changes and will continue to strengthen the process by including the relevant general support system Plan of Action and Milestones as an attachment to each application security assessment report.

Office of Audit Comment: Although the IRS agreed with all of our recommendations, the related corrective actions for the first four recommendations are focused on continuing to follow existing processes or strengthening current processes. As stated in the report, we believe that the existing security vulnerabilities were not caused by process deficiencies. Instead, IRS offices did not carry out their responsibilities for ensuring that security weaknesses were corrected before deployment.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of the review was to determine whether appropriate security controls have been implemented in the CADE and the AMS systems.[1] To accomplish our objective, we:

I. Determined whether appropriate security controls had been considered and included in the CADE and the AMS.

   A. Reviewed the security categorization criteria prescribed by Federal Information Processing Standards Publication 199[2] and NIST Special Publication 800-60[3] and determined whether the security categorizations the IRS assigned to the CADE and the AMS were documented and supported.

   B. Compared the minimum security controls in NIST Special Publication 800-53[4] to the security controls listed in the system security plans for CADE Releases 2.2 and 3.1 and AMS Release 1.1 and determined whether all minimum security controls were included.

   C. Determined whether security controls were integrated early enough in CADE Releases 2.2 and 3.1 and AMS Release 1.1 system development life cycles to be cost effective.

II. Determined whether the security controls were fully tested as prescribed in NIST Special Publication 800-37[5] by an independent test team.

III. Determined whether the security assessment reports were prepared in accordance with NIST Special Publication 800-37.

IV. Obtained supporting documentation for closed recommendations in two prior Treasury Inspector General for Tax Administration reports[6] and determined whether corrective actions were completed and effective.

[1] The CADE will provide the foundation for managing all taxpayer accounts and will replace existing tax processing systems. The AMS will provide faster and improved access by employees to taxpayer account data.
[2] *Standards for Security Categorization of Federal Information and Information Systems*, published February 2004.
[3] *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume 1, published June 2004.
[4] *Recommended Security Controls for Federal Information Systems*, Revision 1, published December 2006.
[5] *Guide for the Security Certification and Accreditation of Federal Information Systems*, published May 2004.
[6] *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems* (Reference Number 2005-20-128, dated August 2005) and *Improvements Are Needed to Ensure the Use of Modernization Applications Is Effectively Audited* (Reference Number 2006-20-177, dated September 29, 2006).

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Preston B. Benoit, Acting Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Jody Kitazono, Lead Auditor
Alan Beber, Senior Auditor
Bret Hunter, Senior Auditor
Louis Lee, Senior Auditor
Midori Ohno, Senior Auditor
Joan Raniolo, Senior Auditor

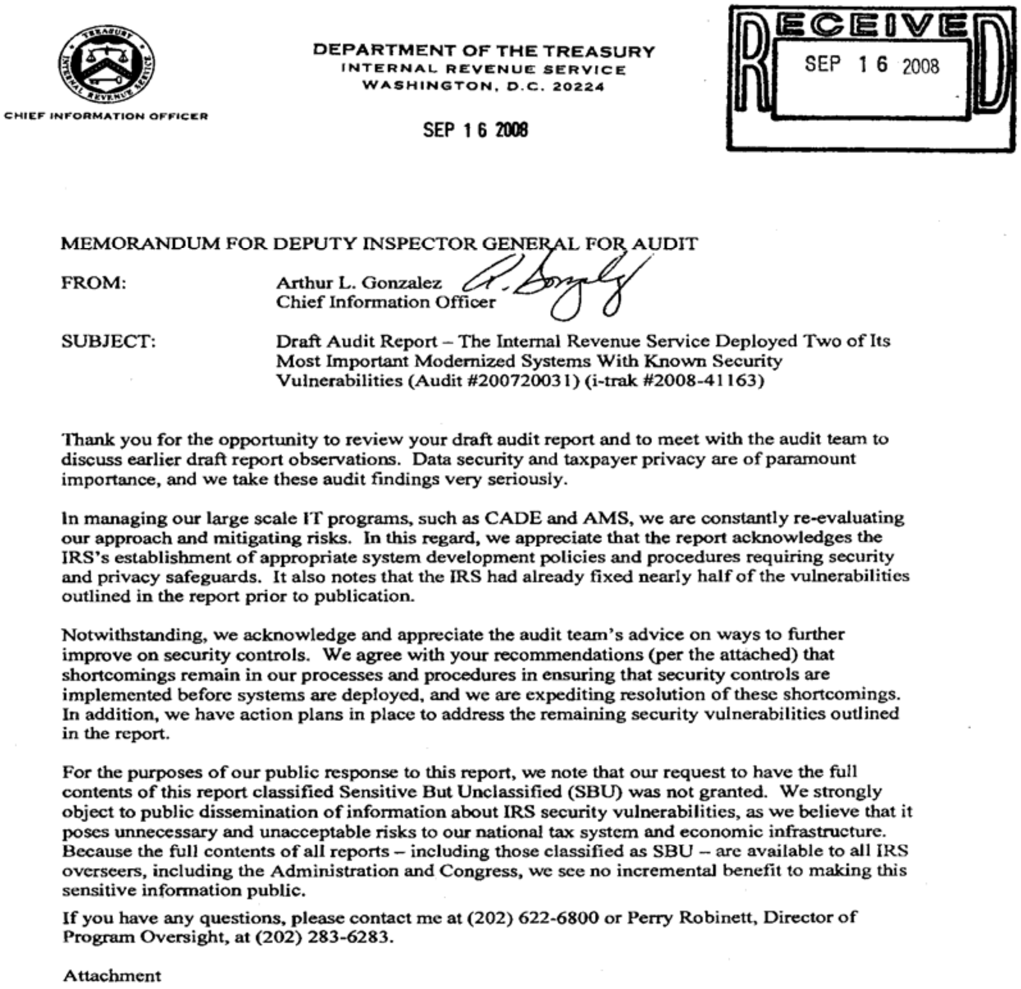
Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Chief Information Officer OS:CIO
Deputy Commissioner, Wage and Investment Division SE:W
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:CPIC:IC
Audit Liaisons:
    Commissioner, Wage and Investment Division SE:W
    Chief Information Officer OS:CIO

Appendix IV

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

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

SEP 16 2008

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Arthur L. Gonzalez
Chief Information Officer

SUBJECT: Draft Audit Report – The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities (Audit #200720031) (i-trak #2008-41163)

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss earlier draft report observations. Data security and taxpayer privacy are of paramount importance, and we take these audit findings very seriously.

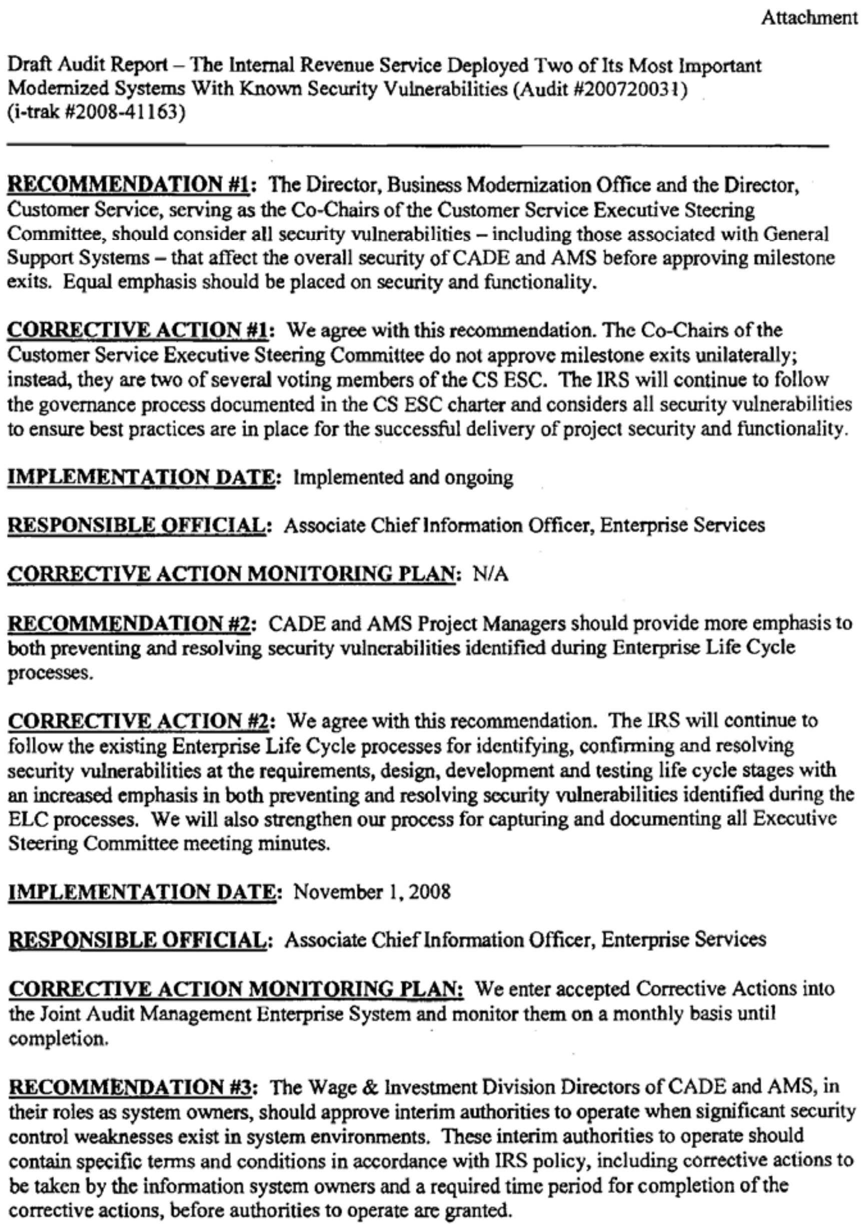
In managing our large scale IT programs, such as CADE and AMS, we are constantly re-evaluating our approach and mitigating risks. In this regard, we appreciate that the report acknowledges the IRS's establishment of appropriate system development policies and procedures requiring security and privacy safeguards. It also notes that the IRS had already fixed nearly half of the vulnerabilities outlined in the report prior to publication.

Notwithstanding, we acknowledge and appreciate the audit team's advice on ways to further improve on security controls. We agree with your recommendations (per the attached) that shortcomings remain in our processes and procedures in ensuring that security controls are implemented before systems are deployed, and we are expediting resolution of these shortcomings. In addition, we have action plans in place to address the remaining security vulnerabilities outlined in the report.

For the purposes of our public response to this report, we note that our request to have the full contents of this report classified Sensitive But Unclassified (SBU) was not granted. We strongly object to public dissemination of information about IRS security vulnerabilities, as we believe that it poses unnecessary and unacceptable risks to our national tax system and economic infrastructure. Because the full contents of all reports – including those classified as SBU – are available to all IRS overseers, including the Administration and Congress, we see no incremental benefit to making this sensitive information public.

If you have any questions, please contact me at (202) 622-6800 or Perry Robinett, Director of Program Oversight, at (202) 283-6283.

Attachment



Attachment

Draft Audit Report – The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities (Audit #200720031)
(i-trak #2008-41163)

RECOMMENDATION #1: The Director, Business Modernization Office and the Director, Customer Service, serving as the Co-Chairs of the Customer Service Executive Steering Committee, should consider all security vulnerabilities – including those associated with General Support Systems – that affect the overall security of CADE and AMS before approving milestone exits. Equal emphasis should be placed on security and functionality.

CORRECTIVE ACTION #1: We agree with this recommendation. The Co-Chairs of the Customer Service Executive Steering Committee do not approve milestone exits unilaterally; instead, they are two of several voting members of the CS ESC. The IRS will continue to follow the governance process documented in the CS ESC charter and considers all security vulnerabilities to ensure best practices are in place for the successful delivery of project security and functionality.

IMPLEMENTATION DATE: Implemented and ongoing

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #2: CADE and AMS Project Managers should provide more emphasis to both preventing and resolving security vulnerabilities identified during Enterprise Life Cycle processes.

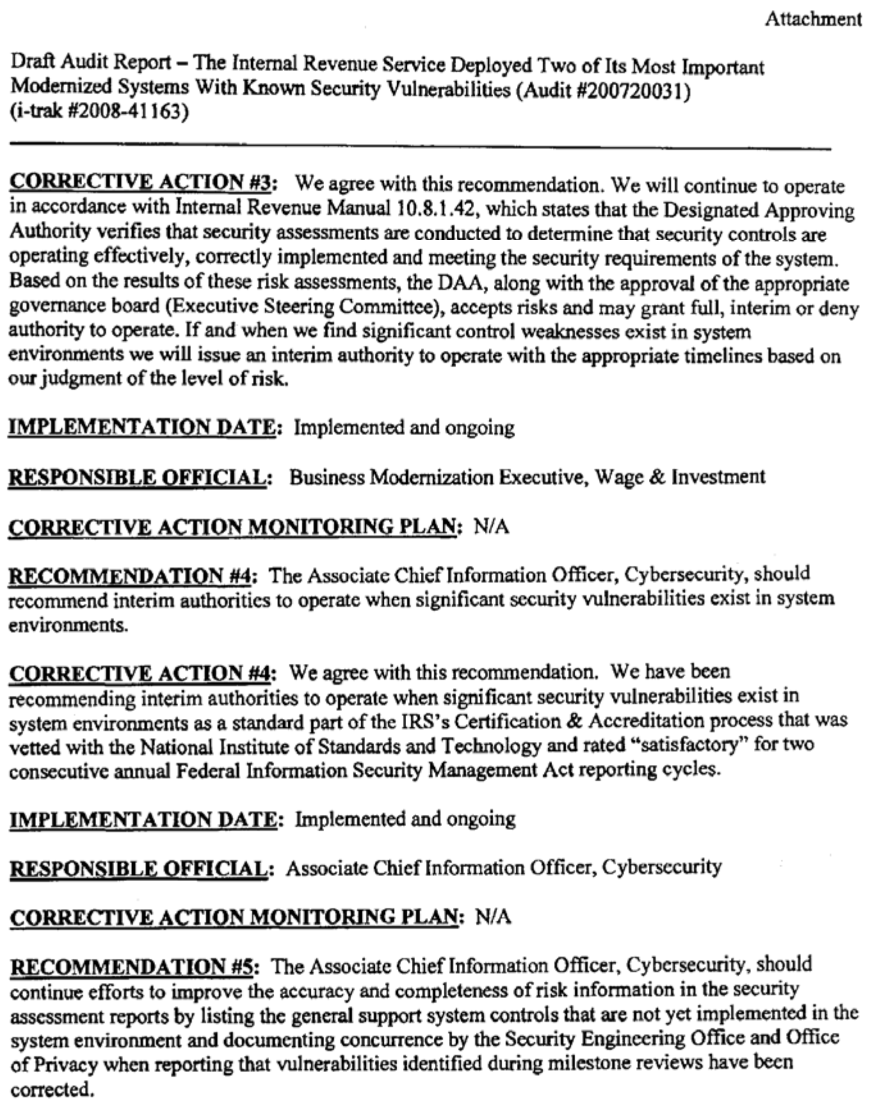
CORRECTIVE ACTION #2: We agree with this recommendation. The IRS will continue to follow the existing Enterprise Life Cycle processes for identifying, confirming and resolving security vulnerabilities at the requirements, design, development and testing life cycle stages with an increased emphasis in both preventing and resolving security vulnerabilities identified during the ELC processes. We will also strengthen our process for capturing and documenting all Executive Steering Committee meeting minutes.

IMPLEMENTATION DATE: November 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Wage & Investment Division Directors of CADE and AMS, in their roles as system owners, should approve interim authorities to operate when significant security control weaknesses exist in system environments. These interim authorities to operate should contain specific terms and conditions in accordance with IRS policy, including corrective actions to be taken by the information system owners and a required time period for completion of the corrective actions, before authorities to operate are granted.



Attachment

Draft Audit Report – The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities (Audit #200720031)
(i-trak #2008-41163)

CORRECTIVE ACTION #3: We agree with this recommendation. We will continue to operate in accordance with Internal Revenue Manual 10.8.1.42, which states that the Designated Approving Authority verifies that security assessments are conducted to determine that security controls are operating effectively, correctly implemented and meeting the security requirements of the system. Based on the results of these risk assessments, the DAA, along with the approval of the appropriate governance board (Executive Steering Committee), accepts risks and may grant full, interim or deny authority to operate. If and when we find significant control weaknesses exist in system environments we will issue an interim authority to operate with the appropriate timelines based on our judgment of the level of risk.

IMPLEMENTATION DATE: Implemented and ongoing

RESPONSIBLE OFFICIAL: Business Modernization Executive, Wage & Investment

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #4: The Associate Chief Information Officer, Cybersecurity, should recommend interim authorities to operate when significant security vulnerabilities exist in system environments.

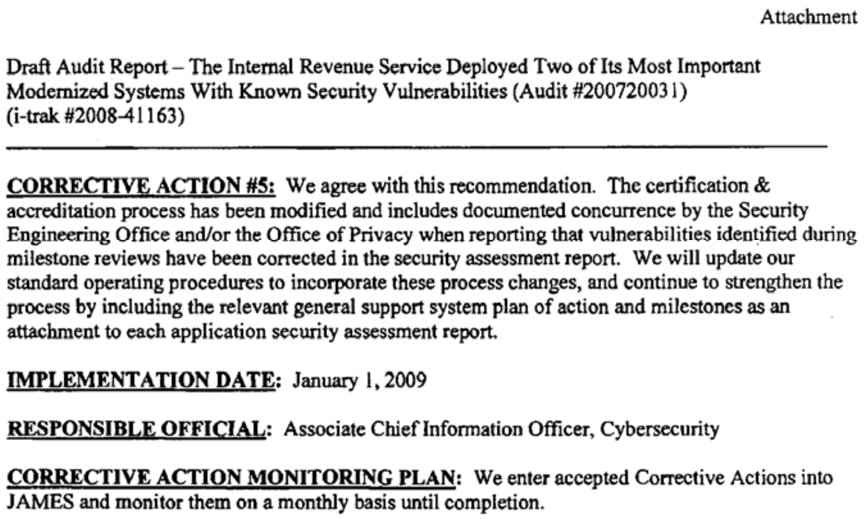
CORRECTIVE ACTION #4: We agree with this recommendation. We have been recommending interim authorities to operate when significant security vulnerabilities exist in system environments as a standard part of the IRS's Certification & Accreditation process that was vetted with the National Institute of Standards and Technology and rated "satisfactory" for two consecutive annual Federal Information Security Management Act reporting cycles.

IMPLEMENTATION DATE: Implemented and ongoing

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #5: The Associate Chief Information Officer, Cybersecurity, should continue efforts to improve the accuracy and completeness of risk information in the security assessment reports by listing the general support system controls that are not yet implemented in the system environment and documenting concurrence by the Security Engineering Office and Office of Privacy when reporting that vulnerabilities identified during milestone reviews have been corrected.



Attachment

Draft Audit Report – The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities (Audit #200720031)
(i-trak #2008-41163)

CORRECTIVE ACTION #5: We agree with this recommendation. The certification & accreditation process has been modified and includes documented concurrence by the Security Engineering Office and/or the Office of Privacy when reporting that vulnerabilities identified during milestone reviews have been corrected in the security assessment report. We will update our standard operating procedures to incorporate these process changes, and continue to strengthen the process by including the relevant general support system plan of action and milestones as an attachment to each application security assessment report.

IMPLEMENTATION DATE: January 1, 2009

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into JAMES and monitor them on a monthly basis until completion.