



*Sufficient Emphasis Was Not
Placed on Resolving Security Vulnerabilities
When Restoring the Electronic Fraud
Detection System*

June 14, 2007

Reference Number: 2007-20-108

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

Phone Number | 202-927-7037

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

June 14, 2007

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

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Sufficient Emphasis Was Not Placed on
Resolving Security Vulnerabilities When Restoring the Electronic
Fraud Detection System (Audit # 200720028)

This report presents the results of our review to assess the effectiveness of the security controls testing conducted as part of the certification and accreditation of the Electronic Fraud Detection System (hereafter referred to as the EFDS or System). We conducted this review to follow up on our Fiscal Year 2006 audit report,¹ which stated the security of the System had not been properly assessed since 2001.

Impact on the Taxpayer

The EFDS is used by the Internal Revenue Service (IRS) Criminal Investigation Division to detect fraudulent returns and is the IRS' second largest repository of taxpayer data. Security over the System is vital to ensure it is available to prevent fraud and to protect the privacy of taxpayers' personal information. Because the focus was to restore the System for the start of the 2007 Filing Season,² insufficient emphasis was placed on the System's security controls. Until security control weaknesses are corrected, the Criminal Investigation Division is jeopardizing the confidentiality, integrity, and availability of the System and the taxpayer data residing on it.

¹ *A Complete Certification and Accreditation Is Needed to Ensure the Electronic Fraud Detection System Meets Federal Government Security Standards* (Reference Number 2006-20-178, dated September 29, 2006).

² The period from January through mid-April when most individual income tax returns are filed.



Sufficient Emphasis Was Not Placed on Resolving Security Vulnerabilities When Restoring the Electronic Fraud Detection System

Synopsis

On January 16, 2007, the IRS launched a restored EFDS. Prior to the System's restoration, the Mission Assurance and Security Services organization conducted a certification of the System that included a thorough testing of the security controls in the application, database, and supporting computers. The Criminal Investigation Division (the System owner) received these test results prior to the System restoration in January 2007. The Mission Assurance and Security Services organization followed National Institute of Standards and Technology³ guidance in selecting the controls to be tested and in applying the appropriate test procedures to protect and evaluate the confidentiality, integrity, and availability of the System and the taxpayer data residing on it.

The EFDS security testing was conducted in two phases: one in September 2006 and one in January 2007. The January 2007 test results identified 34 security vulnerabilities that were also identified in the September 2006 test results. The vulnerabilities occurred in configuration management, user identification, system and communications protection, and detection controls. We believe the Criminal Investigation Division and the EFDS Project Office missed an opportunity during the time between the two tests to correct some of the significant security vulnerabilities prior to restoring the System.

Because the EFDS Project Office was primarily focused on implementing the restored System for the start of the 2007 Filing Season, insufficient emphasis was placed on the System's security controls. In addition, the Criminal Investigation Division did not coordinate with nor pursue a commitment from the EFDS Project Office to correct security vulnerabilities or plan corrective actions for those vulnerabilities. As a result, the restored System continues to operate with significant security vulnerabilities. Until corrective actions are taken, the Criminal Investigation Division and the EFDS Project Office are jeopardizing the confidentiality, integrity, and availability of the System and the taxpayer data residing on it.

We also noted the EFDS security certification memorandum contained a recommendation that the Chief, Criminal Investigation, grant a "restricted authorization to operate" for a period of no more than 1 year. A "restricted authorization to operate" is not a valid accreditation decision. Based on National Institute of Standards and Technology guidance, an Interim Authorization to Operate should be issued when significant vulnerabilities have been identified that can be corrected timely. Considering the nature of the weaknesses identified for the EFDS, an Interim Authorization to Operate would have been more appropriate and would have resulted in more emphasis by IRS management to ensure the vulnerabilities were corrected.

³ The National Institute of Standards and Technology, 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.



Sufficient Emphasis Was Not Placed on Resolving Security Vulnerabilities When Restoring the Electronic Fraud Detection System

Recommendation

The Chief, Criminal Investigation, should issue an Interim Authorization to Operate for the EFDS and require specific terms and conditions be met before an Authorization to Operate is granted. The expiration date should be based on corrective action milestone dates for the security vulnerabilities identified.

Response

IRS management disagreed with our recommendation, and the Chief, Criminal Investigation, has granted the EFDS an Authorization to Operate. The Chief, Criminal Investigation, the authorizing official who made the EFDS accreditation decision and to whom our recommendation was made, did not respond to the draft report. The response was provided by the Chief, Mission Assurance and Security Services, the certification agent who recommended the Chief, Criminal Investigation, grant an Authorization to Operate. In the response, the Chief, Mission Assurance and Security Services, stated that the decision of the Chief, Criminal Investigation, to issue an Authorization to Operate is fully supported because (1) no "high" security risks were identified for the EFDS and (2) an updated Plan of Action and Milestones is in place and being maintained to address issues identified during the certification that have not yet been resolved. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment

We disagree with IRS management's response to our recommendation. The weaknesses identified during security testing increase the risk that unauthorized accesses to the EFDS could be made without detection. We consider these weaknesses to be significant, thereby warranting issuance of an Interim Authorization to Operate. We recognize the accreditation decision is subjective; however, we believe an Interim Authorization to Operate is the more prudent accreditation decision for the EFDS because it will bring increased attention to resolving the significant security weaknesses of this important system.

While we consider our disagreement to be significant, we are not elevating it to the Department of the Treasury Assistant Secretary for Management and the Chief Financial Officer. Our review was limited to one system and consequently we have not identified a trend warranting their involvement. Instead, we will be providing an informational copy of this report to the Department of the Treasury Chief Information Officer under separate cover. Copies of this report are also being sent to the IRS managers affected by the report recommendation. 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.



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Table of Contents

BackgroundPage 1

Results of ReviewPage 3

 The Security of the Electronic Fraud Detection System Was
 Adequately TestedPage 3

 Security Vulnerabilities Identified During Testing Were Not
 Addressed Prior to Restoring the Electronic Fraud Detection SystemPage 3

 The Electronic Fraud Detection System Accreditation Decision
 Does Not Comply With Federal Government Security StandardsPage 4

Recommendation 1:.....Page 5

Appendices

 Appendix I – Detailed Objective, Scope, and MethodologyPage 7

 Appendix II – Major Contributors to This ReportPage 8

 Appendix III – Report Distribution ListPage 9

 Appendix IV – Management’s Response to the Draft ReportPage 10



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Abbreviations

EFDS; System	Electronic Fraud Detection System
IRS	Internal Revenue Service
MA&SS	Mission Assurance and Security Services
NIST	National Institute of Standards and Technology



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Background

The Internal Revenue Service (IRS) Criminal Investigation Division is responsible for detecting and investigating criminal violations of the Internal Revenue Code and financially related crimes. The Electronic Fraud Detection System (hereafter referred to as the EFDS or System), an automated compliance system, was designed to maximize fraud detection at the time tax returns are filed, to prevent the issuance of questionable refunds. The System is the primary information system used to support the Criminal Investigation Division Questionable Refund Program and is the IRS' second largest repository of taxpayer data. Because it contains and processes highly sensitive taxpayer information, security over the System is vital to ensure both the System and the data residing on it are protected from unauthorized access and misuse.

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 System 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, and the client-server application could not be restored in time for use during the 2006 Filing Season.¹ As a result, in a previous audit report,² we estimated \$318.3 million in fraudulent refunds may have been issued as of May 19, 2006.

In April 2006, the IRS stopped all development activities for the web-based application and focused all efforts on restoring the client-server application for use in January 2007 for the 2007 Filing Season. The EFDS Project Office, located in the Modernization and Information Technology Services organization, was responsible for restoring the application. On January 16, 2007, the IRS launched the restored EFDS client-server application.

This review was a follow-up to a prior Treasury Inspector General for Tax Administration audit.³ In September 2006, we reported that the security of the System had not been properly assessed since 2001. We recommended the Chief, Mission Assurance and Security Services (MA&SS), coordinate with the Chief, Criminal Investigation, to complete a full security certification and accreditation for the EFDS client-server application and supporting computers before the restored System was permitted to operate. The Chief, MA&SS, agreed with our

¹ The period from January through mid-April when most individual income tax returns are filed.

² *The Electronic Fraud Detection System Redesign Failure Resulted in Fraudulent Returns and Refunds Not Being Identified* (Reference Number 2006-20-108, dated August 9, 2006).

³ *A Complete Certification and Accreditation Is Needed to Ensure the Electronic Fraud Detection System Meets Federal Government Security Standards* (Reference Number 2006-20-178, dated September 29, 2006).



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

recommendation and began coordination with the Chief, Criminal Investigation, to certify and accredit the restored System.

This review was performed at the MA&SS organization office in New Carrollton, Maryland, and the Enterprise Computing Center⁴ in Memphis, Tennessee, during the period November 2006 through February 2007. 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.

⁴ IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Results of Review

The Security of the Electronic Fraud Detection System Was Adequately Tested

National Institute of Standards and Technology (NIST) guidance⁵ describes certification as a comprehensive assessment of the security controls in a system. An accreditation is an official management decision to authorize the operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on implementation of an agreed-upon set of security controls. IRS policies and Federal Government security standards require that the security of all information systems be independently assessed, certified, and accredited at least every 3 years. Regular testing of security controls is necessary to determine the extent to which these controls are implemented correctly, operating as intended, and meeting the security requirements for the system.

In our September 2006 EFDS security audit report, we stated that key application security controls were not tested when the System was certified and accredited in 2004. Instead, testing was limited to the supporting Windows-based operating system. As a result, the IRS had limited assurance that the System security controls were effective in protecting taxpayer information from unauthorized disclosure.

The recently conducted certification of the System included a thorough testing of the security controls in the application, database, and supporting computers. The MA&SS organization conducted the tests and reported the results to the Criminal Investigation Division (the System owner) prior to the System's restoration on January 16, 2007. The MA&SS organization followed NIST guidance in selecting the controls to be tested and in applying the appropriate test procedures to protect and evaluate the confidentiality, integrity, and availability of the System and the taxpayer data residing on it.

Security Vulnerabilities Identified During Testing Were Not Addressed Prior to Restoring the Electronic Fraud Detection System

NIST guidance states that security vulnerabilities identified during certification testing should be listed in a Plan of Action and Milestones. This document describes the measures that have been

⁵ NIST *Guide for the Security Certification and Accreditation of Federal Information Systems* (Special Publication 800-37). 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.



Sufficient Emphasis Was Not Placed on Resolving Security Vulnerabilities When Restoring the Electronic Fraud Detection System

implemented or planned to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system. For the EFDS, the Criminal Investigation Division is responsible for preparing, monitoring, and updating the Plan of Action and Milestones until the security vulnerabilities are corrected.

The System security testing was conducted in two phases. The first phase, conducted in September 2006, was based on the configuration of the System at that time. The second phase was conducted in January 2007 after upgrades had been made to the database and operating system. In the System security test plan, the MA&SS organization stated the decision to conduct testing in two phases presented an opportunity to resolve any major vulnerabilities discovered during the first testing phase.

The Criminal Investigation Division and the EFDS Project Office did not take advantage of this opportunity and, therefore, security vulnerabilities still have not been corrected. The test results in January 2007 identified 34 security vulnerabilities that had been initially identified in the September 2006 tests. These security vulnerabilities occurred in configuration management, user identification, system and communications protection, and detection controls. The MA&SS organization characterized the combination of user identification and detection controls as high-priority security vulnerabilities because an attacker could easily subvert an account with a weak password with little chance of detection. Actions and milestones to correct these vulnerabilities were not documented in a Plan of Action and Milestones until after the System was restored and operating.

The EFDS Project Office was primarily focused on restoring the System for the start of the 2007 Filing Season and provided insufficient emphasis to correcting the System's security vulnerabilities. In addition, the Criminal Investigation Division did not coordinate with nor pursue a commitment from the EFDS Project Office to correct security vulnerabilities or plan corrective actions for those security vulnerabilities when they were identified in September 2006. As a result, the restored System was implemented and continues to operate with significant security vulnerabilities that jeopardize the confidentiality, integrity, and availability of both the System and the data residing on it.

The Electronic Fraud Detection System Accreditation Decision Does Not Comply With Federal Government Security Standards

Based on NIST guidance, the authorizing official must decide whether a system should be allowed to operate. The authorizing official has three options: (1) authorize the system to operate; (2) authorize the system to operate on an interim basis under strict terms and conditions, known as an Interim Authorization to Operate; or (3) deny authorization to operate the system. By approving operation of the system, the authorizing official assumes responsibility for the system and becomes accountable for the risks associated with operating the system.



Sufficient Emphasis Was Not Placed on Resolving Security Vulnerabilities When Restoring the Electronic Fraud Detection System

The EFDS security certification memorandum contained a recommendation that the Chief, Criminal Investigation, as the authorizing official for the System, grant a “restricted authorization to operate” for a period of no more than 1 year. A “restricted authorization to operate” is not a valid accreditation decision based on NIST guidance. We were advised that the decision to grant the authorization to operate was made because the certifying agent and authorizing official believed the vulnerabilities identified were not significant enough to warrant issuance of an Interim Authorization to Operate. The term “restricted” was added to emphasize to the authorizing official that the System would need to be recertified within 1 year due to the importance of the System for identifying fraud each filing season.

NIST guidance states that an Interim Authorization to Operate is rendered when identified vulnerabilities are significant but can be addressed timely. Considering the nature of the weaknesses identified for the EFDS, an Interim Authorization to Operate should have been issued.

We understand the Chief, MA&SS, as the certifying agent, intended to notify the authorizing official that the System needed to be recertified within 1 year. However, because agencies are measured on the percentage of systems that have full authorizations to operate,⁶ an Interim Authorization to Operate is likely to bring more emphasis by IRS management to resolve a system’s vulnerabilities, so it can receive a full Authorization to Operate. The Interim Authorization to Operate should not be rescinded until the risks to the agency have been decreased to an acceptable level.

Without additional emphasis by the IRS, we are concerned the significant vulnerabilities identified for the EFDS will not be corrected in time for the next filing season. In addition, the true status of security controls for the System is not being accurately reported.

Recommendation

Recommendation 1: The Chief, Criminal Investigation, should issue an Interim Authorization to Operate for the EFDS and require that specific terms and conditions be met before an Authorization to Operate is granted. The expiration date should be based on corrective action milestone dates in the EFDS Plan of Action and Milestones.

Management’s Response: IRS management disagreed with our recommendation, and the Chief, Criminal Investigation, has granted the EFDS an Authorization to Operate. The Chief, Criminal Investigation, the authorizing official who made the EFDS accreditation decision and to whom our recommendation was made, did not respond to the draft report. The response was provided by the Chief, MA&SS, the certification

⁶ Federal Information Security Management Act, Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002). This law requires agencies to report annually on the status of key security measurements, including the percentage of systems certified and accredited.



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

agent who recommended the Chief, Criminal Investigation, grant an Authorization to Operate. In the response, the Chief, MA&SS, stated that the decision of the Chief, Criminal Investigation, to issue an Authorization to Operate is fully supported because (1) no “high” security risks were identified for the EFDS and (2) an updated Plan of Action and Milestones is in place and being maintained to address issues identified during the certification that have not yet been resolved.

Office of Audit Comment: We disagree with IRS management’s response to our recommendation. The weaknesses identified during security testing increase the risk that unauthorized accesses to the EFDS could be made without detection. We consider these weaknesses to be significant, thereby warranting issuance of an Interim Authorization to Operate. We recognize the accreditation decision is subjective; however, we believe an Interim Authorization to Operate is the more prudent accreditation decision for the EFDS because it will bring increased attention to resolving the significant security weaknesses of this important system.



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of the security controls testing conducted as part of the certification and accreditation of the EFDS (the System). To accomplish this objective, we:

- I. Determined whether all applicable security controls were tested.
 - A. Identified the mandatory controls for a moderate impact system from the NIST *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53).¹
 - B. Compared the System controls tested during the security test and evaluation to the controls identified from Special Publication 800-53 for a moderate impact system and determined whether all recommended controls were tested.
- II. Determined whether all applicable controls were adequately tested to determine whether the controls were in place, operating as intended, and producing the desired results.
 - A. For each control tested, identified the applicable assessment procedures from the NIST *Guide for Assessing the Security Controls in Federal Information Systems* (Special Publication 800-53A).
 - B. Compared the test cases or assessment methods used to test the System controls with the recommended assessment procedures contained in Special Publication 800-53A to identify any gaps in the test cases.
- III. Determined whether the accreditation recommendation made by the MA&SS organization certification agent was supported by and consistent with the results of the security testing.
- IV. Determined whether all the System security vulnerabilities are being tracked for remediation.

¹ The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
Marybeth Schumann, Audit Manager
Joan Raniolo, Lead Auditor
Richard Borst, Senior Auditor
Michael Howard, Senior Auditor



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Appendix III

Report Distribution List

Acting 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 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:
 Chief, Criminal Investigation SE:CI
 Chief Information Officer OS:CIO
 Chief, Mission Assurance and Security Services OS:MA
 Director, Program Oversight Office OS:CIO:SM:PO



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Appendix IV

Management's Response to the Draft Report



CHIEF
MISSION ASSURANCE AND SECURITY SERVICES

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

RECEIVED

MAY - 3 2007

May 3, 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Response to Draft Audit Report – Sufficient Emphasis Was Not
Placed on Resolving Security Vulnerabilities When Restoring the
Electronic Fraud Detection System (Audit # 200720028, Itrak
#2007-22958)

Thank you for the opportunity to review and respond to the referenced draft audit report. The Electronic Fraud Detection System (EFDS) was put into production on January 16, 2007, without any major problems. The system was deployed subject to certification and accreditation processes that were in accordance with IRS policies and Federal Government security standards requiring that the security of all information systems be independently assessed, certified, and accredited at least every 3 years. The National Institute of Standards and Technology (NIST) guidance describes certification as a comprehensive assessment of the security controls in a system. An accreditation is an official management decision to authorize the 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 IRS has continued to make steady progress in bringing IRS systems into compliance with evolving Federal Government security standards and process guidance. We are pleased that your report acknowledges that the recently conducted certification of EFDS included a thorough testing of the security controls in the application, database, and supporting computers. You also reported that the Mission Assurance and Security Services organization followed NIST guidance in selecting the controls to be tested and in applying the appropriate test procedures to protect and evaluate the confidentiality, integrity, and availability of the system and the data residing on it.

Regarding the EFDS security certification, based on the certification information and my resulting recommendation as the IRS Security Certification Agent, the acting Chief Criminal Investigation (CI) signed a "restricted" Authorization to Operate (ATO) for EFDS. Specifically, the most important information from the EFDS security certification was that the EFDS Security Assessment Report (SAR), Version 1.1, January 1, 2007, stated that a total of seven risks were discovered on the application. Of the seven risks, three were deemed "Low" and four were deemed "Medium." None of the risks identified



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

2

in the EFDS security certification are deemed "High." In addition, the total number of risks showed an overall improvement in the enforcement of security controls when compared to the risks identified in the previous SAR developed in November 2006. As the Designated Accrediting Agent (DAA), the acting Chief, CI, reviewed the findings from the EFDS security certification and concurred with the Certification Agent recommendation, and issued the restricted ATO.

In subsequent discussions with the CI security team and TIGTA staff, I clarified that the term "restricted" was added in the Authority To Operate (ATO) accreditation recommendation for the specific purpose of ensuring that the length of the accreditation period be shortened to only 1 year, instead of the usual 3 years. This was done because I felt that security for this important program should be reviewed each year, based on issues with security processes in support of past EFDS upgrades, and recognizing that additional upgrades were being planned and considered for the future. Overall, the Certification Agent recommendation supports an ATO, with the understanding that a valid Plan of Action and Milestones (POA&Ms) is in place, and is being used to track the progress of the identified corrective actions to further mitigate the security risks to EFDS.

Your report contains a single recommendation, "The Chief, Criminal Investigation, should issue an Interim Authorization to Operate for the EFDS and require specific terms and conditions be met before an Authorization to Operate is granted. The expiration date should be based on corrective action milestone dates in the EFDS Plan of Action and Milestones." Considering the fact that a quality security certification was conducted and that there are no "High" security risks, we believe the basis was fully supportable for issuing an ATO. Since the term "restricted" is not recognized as a valid qualifier for an ATO, as reported by TIGTA, CI will consider EFDS as operating under a full ATO until significant changes to the system require a new security certification as detailed in NIST and IRS guidance. This decision was also based on the fact that an updated Plan of Action and Milestones (POA&M) for EFDS is in place, and is being maintained to address issues identified during certification that have not yet been resolved. CI is closely tracking the corrective actions and milestone dates. The Certification Agent will specifically review the security posture of EFDS in 1 year, and will issue a certification and accreditation update at that time, as required. This information is reemphasized in our attached detailed response.

If you have any questions, please contact me at (202) 622-8910, or Eileen Mayer, Chief, Criminal Investigation, at (202) 622-3200.

Attachment



*Sufficient Emphasis Was Not Placed on Resolving
Security Vulnerabilities When Restoring the
Electronic Fraud Detection System*

Attachment

Management Response to Draft Audit Report – Sufficient Emphasis Was Not Placed on Resolving Security Vulnerabilities When Restoring the Electronic Fraud Detection System (Audit # 200720028)

RECOMMENDATION #1:

The Chief, Criminal Investigation (CI), should issue an Interim Authorization to Operate for the EFDS and require specific terms and conditions be met before an Authorization to Operate is granted. The expiration date should be based on corrective action milestone dates in the EFDS Plan of Action and Milestones.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The IRS does not concur that the Chief, Criminal Investigation (CI) should issue an Interim Authorization to Operate for the Electronic Fraud Detection System (EFDS). Specifically, the Treasury Inspector General for Tax Administration's (TIGTA) audit report concluded that a quality security certification was completed on EFDS by the Mission Assurance and Security Services (MA&SS) organization. When conducting the certification, MA&SS followed applicable National Institute of Standards and Technology (NIST) guidance. The results of the certification effort indicated that there are no "High" risks. In addition, the Certification Agent assessed that the overall level of security risk to EFDS operations is acceptable, as long as the corrective actions to resolve the residual risks were closely tracked in a Plan of Action and Milestones (POA&M). The Certification Agent recommended that the term of the Authorization to Operate (ATO) be limited to 1 year, instead of the normal 3 years, in order to specifically ensure that the security posture be reviewed prior to each filing season. However, since the term "restricted" is not recognized as a valid qualifier for an ATO, as reported by TIGTA, CI will consider EFDS as operating under a full ATO until significant changes to the system require a new security certification as detailed in NIST and IRS guidance. The Certification Agent will also specifically review the security posture of EFDS in 1 year, and will issue a certification and accreditation update at that time, as required.

The POA&M for EFDS has been updated, and CI is closely tracking the corrective actions and milestone dates for EFDS issues identified during certification that have not yet been resolved. The information in the POA&M was reviewed and taken into consideration in making the Designated Accrediting Agent's risk acceptance decision to grant an ATO.

IMPLEMENTATION DATE:

Completed - 4/15/07

RESPONSIBLE OFFICIAL:

Director, Director, Technology Operations and Investigative Services, SE:CI:TOIS

CORRECTIVE ACTION MONITORING PLAN:

Not applicable