A Complete Certification and Accreditation Is Needed to Ensure the Electronic Fraud Detection System Meets Federal Government Security Standards

September 29, 2006

Reference Number: 2006-20-178

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(d) = Law Enforcement Technique(s)
2(e) = Law Enforcement Procedure(s)

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 29, 2006

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

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – A Complete Certification and Accreditation Is Needed to Ensure the Electronic Fraud Detection System Meets Federal Government Security Standards (Audit # 200620040)

This report presents the results of our review to assess the effectiveness of security controls over the Electronic Fraud Detection System (EFDS) by evaluating its certification and accreditation (C&A) packages.

Impact on the Taxpayer

The EFDS, an automated compliance system, was designed to maximize fraud detection at the time tax returns are filed to prevent the issuance of questionable refunds. Security certifications conducted for the EFDS have been incomplete since October 2001, resulting in limited assurance that EFDS security controls are effective in protecting taxpayer information from unauthorized disclosure. This is especially significant because the EFDS contains the Internal Revenue Service's (IRS) second largest repository of taxpayer information.

Synopsis

The IRS uses its enforcement authority to collect taxes due from individuals who do not fulfill their tax obligations. The IRS Criminal Investigation function is responsible for detecting and investigating criminal violations of the Internal Revenue Code and financially related crimes. The EFDS is the primary system used by the Criminal Investigation function to identify questionable tax return refunds.

Since its initial development in 1995, the EFDS has gone through significant changes. The EFDS began as a client server application, allowing users to access the application through the IRS network. In June 2001, the IRS approved the conversion to a web-based application, which would enable users to access the EFDS through the IRS Intranet. While the web-based application was under development, the client server application continued to operate. The web-based application was expected to be available to process tax returns in 2006, so the client server application was shut down in December 2005. However, the web-based application never became operational. In April 2006, the IRS decided to restore the client server application to process tax returns in 2007.

Because the EFDS contains and processes highly sensitive taxpayer information, the security over the system is paramount to ensure all data are protected from unauthorized access and misuse. To ensure systems are secure, Federal Government Security Standards[1] dictate that all systems and applications be certified and accredited every 3 years or when major changes are made to the system. The Mission Assurance and Security Services (MA&SS) organization has responsibility to certify IRS systems. Part of that role is to ensure security controls are adequately tested. The system owner uses the results of those tests to authorize the system's operation and by doing so accepts the risks associated with that system.

Overall, the security controls for the EFDS have not been adequately tested since October 2001. As a result, system owners accredited the systems with only limited assurance that security controls were effective to protect taxpayer information from being inappropriately accessed or misused. Our review assessed three separate components of the EFDS: the client server application,[2] the web-based application,[3] and the computers supporting the EFDS application.

When the EFDS client server application was certified and accredited in August 2004, the testing to support the certification did not follow IRS policies and Federal Government Security Standards. Key application security controls were not tested. Instead, the C&A was based solely on the security of the supporting Windows-based operating system.

Tests were not adequate because the MA&SS organization omitted steps in the certification process in order to meet its goal of certifying and accrediting 100 percent of IRS systems by the end of Fiscal Year 2004. Emphasis was placed on ensuring system owners signed accreditation memoranda rather than performing adequate tests. In the fourth quarter of Fiscal Year 2004, the IRS certified and accredited 30 major applications, which included the EFDS, representing over one-half of its inventory of major applications at the time.

Prior to the IRS' decision to stop all development of the EFDS web-based application, we evaluated its January 2006 C&A to determine whether it met IRS security standards. We

[1] Appendix III to Office of Management and Budget Circular A-130, *Security of Federal Automated Information Resources.*
[2] The client server application allows users to access the EFDS system internally on the network.
[3] A system development effort that would allow users to access the EFDS via the IRS Intranet.

determined that required controls for data integrity, transmission confidentiality, and user authorization were not tested during the C&A process. As a result, the IRS had limited assurance that sensitive taxpayer information stored, processed, and transmitted by the EFDS web-based application would have been accurate, reliable, and protected from unauthorized access. The MA&SS organization again did not adequately follow the certification process in testing the EFDS because the implementation date for the system was imminent.

We also reviewed the August 2004 certification of computers supporting the EFDS application at the Enterprise Computer Center in Memphis, Tennessee. Certification testing identified that the IRS had not established the priority for when the EFDS application would be restored in the event of an emergency or significant service disruption. These priorities should be documented in a Business Impact Analysis. While this weakness has been outstanding since August 2004, the IRS does not consider it to be a high-risk issue and therefore is not monitoring its status. As a result, the priority that the EFDS application would be given after an emergency is uncertain, possibly affecting the Criminal Investigation function's ability to identify fraudulent returns. As of July 2006, the Enterprise Computing Center in Memphis, Tennessee, hosted [redacted] applications.

2(d),2(e)

Recommendations

We recommended the Chief, MA&SS, coordinate with the Chief, Criminal Investigation, to complete a full security C&A package for the EFDS client server application and supporting computers before the system is permitted to operate. In addition, if the EFDS web-based application is redeployed, any tests of security controls that are omitted from the C&A process should be fully disclosed and the associated risks explained in the body of the security testing and security assessment reports. Criteria should also be included for identifying compensating tests and establishing follow-up testing for omitted tests. Also, the Chief Information Officer should develop a Business Impact Analysis for the Enterprise Computer Center in Memphis, Tennessee, that places the EFDS at an appropriate priority among the other major applications at the Center.

Response

The IRS agreed with our findings and recommendations. The Chief, MA&SS, has begun the process for completing a full security C&A of the EFDS client server application, which will be conducted prior to the EFDS being placed into operation for the next tax filing season. In addition, the Chief, MA&SS, will update its processes to ensure that all security testing reports and security assessment reports for EFDS and all other IRS systems explain any omitted tests and the associated risks. The process will ensure criteria will be included for identifying compensating tests and establishing plans for follow-up testing for omitted control tests.

The Chief Information Officer will develop a Business Impact Analysis for the Enterprise Computing Center in Memphis, Tennessee. This process will include stakeholders, such as IRS

Business Operating Divisions, to determine the recovery priority for critical business processes and major applications. Management's complete response to the draft report is included as Appendix IV.

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

BIA	Business Impact Analysis
C&A	Certification and Accreditation
CI	Criminal Investigation
ECC-MEM	Enterprise Computing Center-Memphis
EFDS	Electronic Fraud Detection System
FY	Fiscal Year
IRS	Internal Revenue Service
MA&SS	Mission Assurance and Security Services
NIST	National Institute for Standards and Technology
POA&M	Plan of Actions and Milestones
PY	Processing Year

Background

The Internal Revenue Service (IRS) uses its enforcement authority to collect taxes due from individuals who do not fulfill their tax obligations. Noncompliance may not be deliberate and can stem from a wide range of causes, including lack of knowledge, confusion, poor record keeping, differing legal interpretations, unexpected personal emergencies, and temporary cash flow problems. However, some noncompliance may be willful, even to the point of criminal tax evasion. The IRS Criminal Investigation (CI) function is responsible for detecting and investigating criminal violations of the Internal Revenue Code and financially related crimes.

The Electronic Fraud Detection System (EFDS), an automated compliance system, is the primary information system used to support the CI function's Questionable Refund Program.[1] The EFDS was designed to maximize fraud detection at the time that tax returns are filed to prevent the issuance of questionable refunds. It is generally harder and more costly to recover fraudulent refunds once they have been issued.

The EFDS is used to maximize fraud detection at the time that tax returns are filed to prevent the issuance of questionable refunds.

Since its initial development in 1995, the EFDS has gone through significant changes. In June 2001, the IRS approved the conversion of the existing client server application[2] to a web-based application.[3] From Processing Years (PY)[4] 2001 through 2005, the client server application continued to operate as the web-based application was under development. The new application was initially expected to be available for PY 2005, but was subsequently delayed until PY 2006 due to system development problems. In December 2005, the client server application was shut down because of the impending release of the web-based application. However, the web-based application never became operational. In April 2006, the IRS decided to restore the client server application for PY 2007.

Because the EFDS contains and processes highly sensitive taxpayer information, the security over the system is paramount to ensure all data are protected from unauthorized access and misuse. Federal Government Security Standards issued by the Office of Management and Budget[5] require that all systems and applications must be certified and accredited every 3 years

[1] A nationwide program established to detect and stop fraudulent claims for refunds on income tax returns.
[2] The client server application allows users to access the EFDS system internally on the IRS network.
[3] A system development effort that would allow users to access the EFDS via the IRS Intranet.
[4] A PY is the year in which tax returns and other tax data are processed by the IRS.
[5] Appendix III to Office of Management and Budget Circular A-130, *Security of Federal Automated Information Resources.*

or when major changes to systems occur. Guidelines issued by the National Institute for Standards and Technology (NIST)[6] further describe this certification and accreditation (C&A) process, which includes the following three phases:

- Initiation: A categorization of the sensitivity of the system as high, moderate, or low risk. During this phase, the system security plan should be updated. The system security plan provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements.
- Certification: A comprehensive assessment of the management, operational, and technical security controls in a system. Security controls testing of a system is performed to support the assessment, which is documented in a security assessment report. Any weaknesses identified during the testing are listed in a plan of actions and milestones (POA&M), which is monitored and updated until the weaknesses are corrected.
- Accreditation: An official management decision made by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

The Mission Assurance and Security Services (MA&SS) organization has responsibility to certify IRS systems. Part of that role is to ensure security controls are adequately tested. The system owner uses the results of those tests to authorize the system's operation and, by doing so, accepts the risks associated with that system.

The IRS has a long-standing computer security material weakness,[7] which includes the C&A process. We have issued several reports critical of the IRS C&A process, with the most recent issued in August 2004.[8] We also commented in our Fiscal Year (FY) 2005 report for the Federal Information Security Management Act of 2002[9] on the IRS' improvements and continuing struggles with its C&A process.

We initiated this audit to review the EFDS security controls. Two other audits were initiated to answer questions raised by the House Ways and Means Subcommittee on Oversight regarding the EFDS. One audit was performed to determine whether the IRS effectively managed annual programming changes and requested modifications to the EFDS prior to

[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] The Department of the Treasury defines 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."
[8] *The Certification and Accreditation of Computer Systems Should Remain in the Computer Security Material Weakness* (Reference Number 2004-20-129, dated August 2004).
[9] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

PY 2006.[10] Another audit (Audit Number 200610003) is being performed to determine the effectiveness of the IRS' procedures for detecting fraudulent and potentially fraudulent refund returns (including inventory controls) and the timely and proper hold and release of refunds.

In addition, in June 1999 we reported[11] that the EFDS had numerous security weaknesses, including inadequate audit trails[12] and contingency plans. Our review of the IRS' corrective actions to recommendations in this report determined the weaknesses identified in the report have been adequately addressed.

Our review was performed at the MA&SS organization in New Carrollton, Maryland, during the period March through June 2006. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[10] *The Electronic Fraud Detection System Redesign Failure Resulted in Fraudulent Returns and Refunds Not Being Identified* (Reference Number 2006-20-108, dated August 2006).
[11] *Review of the Electronic Fraud Detection System* (Reference Number 093009, dated June 1999).
[12] A chronological record of system activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.

Results of Review

Security Controls for the Electronic Fraud Detection System Client Server Application Have Not Been Adequately Tested Since 2001

IRS policies and Federal Government Security Standards require security controls for all major applications[13] be independently assessed, certified, and accredited at least every 3 years. Regular testing of security controls is necessary to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements for the system. Failure to regularly test security controls can result in undetected security weaknesses that place taxpayer information at risk of unauthorized disclosure, potentially resulting in identity theft or other privacy violations. For the EFDS, insufficient security controls could place millions of taxpayer records at risk for unauthorized access or modification, as the EFDS is the IRS' second largest repository of taxpayer information.

Insufficient security controls for the EFDS, the IRS' second largest repository of taxpayer information, could place millions of taxpayer records at risk of unauthorized access or modification.

Security controls for applications are generally provided through the operating system (e.g., Windows) on which they reside and by the application itself. To reduce the resources required for certification, operating system controls do not have to be retested for each application. However, the application's security controls must be tested. These controls are often the last line of defense for protecting the confidentiality, integrity, and availability of sensitive information.

Application security controls for the EFDS client server application were last tested in October 2001 as part of the certification that was signed in April 2002. The October 2001 testing identified 10 high-risk weaknesses that have since been addressed.

In August 2004, the EFDS was again certified and accredited. However, this C&A relied on certification of the Windows-based computers supporting the system and did not include testing of the client server application security controls. The application controls are critical for ensuring the confidentiality, integrity, and availability of taxpayer information in the EFDS. As

[13] Major applications are a category of applications used by the IRS that require special attention to security because of the severe adverse effect that compromise of those applications would have on the IRS mission, tax administration functions, and/or employee welfare.

such, this August 2004 EFDS client server application C&A provided only limited assurance that the EFDS security controls were adequate.[14]

Application security controls were not tested because the MA&SS organization omitted steps in the certification process in order to meet its goal of certifying and accrediting 100 percent of IRS systems by the end of FY 2004. Specifically, instead of performing a full certification on each system, the MA&SS organization focused on obtaining signed accreditation memoranda from system owners. As a result, many systems were accredited without adequate documentation and security testing. In the fourth quarter of FY 2004, the IRS certified and accredited 30 major applications, including the EFDS, representing 57 percent of the IRS' inventory of major applications at the time.

The Chief, MA&SS, provided us with his perspective on the FY 2004 C&A activities. The Chief informed us that, upon assuming his new position in FY 2004, he quickly discovered the IRS processes for C&A were incomplete and not in accordance with Office of Management and Budget Circular A-130 guidance. Of greatest concern was the fact that very few applications or systems had been accredited by the system owners or the Chief Information Officer. Because the systems were already in operation, the Chief, MA&SS, indicated his intent was to have system owners sign accreditation memoranda for all major systems so they would recognize their responsibilities for accepting the risks associated with their systems.

At the end of FY 2004, the IRS initiated a major effort to at least get a signed accreditation memorandum in place for every major application and general support system. The MA&SS organization's review of the security documentation of many systems at that time, including the EFDS, revealed that Security Plans and other security documentation were incomplete and did not contain the level of detail necessary to accurately capture all security considerations.

While accreditation is an important and a required step in the C&A process, NIST guidelines[15] state, "it is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems." Because the EFDS client server application was tested inadequately, we believe the system owner signed the accreditation without a full understanding of the status of EFDS security controls.

[14] During Fiscal Year 2004, the IRS decided to recategorize its C&A approach to include general support systems, major applications, and other applications. The IRS assigned all of its other applications to a general support system with the assumption that the general support systems provide the majority of the security controls for the other applications.

[15] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

Recommendation

Recommendation 1: The Chief, MA&SS, should coordinate with the Chief, CI, to complete a full security C&A package for the EFDS client server application and supporting computers before the system is permitted to operate.

> ***Management's Response:*** The Chief, MA&SS, has already begun coordination with the Chief, CI, to complete a full security C&A of the EFDS which will be conducted prior to the EFDS being placed into operation for the next tax filing season. This C&A will be based on currently available draft and final versions of Federal Government security process guidance. The EFDS application security controls will be tested based on NIST guidance as well as any other available security controls testing process guidance from other Government organizations and industry best practices.

If the Web-Based Electronic Fraud Detection System Had Become Operational, It May Have Allowed Unauthorized Access to Taxpayer Information

Prior to the IRS decision in April 2006 to stop all system development activities for the EFDS web-based application, we evaluated the effectiveness of its January 2006 C&A to determine whether it would have met IRS security standards. Our review identified problems with the completeness of security controls testing and the IRS process for reporting omitted security control tests. Specifically, key security controls in the following areas were not tested as part of the C&A process:

Required security controls for the EFDS web-based application were not tested as part of its C&A.

- Data integrity, which ensures data processed by the system are accurate, complete, valid, and protected.
- Transmission confidentiality, which ensures communications through the EFDS web-based application are encrypted to protect information, such as user passwords and taxpayer information, during transmission between the EFDS application and a user's computer.
- User authorizations, which ensure users are authorized to access the system.

Controls in these areas are required by IRS policies and the EFDS security plan. In addition, they are included in the required set of controls for high-risk Federal Government systems specified by the NIST. This is not the first time IRS management has omitted tests in C&A packages for the EFDS. Our review of the 2002 C&A for the client server application also identified omitted security tests. Specifically, two configuration management tests were omitted

because the tools needed to execute the tests were not available. No alternative tests were performed to ensure the controls were adequate.

By not testing these controls, the IRS had limited assurance that sensitive taxpayer information stored, processed, and transmitted by the EFDS web-based application would have been accurate and reliable. In addition, there are limited assurances this sensitive information would have been protected from unauthorized access, modification, or deletion.

The MA&SS organization did not adequately follow the certification process in testing the EFDS due to the imminent implementation date of the System. Testing was conducted in 1 day only a few weeks prior to implementation. In addition, testing was performed on the EFDS training system and not the actual EFDS production system. IRS management informed us that the 2005 version of the System was unusable for testing since it was undergoing significant changes and the EFDS training system was the best system available to use at that time. However, they also informed us that, due to the volume of changes being made to the production web-based application, they were unable to mirror those changes on the training system. Because the training system did not have actual EFDS data or follow IRS user authorization processes, tests for data integrity, user authorization, and transmission confidentiality controls were not performed.

In addition, the MA&SS organization did not prominently disclose the omitted tests in the C&A report. While the omitted tests were identified in the report appendices, they were not discussed in the body of the security test report or the security assessment report. Consequently, the system owners may not have seen all of the necessary information on the status of security controls to make an appropriate decision on whether to accredit the system.

We recognize the IRS has ceased development of the web-based application. As such, the recommendation for this finding pertains to any future C&A work on the EFDS application.

Recommendation

Recommendation 2: If the EFDS web-based application is redeployed, the Chief, MA&SS, should ensure the certification process fully discloses and explains any omitted tests for security controls and the associated risks in the body of the security testing report and the security assessment report. In addition, criteria should be included for identifying compensating tests and establishing plans for follow-up testing for control tests omitted during the certification.

> ***Management's Response:*** Although the EFDS web-based application is not being redeployed in 2007, the Chief, MA&SS, will update its processes to ensure that all security testing reports and security assessment reports for EFDS and all other IRS systems explain any omitted tests and the associated risks. The process will ensure criteria will be included for identifying compensating tests and establishing plans for follow-up testing for omitted control tests.

Unresolved Weaknesses at the Enterprise Computing Center-Memphis May Affect the Security and Recovery of the Electronic Fraud Detection System Client Server Application

The computers supporting the EFDS client server applications reside primarily at the Enterprise Computing Center in Memphis, Tennessee (ECC-MEM). Several unresolved weaknesses at the ECC-MEM relate to the security of the EFDS client server application as well as the recovery of the application in the event of an emergency. The ECC-MEM computer environment was certified in November 2004 and accredited in August 2005. Our review of the C&A documentation identified three weaknesses affecting the EFDS client server application.

2(d),2(e)

The third weakness is the lack of a complete Business Impact Analysis (BIA) for the ECC-MEM, which would identify the processing priorities in which applications are restored in the event of an emergency or significant service disruption. The BIA included in the ECC-MEM's October 2004 contingency plan does not meet all of the requirements of IRS policies and NIST standards. Specifically:

- Recovery priorities: No processing or recovery priorities are specifically assigned for the list of systems. While a critical rating is listed, there is no explanation for this measure.
- Allowable outage time: Fifty-five percent of the systems listed do not have a maximum allowable outage time assigned, which is the maximum allowable time a system may be unavailable before it prevents or inhibits the performance of an essential business process. Also, the allowable outage time appears to be linked to the critical rating and not based on analysis of each system.
- Outage impact: Forty percent of the systems listed do not contain a description of the business areas impacted by service disruptions.

2(d),2(e)

Although the contingency plan does contain a partial BIA, we identified additional information indicating this BIA may not be valid. Most notably is a notation in an appendix to the contingency plan that a BIA is a planned activity for the ECC-MEM. In addition, the IRS 2005 security self-assessment for the ECC-MEM identified the need to establish processing priorities, which is included in the ECC-MEM's October 2004 POA&M along with the need for a BIA. We also discussed this issue with IRS personnel, who informed us there is no BIA for the ECC-MEM.

These processing priorities are needed to minimize the impact to the IRS mission as systems are restored. IRS policies require that each IRS facility must establish processing priorities of critical business processes in a BIA. Since there is no valid BIA, the priority the EFDS application would be given after an emergency is uncertain, possibly affecting the CI function's ability to identify fraudulent returns. As of July 2006, there were 2(d),2(e) applications hosted at the ECC-MEM.

IRS policies specify that the system owner should complete the BIA. For the ECC-MEM, the Enterprise Operations Division within the Modernization and Information Technology Services organization is the designated system owner. The mission of the Enterprise Operations Division is to provide efficient, cost effective, secure, and highly reliable computing (server and mainframe) services for all IRS business entities and taxpayers.

The BIA has not been completed because the weakness is not listed on the current POA&M for the ECC-MEM. Although the weakness is included in the ECC-MEM's October 2004 POA&M, the dates established for corrective actions have passed and no new dates were established. The IRS does not consider this to be a high-risk issue and consequently is not monitoring the weakness on the current POA&M for the ECC-MEM.

Recommendation

Recommendation 3: The Chief Information Officer should develop a BIA for the ECC-MEM that places the EFDS at an appropriate priority among the other major applications residing at the ECC-MEM.

> ***Management's Response:*** A BIA will be developed and administered to enable the ECC-MEM and its stakeholders to determine the restoration priority of major applications. In addition, IRS Business Operating Divisions will be consulted about the recovery prioritization of critical business processes.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of security controls over the EFDS by evaluating its C&A packages. To accomplish this objective, we:

I. Determined whether the C&A packages for the EFDS client server and web-based applications and the infrastructure at the ECC-MEM effectively identified and addressed security control weaknesses.

   A. Determined whether the IRS developed an adequate security plan.

   B. Determined whether the IRS identified and tested the significant security controls for the system and adequately addressed identified security weaknesses.

   C. Assessed whether the C&A decisions were justified.

   D. Assessed the adequacy of the contingency planning documents.

II. Determined whether security weaknesses identified in our report entitled *Review of the Electronic Fraud Detection System* (Reference Number 093009, dated June 1999) were adequately addressed in the C&A process.

   A. Identified the status of IRS corrective actions to the report recommendations.

   B. Determined whether C&A testing adequately addressed the security weaknesses identified in the report.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Kent Sagara, Acting Director
Marybeth Schumann, Audit Manager
Michael Howard, Lead Auditor
Richard Borst, Senior Auditor
Jody Kitazono, Senior Auditor
Thomas Nacinovich, Senior Auditor
Stasha Smith, Senior Auditor

Appendix III

Report Distribution List

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

Appendix IV

Management's Response to the Draft Report

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

RECEIVED
SEP 25 2006

CHIEF
MISSION ASSURANCE AND SECURITY SERVICES

SEP 25 2006

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Response to Draft Audit Report – A Complete Certification and Accreditation is Needed to Ensure the Electronic Fraud Detection System Meets Federal Government Security Standards (Audit #200620040)

Thank you for the opportunity to review the subject draft audit report, dated August 28, 2006. We agree that a complete certification and accreditation is needed to ensure the Electronic Fraud Detection System (EFDS) meets Federal Government security standards. The IRS initiated major revisions to its certification and accreditation processes in 2004, immediately after the National Institute for Standards and Technology (NIST) issued new process guidance in May 2004. Since 2004, the IRS has continued to make steady progress in bringing IRS systems into compliance with evolving Federal Government security standards and process guidance. Federal Government security standards and process guidance have undergone several significant changes and updates over the past 3 years as NIST has issued several draft and final versions of new security standards and process guidance publications. The Federal Information Security Management Act (FISMA) has focused priority on making cost effective risk-based decisions in providing adequate security for Federal information systems. The IRS has implemented processes to ensure that all of the appropriate senior officials are engaged in making these important risk-based decisions, which has been very challenging during a period when the Federal Government security standards and process guidance continue to undergo significant changes and updates.

After NIST issued its new process guidance for security certification and accreditation in May 2004, the IRS reviewed the security certification and accreditation status of all of its major systems (including EFDS) during the third and fourth quarters of Fiscal Year 2004. The Mission Assurance and Security Services (MA&SS) organization issued a Security Assessment Report (SAR) in August 2004 for EFDS and for all other major systems, for the purposes of providing an updated overall security status report for each major system. EFDS and most other IRS major systems at that time had completed security certification within the 3 previous years, but had not completed the final important step of security accreditation. The MA&SS organization focused priority on a

goal of incorporating the security accreditation step into IRS security certification and accreditation processes, in order to continue the updates that would be necessary to ultimately bring IRS security certification and accreditation processes into compliance with the new NIST guidance that had just been issued. The IRS had completed supporting infrastructure security controls testing on EFDS and all other IRS major systems during certification efforts completed over the previous 3 years, recognizing that limited Federal Security process guidance existed for application level security controls testing in 2004.

In February 2005, NIST issued Special Publication 800-53, "Recommended Security Controls for Federal Information Systems." In April 2006, NIST issued a draft version of Special Publication 800- 53A, "Guide for Assessing the Security Controls in Federal Information Systems" which includes procedures for evaluating application level security controls. The IRS initiated another major initiative in Fiscal Year 2006 to incorporate the new NIST guidance into its security certification and accreditation processes. We are pleased that the recent TIGTA draft report distributed in September 2006 entitled, "Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2006," contained several favorable comments indicating that the IRS made significant improvements in its security certification and accreditation process in 2006. Unfortunately, the EFDS system was too far along in its development in early Fiscal Year 2006, and there was not enough time to apply the new comprehensive FISMA/NIST compliant IRS certification and accreditation process to EFDS in December of 2005 and January of 2006. The IRS intends to conduct a full security certification and accreditation of the EFDS system, based on the currently available draft and final versions of Federal Government security process guidance, prior to EFDS being placed into operation for the next tax filing season. The application level security controls for EFDS will be tested based on the new draft NIST guidance, and will also make use of any other available security controls testing process guidance that may be available from other Government organizations and from industry best practices.

We concur with all three report recommendations, and have already applied the new comprehensive IRS security certification and accreditation process to the EFDS version that is being prepared for the next tax filing season. We are working in conjunction with the Chief, Criminal Investigation, and the Chief Information Officer, to implement corrective actions. Attached is a detailed response outlining the corrective action plans for each of the report recommendations. We appreciate your continued support and valuable oversight assistance. If you have any questions, please contact me at (202) 622-8910, or Devon Bryan, Director, Information Technology Security, at (202) 283-7271.

Attachment

Management response to Draft Audit Report – A Complete Certification and Accreditation Is Needed to Ensure the Electronic Fraud Detection System Meets Federal Government Security Standards (Audit # 200620040)

RECOMMENDATION #1:

The Chief, Mission Assurance and Security Services, should coordinate with the Chief, Criminal Investigation, to complete a full security Certification and Accreditation package for the Electronic Fraud Detection System (EFDS) client server application and supporting computers before the system is permitted to operate.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The Chief, Mission Assurance and Security Services has already begun coordination with the Chief, Criminal Investigation, in order to complete a full security certification and accreditation (C&A) of the EFDS system. Based on the currently available draft and final versions of Federal Government security process guidance, and prior to EFDS being placed into operation for the next tax filing season, the full security C&A will be conducted. The application level security controls for EFDS will be tested based on the new draft National Institute of Standards and Technology (NIST) guidance. We will also make use of any other available security controls testing process guidance that may be available from other Government organizations and from industry best practices.

IMPLEMENTATION DATE:

February 15, 2007

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance and Security Services, OS:MA

CORRECTIVE ACTION MONITORING PLAN:

EFDS certification and accreditation process steps will be monitored on a monthly basis by the existing governance committees that exist for EFDS.

1

Management response to Draft Audit Report – A Complete Certification and Accreditation Is Needed to Ensure the Electronic Fraud Detection System Meets Federal Government Security Standards (Audit # 200620040)

RECOMMENDATION #2:

If the Electronic Fraud Detection System (EFDS) web-based application is redeployed, the Chief, Mission Assurance and Security Services, should ensure the certification process fully discloses and explains any omitted tests for security controls and the associated risks in the body of the security testing report and the security assessment report. In addition, criteria should be included for identifying compensating tests and establishing plans for follow-up testing for control tests omitted during the certification.

CORRECTIVE ACTION TO RECOMMENDATION #2:

The EFDS web-based application is not being redeployed in 2007. However, the Chief, Mission Assurance and Security Services organization, will update its processes to ensure that all security testing reports and security assessment reports for EFDS and all other IRS systems explain any omitted tests and the associated risks. The process will ensure criteria will be included for identifying compensating tests and establishing plans for follow-up testing for omitted control tests.

IMPLEMENTATION DATE:

January 15, 2007

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance and Security Services, OS:MA

CORRECTIVE ACTION MONITORING PLAN:

Implementation of this process will be monitored by the established IRS Federal Information Security Management Act Certification and Accreditation Working Group, and the Security Services and Privacy Executive Steering Committee.

2

Management response to Draft Audit Report – A Complete Certification and Accreditation Is Needed to Ensure the Electronic Fraud Detection System Meets Federal Government Security Standards (Audit # 200620040)

RECOMMENDATION #3:

The Acting Chief Information Officer should develop a Business Impact Analysis for the Enterprise Computer Center in Memphis, Tennessee (ECC-MEM) that places the Electronic Fraud Detection System (EFDS) at an appropriate priority among the other major applications residing at the ECC-MEM.

CORRECTIVE ACTION TO RECOMMENDATION #3:

A Business Impact Assessment will be developed and administered to enable ECC-MEM and its stakeholders to determine the restoration priority of major applications. In addition, we will consult with the Business Operating Divisions about the recovery prioritization of critical business processes.

IMPLEMENTATION DATE:

January 15, 2008

RESPONSIBLE OFFICIAL:

Director, Associate Chief Information Officer, Enterprise Operations, OS:CIO:EO

RESPONSIBLE STAKEHOLDER:

Director, CSIRC and IT Disaster Recovery, OS:MA:IT:C

CORRECTIVE ACTION MONITORING PLAN:

The Computer Security Incident Response Center and IT Disaster Recovery organization will maintain a comprehensive Business Impact Assessment plan that is reviewed quarterly to monitor recommendation implementation.

3