TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Internal Revenue Service Deployed the Modernized e-File System With Known Security Vulnerabilities

December 30, 2008

Reference Number: 2009-20-026

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.

Redaction Legend:

2(f) = Law Enforcement - Risk circumvention of Agency regulation or statute

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

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

December 30, 2008

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION
CHIEF TECHNOLOGY OFFICER

Nancy A. Nakamura

FROM: *(for)* Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Deployed the Modernized e-File System With Known Security Vulnerabilities (Audit # 200720024)

This report presents the results of our review to determine whether appropriate security controls have been implemented in the Modernized e-File (MeF) system. 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 MeF system will provide a single method for filing all IRS tax returns, information returns, forms, and schedules via the Internet. The Modernized Tax Return Database (M-TRDB), a component of the MeF system, is the authoritative store of accepted returns and extensions submitted through the MeF system. Security weaknesses in the controls over system access, monitoring of system access, and disaster recovery have continued to exist even though key phases of the MeF system and the M-TRDB 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 phases are put into operation.

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

We believe that these security vulnerabilities are significant because they affect the IRS' ability 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. Many of these same vulnerabilities have been designated as a bureau-wide material weakness by the IRS. The significance of these security vulnerabilities is heightened because the MeF system is a critical modernized system that will affect the future success of the IRS computing environment.

The MeF project office did not prevent and resolve known security vulnerabilities before deployment of the system. The Submission Processing Executive Steering Committee,[1] which has final milestone[2] exit approval authority, 1) did not provide sufficient oversight to ensure that security controls were implemented and 2) signed off unconditionally on MeF system milestones despite the existence of weaknesses repeatedly reported to the Committee. Finally, the Cybersecurity organization recommended, and the MeF system owner approved, that the system be fully accredited[3] without giving adequate consideration of what we view as significant security vulnerabilities on the system. In our opinion, the system owner's acceptance of the excessive risks associated with these security vulnerabilities was not reasonable.

We identified some of these same vulnerabilities in prior audit reports on modernization projects, including a September 2008 report on the Customer Account Data Engine and the Account Management Services.[4] IRS management agreed with most of our prior report findings and responded that they would ensure that security control requirements were planned for early in the

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

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

[3] 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.

[4] *The Audit Trail System for Detecting Improper Activities on Modernized Systems Is Not Functioning* (Reference Number 2004-20-135, dated August 2004), *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems* (Reference Number 2005-20-128, dated August 2005), *Improvements Are Needed to Ensure the Use of Modernization Applications Is Effectively Audited* (Reference Number 2006-20-177, dated September 29, 2006), and *The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities* (Reference Number 2008-20-163, dated September 24, 2008).

Enterprise Life Cycle[5] process and that they were committed to addressing deficiencies in audit logging on modernized systems. Until security control vulnerabilities are corrected, the IRS is jeopardizing the confidentiality, integrity, and availability of an increasing volume of tax information for millions of taxpayers as MeF system phases are put into operation.

Recommendations

We recommended that the Submission Processing Executive Steering Committee consider all security vulnerabilities that affect the overall security of the MeF system and the M-TRDB before approving milestone exits. The Commissioner, Wage and Investment Division, and the Chief Information Officer should provide more emphasis to the MeF project office to both prevent and resolve security vulnerabilities identified during Enterprise Life Cycle processes.

The Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division, as the MeF system owner, 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 that must be met, 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.

Response

IRS management agreed with our recommendations. They will continue to follow the governance process documented in the Submission Processing Executive Steering Committee charter, which includes the review of all security vulnerabilities, before milestone exits. They 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. They will also strengthen the process for capturing and documenting Executive Steering Committee meeting minutes.

IRS management will continue to operate in accordance with policies and procedures, which state that the Designated Approving Authority verifies that security assessments are conducted to determine that security controls are operating effectively, correctly implemented, and meeting security requirements of the system. If and when they find that significant control weaknesses exist in the system environments, they will issue an interim authority to operate with the appropriate timelines based on the level of risk. Management's complete response to the draft report is included as Appendix IV.

[5] The Enterprise Life Cycle is a structured business systems development method that requires preparation of specific work products during different phases of the development process.

Office of Audit Comment

Although the IRS agreed with all of our recommendations, its related corrective actions 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, Acting Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-8510.

Table of Contents

Appendices

Abbreviations

IRS	Internal Revenue Service
MeF	Modernized e-File
M-TRDB	Modernized Tax Return Database
NIST	National Institute of Standards and Technology

Background

The Internal Revenue Service (IRS) is currently undergoing a modernization effort to update its tax processing systems. One of its three[1] most important modernized systems is the Modernized e-File (MeF) system. The MeF system will provide a single method for filing all IRS tax returns, information returns, forms, and schedules via the Internet. The Modernized Tax Return Database (M-TRDB), a component of the MeF system, is the authoritative store of accepted returns and extensions submitted through the MeF system. The key drivers for the MeF system are to allow the IRS to collect more tax documents electronically and reduce the costs associated with the inefficiencies of paper documents and manual processing, while enhancing customer service and increasing availability of taxpayer information. Internet-based filing directly supports the goal of revolutionizing how taxpayers transact and communicate with the IRS.

The Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division, is the functional owner of the MeF system. The MeF system is being incrementally developed over multiple releases.[2] The first release of the MeF system was originally deployed in January 2004 for the filing season.[3] The system is scheduled to cost $673 million to develop, operate, and maintain through Fiscal Year 2020, which is the project's planned completion date. Release 4 of the MeF system, which was deployed in January 2007, allows for the processing of the U.S. Return of Partnership Income (Form 1065) and associated forms and schedules[4] for Tax Year 2006 submissions. Previous releases of the MeF added the Return of Organization Exempt From Income Tax (Form 990); the U.S. Corporation Income Tax Return (Form 1120); and the Application for Automatic 6-Month Extension of Time To File Certain Business Income Tax, Information, and Other Returns (Form 7004). Future releases will add the redesigned Form 990 and the U.S. Individual Income Tax Return (Form 1040).

The MeF system is 1 of more than 200 computer systems maintained by the IRS to administer the nation's tax system. The IRS stores sensitive financial and personal information for more than 130 million individual taxpayers who file annual Federal income tax returns. Each tax

[1] The three projects at the heart of the IRS Business Systems Modernization program are the Modernized e-File, the Customer Account Data Engine, and the Account Management Services systems.
[2] A release is a specific edition of software.
[3] The period from January through mid-April when most individual income tax returns are filed.
[4] This adds electronic file submission support for partnerships so that they might submit partnership-related forms in the same way and through the same process as exempt organizations and corporations currently do through the MeF system.

return contains personally identifiable information,[5] such as the filer's name, address, Social Security Number, and other personal information. Because of the volume of data it maintains, the IRS is an attractive target for criminals with the intent to commit identity theft by stealing and using someone else's identity for their own financial gain.

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 the National Institute of Standards and Technology (NIST)[6] Special Publication 800-53.[7] This Publication specifies the minimum baseline of security controls that all Federal information systems must address, based on the security categorization level for a system of high, moderate, or low. These security controls include system access, audit logging, and contingency planning.

The IRS is specifically required by Federal law to keep taxpayer data confidential and prevent unauthorized disclosure or browsing of taxpayer records. Section 6103[8] of the Internal Revenue Code prohibits the disclosure of tax returns and tax return information and requires that the storage of such information be secured and restricted to only persons whose duties and responsibilities require access. The Taxpayer Browsing Protection Act of 1997[9] also provided 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.

This review was performed at the offices of the Chief Information Officer in New Carrollton, Maryland, and the Enterprise Computing Center in Martinsburg, West Virginia, during the period September 2007 through August 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 findings 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.

[5] Personally identifiable information is any information that can potentially be used to uniquely identify, contact, or locate a single person.
[6] 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.
[7] *Recommended Security Controls for Federal Information Systems*, Revision 1 published December 2006.
[8] 26 U.S.C. Section 6103.
[9] 26 U.S.C.A. Sections 7213, 7213A, 7431 (West 2006).

Results of Review

Security Vulnerabilities Were Not Given Sufficient Attention During the Development and Accreditation of the Modernized e-File System

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] 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 the MeF system was deployed with known security vulnerabilities. For the MeF system and its database component, the M-TRDB, the following 13 security control vulnerabilities were identified by the Office of Privacy, the Security Engineering Office, and the Cybersecurity organization during testing of its Release 4, which was deployed in January 2007.

1. **Unauthorized users had direct access to the MeF system management console,**[12] **which provided system administrative functionalities such as the ability to change security settings and web services configurations. Any IRS employee with access to the Intranet could login to the console.** Unauthorized access to the MeF system management console increases the risk that the application might be compromised.

2. **Security configuration settings on the MeF system servers and database were not sufficiently restrictive.** Weak configuration management leaves the database susceptible

[10] The Enterprise Life Cycle is a structured business systems development method that requires preparation of specific work products during different phases of the development process.
[11] Milestones provide for "go/no-go" decision points in a project and are sometimes associated with funding approval to proceed.
[12] The IBM WebSphere® Console is used to process web services requests and remote applications belonging to transmitters or State Governments.

to known exploitable vulnerabilities as well as potentially allowing unauthorized modifications to its data.

3. **Information input restrictions for State Government electronic tax filings were not in place on the MeF system.** Without strict information input restrictions, the MeF system might accept invalid data from State transmitters, which could affect the integrity of MeF system data.
4. **The processes for establishing and confirming user identification on the MeF system did not meet Federal Government standards for accrediting cryptographic modules.**[13] Weak identification and authentication controls increase the risk that an unauthorized user might gain undetected access to the MeF system and compromise the confidentiality, accuracy, validity, and availability of application data.
5. **Database users had more access privileges than they needed to carry out their responsibilities.** Unnecessary access privileges increase the risk that an unauthorized user might gain undetected access to the MeF system and compromise the confidentiality, accuracy, validity, and availability of application data.
6. **After the maximum number of consecutive unsuccessful login attempts, the MeF system did not enforce automatic account locks on user accounts for a minimum of 24 hours in accordance with IRS policies. The account lockout feature was set to** 2(f) [redacted] An insufficient lockout mechanism allows a user multiple attempts to gain access to a system, thus increasing the risk that the application data might be compromised.
7. **Several database user accounts had multiple invalid password settings that were not in accordance with IRS policy.** Weak authentication controls increase the opportunity for an unauthorized user to gain access to the application, thus increasing the risk that the application data might be compromised.
8. **System users with limited access needs were granted full access to database records. Also, database administrator privileges were provided to non-database administrative personnel.** Weak identification controls increase the opportunity for an unauthorized user to gain access to the application, thus increasing the risk that the application data might be compromised.
9. **The MeF system and database have a number of audit log**[14] **weaknesses, including 1) all required auditable events are not being captured, 2) no official has been**

[13] The Federal Information Processing Standard 140-2 is a Federal Government computer security standard used to accredit cryptographic modules (i.e., practice or study of hiding information).

[14] An audit log is a chronological record of activities that allows 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.

assigned to monitor and maintain system audit mechanisms, 3) no database audit reduction tools were used, and 4) certain users that should have limited access have full capabilities to access database records, including taxpayer information. Without proper audit controls, system compromise could go undetected, resulting in prolonged unauthorized access that could otherwise be restricted or prevented. Consequently, the confidentiality, integrity, and availability of the taxpayer records maintained by the MeF system could be affected.

10. **An audit log review process was not in place, and logs were not being reviewed by MeF system officials.** Weak supervision and review of user activities increases the opportunity for a user to perform undesirable actions that could go undetected by organization officials.
11. **An alternate processing site agreement had not been established for the MeF system.** To ensure the continued operation of the system in the event of a failure or disaster, written agreements should be in place to continue processing at an alternate site.
12. **Reports containing personally identifiable information were transmitted in clear text.** Failure to protect the integrity of transmitted information could allow unauthorized access to the information and exposes the IRS to unnecessary risks.
13. **System and database administrators used insecure methods to transmit MeF system data within the IRS.** Failure to comply with security configuration standards and requirements could permit an attacker to compromise the confidentiality, integrity, and availability of the system and its data.

Missing security controls in the MeF system relate mainly to system access, audit logging, disaster recovery, and the protection of sensitive data. These security vulnerabilities increase the risks that an unscrupulous person could gain unauthorized access to the vast amount of taxpayer information the IRS processes with little chance of detection and that the system 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 an increasing volume of tax information for millions of taxpayers as application phases are put into operation.

We believe that these security vulnerabilities are significant because they affect the IRS' ability 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. Many of these same vulnerabilities have been designated as a bureau-wide material weakness[15] by the IRS. We also believe that the significance of these security vulnerabilities is heightened because the MeF system is a critical modernized system that will affect the future success of the IRS computing environment. If these issues are not addressed on modernized systems, these weaknesses will continue to exist.

***Management Action**: Subsequent to our audit fieldwork, the IRS provided us with the current status of the 13 vulnerabilities cited in our report. We plan to perform a followup review to evaluate the effectiveness of the IRS' corrective actions.*

- *Seven security vulnerabilities (numbers 1, 2, 4, 5, 7, 8, and 11) have been resolved.*
- *Two security vulnerabilities (numbers 3 and 12) were found to be invalid and closed.*
- *Two security vulnerabilities (numbers 6 and 13) are unresolved, with one of the vulnerabilities (number 13) to be resolved when MeF Release 5.5 deploys in January 2009.*
- *One security vulnerability (number 9) is partially resolved, with the remaining actions to be completed in Fiscal Year 2009.*
- *One security vulnerability (number 10) is being addressed by the Wage and Investment Division Office of Electronic Tax Administration and Refundable Credits and the Cybersecurity organization to develop a process to enable the review of exception audit reports. Additional time is required to complete this process, and the target completion date is December 31, 2008.*

We identified two areas of concern as to why the MeF system was deployed with significant security vulnerabilities.

- The MeF project office did not prevent and resolve known security vulnerabilities before deployment of the system, and the Submission Processing Executive Steering Committee[16] approved milestone exits without giving adequate consideration to what we view as significant security vulnerabilities on the system.

[15] The Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. Sections 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."

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

- The Cybersecurity organization recommended, and the MeF system owner approved, that the system be fully accredited[17] without giving adequate consideration to what we view as significant security vulnerabilities on the system.

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

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 the MeF system development, the IRS established a specific project office for the system. The project office 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 Submission Processing Executive Steering Committee has the responsibility for final exit approval at each milestone. This Committee consists of 15 IRS executives from all business operating divisions and is co-chaired by an executive from the Wage and Investment Division and the Modernization and Information Technology Services organization. Governance by the Committee includes ensuring that projects adhere to accepted principles and practices of the Enterprise Life Cycle and resolving enterprise-wide issues for its projects, such as the MeF system.

The decisions to approve milestone exits are 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 might be recommended and generally requires that the condition be corrected prior to the next milestone exit. Otherwise, the Submission Processing Executive Steering Committee will approve an unconditional exit approval and the system development proceeds to the next milestone effort.

As an example, in April 2006, the Director, Security Engineering Office, issued a memorandum to the Director, Tax Administration Modernization, and the Director, Infrastructure Shared Services, recommending that MeF system Release 4, milestone 4a exit be postponed for 30 days. The postponement was due to two security risks traced in two prior releases (Release 3.2, milestone 4b and Release 4, milestone 2/3) and to the absence of a documented strategy with dates of implementation, which created a "high" risk scenario for the system. Once the documented strategy was provided, the milestone exit was approved even though the security weaknesses remained.

[17] 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.

Despite these requirements, we found that six[18] of the security vulnerabilities mentioned previously were identified repeatedly during MeF system milestone reviews and were not corrected. Rather, they were carried over from milestone to milestone, and some were even carried over from release to release. The Submission Processing Executive Steering Committee, which has final milestone exit approval, signed off unconditionally on MeF system milestones despite the existence of weaknesses repeatedly reported by the Security Engineering Office and the Cybersecurity organization. The existence of these security vulnerabilities since earlier releases indicates that security controls might not have been sufficiently considered during the development phase of the system.

We believe that the Submission Processing 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 discussed previously, the Committee 1) did not provide sufficient oversight to ensure that security controls were implemented and 2) decided to deploy the release despite the presence of repeatedly reported significant security vulnerabilities, as opposed to placing conditional restrictions on the release or delaying the system's release all together.

Of the security vulnerabilities discussed previously, we are most concerned about the lack of audit logs, access controls, and disaster recovery capabilities in modernized systems. While 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, the IRS should ensure that these requirements are included in modernized systems. According to the NIST,[19] 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 developmental phases 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 to ensure that security needs and requirements were being implemented. Consequently, the MeF system 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 system deployment.

The IRS continues to struggle with addressing security vulnerabilities on modernized systems. We identified some of these same vulnerabilities in prior audit reports on modernization projects. Specifically, in Fiscal Year 2005, we reported that the IRS was not adequately considering

[18] Security control vulnerabilities numbers 1, 4, 9, 10, 11, and 13 listed on pages 3 through 5.

[19] *Security Considerations in the Information Development Life Cycle*, NIST Special Publication 800-64 Revision 1, published June 2004.

security controls early enough in the development phase of a system, including the MeF system.[20] 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 Fiscal Years 2004 and 2006, we reported that audit logs for IRS modernized systems, including the MeF system, were not functioning.[21] IRS management agreed with most of our findings and responded that they would ensure that security control requirements were planned for early in the Enterprise Life Cycle process and that they were committed to addressing deficiencies in audit logging on modernized systems.

In September 2008, we issued a report[22] regarding the deployment of the Customer Account Data Engine and the Account Management Services systems with known security vulnerabilities. Similar to this report, the September 2008 report raised concerns over decisions made to approve milestone exits and to accredit the systems for deployment.

The MeF system was 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 an information system, 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 the system an interim authority to operate for a period of time until significant deficiencies are corrected, or prevent the system from being deployed.[23] The system owner bases his or her accreditation decisions on several certification documents.

During the certification process, the Cybersecurity organization develops a test plan based on the system security plan, performs the testing of application-specific security controls, and provides the results in a security assessment report. The Cybersecurity organization also issues a certification memorandum that provides a summary of the certification results and

[20] *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernization Systems* (Reference Number 2005-20-128, dated August 2005).
[21] *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).
[22] *The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities* (Reference Number 2008-20-163, dated September 24, 2008).
[23] The NIST issued a draft revision to its *Guide for Security Authorization of Federal Information Systems* (Special Publication 800-37) in August 2008. This draft document will require only two options for a system authorization decision. An agency can either provide an authorization to operate or a denial of authorization to operate. The current "interim authority to operate" designation will be phased out and replaced with an authorization to operate with terms and conditions (i.e., limits and restrictions which must be followed by the system owner) and authorization termination time limits.

recommendation for the system owner to grant the authority to operate, grant an interim authority to operate, or deny the authority to operate.

Despite the presence of what we believe were significant unresolved security vulnerabilities on the MeF system, the system owner gave the authorities to operate for the system and its database component, the M-TRDB. In our opinion, the system owner should have given the MeF system an interim authority to operate in consideration of the excessive risk associated with these security vulnerabilities, particularly the inabilities to prevent modifying critical system security settings, 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 cyber-threat environment in the Federal Government dictates the need for any significant system to have these capabilities. As a result, we believe that the system owner's acceptance of excessive risk was not reasonable.

We also disagree with the MeF system certification memoranda issued by the Cybersecurity organization, which recommended that the system owner grant an authority to operate. While the certification memoranda mentioned the existence of security vulnerabilities on the systems, the memorandum for MeF Release 4 stated, "With your commitment to develop a plan to address and ultimately resolve all identified risks for the MeF application timely, I am recommending you grant an Authorization to Operate for the MeF application." We believe that the system owner relied heavily on the Cybersecurity organization's recommendation as well as the Submission Processing Executive Steering Committee's exit approvals during the Enterprise Life Cycle.

As stated previously, the IRS has designated computer security as a material weakness, 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; 7) monitoring of key networks and systems; 8) security training; and 9) certification and accreditation. By the IRS' own designation and admission, these computer security areas are materially important, meaning that any security vulnerability within these areas is significant. While the IRS is working toward addressing 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 organization's ability to objectively evaluate the security posture of its systems, specifically with the MeF system. 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.

[24] *Guide for the Security Certification and Accreditation of Federal Information Systems*, published May 2004.

- 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 number of agency 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 Submission Processing Executive Steering Committee should consider all security vulnerabilities, including those associated with general support systems, that affect the overall security of the MeF system and the M-TRDB before approving milestone exits.

> **Management's Response:** IRS management agreed with this recommendation. They will continue to follow the governance process documented in the Submission Processing Executive Steering Committee charter, which includes review of all security vulnerabilities, before milestone exits and will document milestone exit review discussions in the Submission Processing Executive Steering Committee meeting minutes.

Recommendation 2: The Commissioner, Wage and Investment Division, and the Chief Information Officer should provide more emphasis to both preventing and resolving security vulnerabilities identified during Enterprise Life Cycle processes to the MeF system project office.

> **Management's Response:** IRS management agreed with this recommendation. They will continue to follow the existing Enterprise Life Cycle processes for identifying, confirming, and resolving security vulnerabilities at the requirements, design, developmental, and testing life cycle stages, with an increased emphasis in both

[25] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[26] Exhibit 300 is the primary tool for capital planning and investment control in the Federal Government.
[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.).

preventing and resolving security vulnerabilities identified during the Enterprise Life Cycle. They will also strengthen the process for capturing and documenting meeting minutes.

Recommendation 3: The Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division, as the MeF system owner, 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 that must be met, 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.[28]

Management's Response: IRS management agreed with this recommendation. They will continue to operate in accordance with policies and procedures, which state that the Designated Approving Authority verifies that security assessments are conducted to determine that security controls are operating effectively, correctly implemented, and meeting security requirements of the system. If and when they find that significant control weaknesses exist in the system environments, they will issue an interim authority to operate with the appropriate timelines based on the level of risk.

Office of Audit Comment: Although the IRS agreed with all of our recommendations, its related corrective actions 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.

[28] As stated previously, the August 2008 draft NIST Special Publication 800-37 has replaced interim authority to operate with an authorization to operate with terms, conditions, and termination dates.

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 MeF system.[1] To accomplish our objective, we:

I. Determined whether appropriate security controls had been considered and included in the MeF system and the M-TRDB.

A. Reviewed the security categorization criteria prescribed by the *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standards Publication 199, published February 2004) and *Guide for Mapping Types of Information and Information Systems to Security Categories* (NIST Special Publication 800-60 Volume 1, published June 2004) and determined whether the security categorizations the IRS assigned to the MeF system and the M-TRDB were documented and supported.

B. Compared the minimum security controls in the *Recommended Security Controls for Federal Information Systems* (NIST Special Publication 800-53 Revision 1, published December 2006) to the security controls listed in the system security plans for the MeF system Release 4 and the M-TRDB and determined whether all minimum security controls were included.

C. Determined whether security controls were integrated early in MeF system Release 4 and the M-TRDB development life cycles to be cost effective.

II. Determined whether the security controls were fully tested by an independent test team as prescribed in the *Guide for the Security Certification and Accreditation of Federal Information Systems* (NIST Special Publication 800-37, published May 2004).

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

IV. Determined whether the MeF system and the M-TRDB are continually monitored to ensure that they are configured in accordance with the security policies.

V. Obtained supporting documentation for closed recommendations in two prior Treasury Inspector General for Tax Administration audit reports and determined whether

[1] The MeF system will provide a single method for filing all IRS tax returns, information returns, forms, and schedules via the Internet. The M-TRDB, a component of the MeF system, is the authoritative store of accepted returns and extensions submitted through the MeF system.

corrective actions were completed and effective. The two reports were *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, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Preston B. Benoit, Acting Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Esther Wilson, Lead Auditor
Charles Ekunwe, Senior Auditor
Jacqueline Nguyen, Senior Auditor

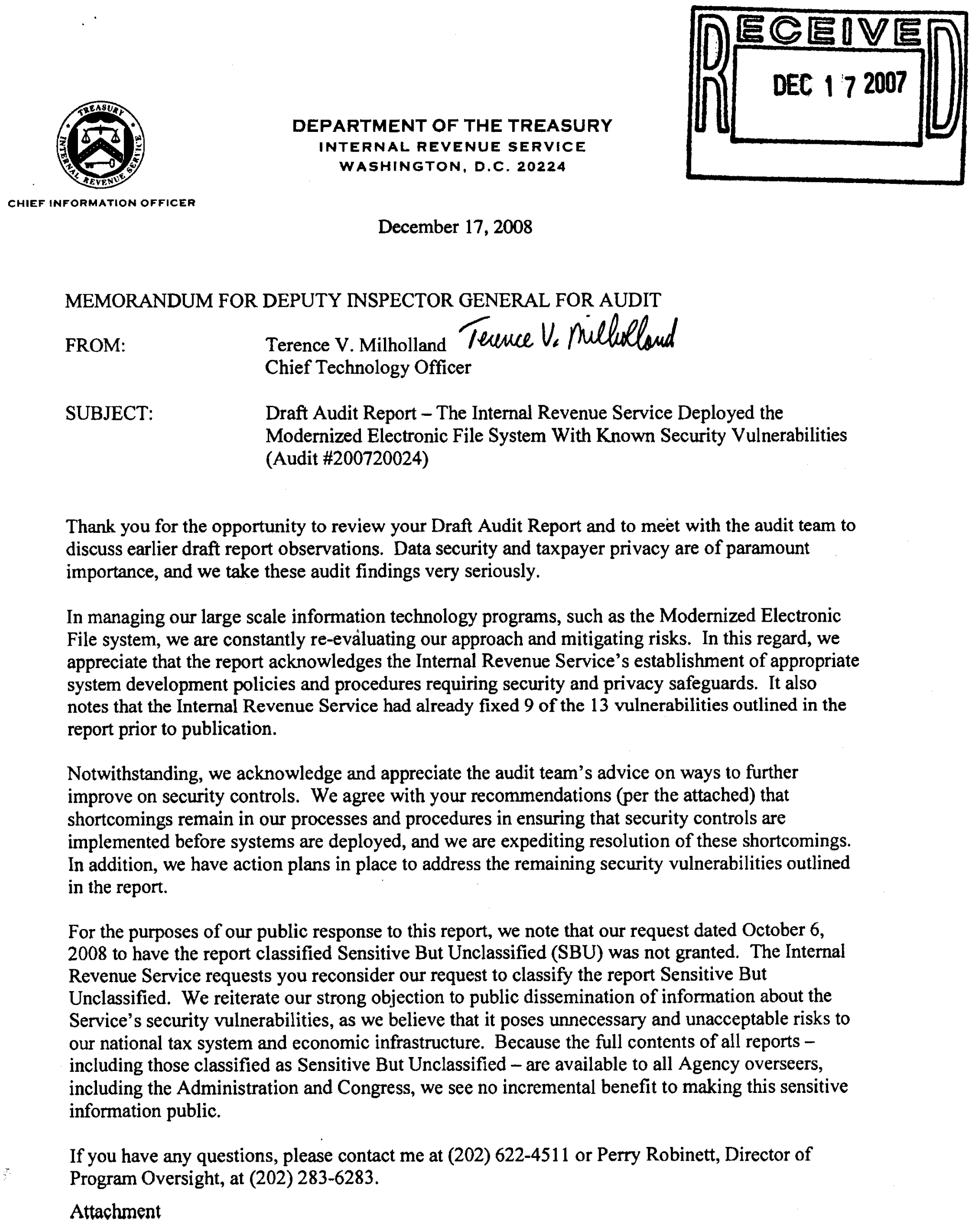
Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Chief Information Officer OS:CIO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
    Commissioner, Wage and Investment Division SE:W
    Chief Information Officer OS:CIO

Appendix IV

Management's Response to the Draft Report



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

CHIEF INFORMATION OFFICER

December 17, 2008

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – The Internal Revenue Service Deployed the Modernized Electronic File System With Known Security Vulnerabilities (Audit #200720024)

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.

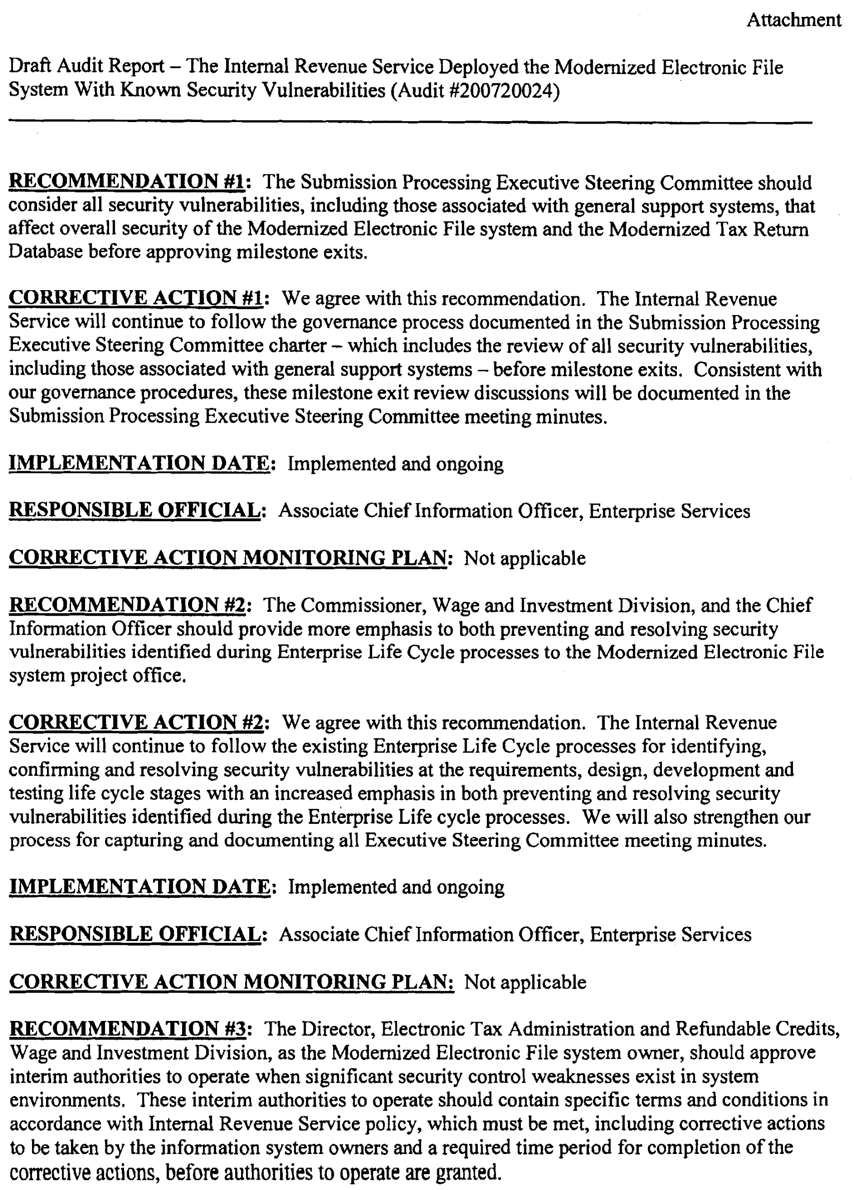
In managing our large scale information technology programs, such as the Modernized Electronic File system, we are constantly re-evaluating our approach and mitigating risks. In this regard, we appreciate that the report acknowledges the Internal Revenue Service's establishment of appropriate system development policies and procedures requiring security and privacy safeguards. It also notes that the Internal Revenue Service had already fixed 9 of the 13 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 dated October 6, 2008 to have the report classified Sensitive But Unclassified (SBU) was not granted. The Internal Revenue Service requests you reconsider our request to classify the report Sensitive But Unclassified. We reiterate our strong objection to public dissemination of information about the Service's 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 Sensitive But Unclassified – are available to all Agency 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) 622-4511 or Perry Robinett, Director of Program Oversight, at (202) 283-6283.

Attachment



Attachment

Draft Audit Report – The Internal Revenue Service Deployed the Modernized Electronic File System With Known Security Vulnerabilities (Audit #200720024)

RECOMMENDATION #1: The Submission Processing Executive Steering Committee should consider all security vulnerabilities, including those associated with general support systems, that affect overall security of the Modernized Electronic File system and the Modernized Tax Return Database before approving milestone exits.

CORRECTIVE ACTION #1: We agree with this recommendation. The Internal Revenue Service will continue to follow the governance process documented in the Submission Processing Executive Steering Committee charter – which includes the review of all security vulnerabilities, including those associated with general support systems – before milestone exits. Consistent with our governance procedures, these milestone exit review discussions will be documented in the Submission Processing Executive Steering Committee meeting minutes.

IMPLEMENTATION DATE: Implemented and ongoing

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: Not applicable

RECOMMENDATION #2: The Commissioner, Wage and Investment Division, and the Chief Information Officer should provide more emphasis to both preventing and resolving security vulnerabilities identified during Enterprise Life Cycle processes to the Modernized Electronic File system project office.

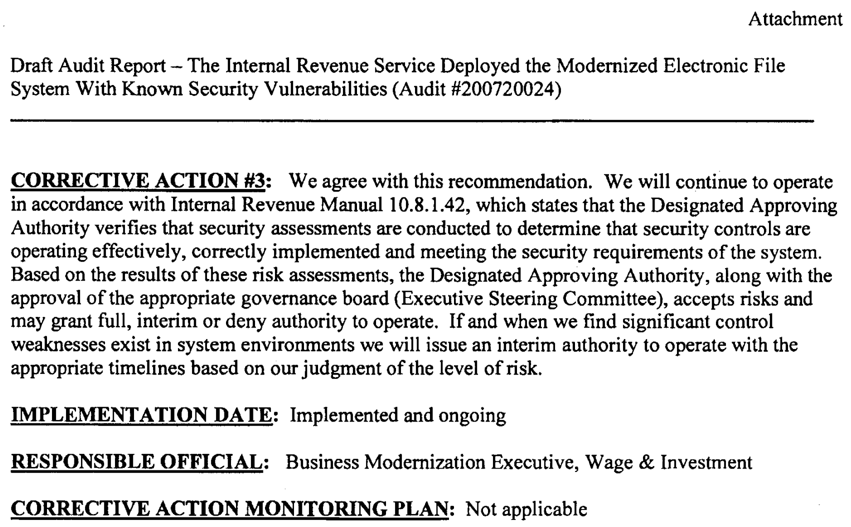
CORRECTIVE ACTION #2: We agree with this recommendation. The Internal Revenue Service will continue to follow the existing Enterprise Life Cycle processes for identifying, confirming and resolving security vulnerabilities at the requirements, design, development and testing life cycle stages with an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

IMPLEMENTATION DATE: Implemented and ongoing

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: Not applicable

RECOMMENDATION #3: The Director, Electronic Tax Administration and Refundable Credits, Wage and Investment Division, as the Modernized Electronic File system owner, 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 Internal Revenue Service policy, which must be met, 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 the Modernized Electronic File System With Known Security Vulnerabilities (Audit #200720024)

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 Designated Approving Authority, 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: Not applicable