The Method of Tracking Corrective Actions for Known Security Weaknesses Has Not Been Adequately Developed

January 2005

Reference Number: 2005-20-027

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

January 12, 2005

MEMORANDUM FOR CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

FROM: *(for)* Gordon C. Milbourn III
Assistant Inspector General for Audit
(Small Business and Corporate Programs)

SUBJECT: Final Audit Report - The Method of Tracking Corrective Actions for Known Security Weaknesses Has Not Been Adequately Developed (Audit # 200420030)

This report presents the results of our review of the effectiveness of the Internal Revenue Service's (IRS) process for monitoring security weaknesses. The purpose of this review was to evaluate the Plans of Action and Milestones (POA&M) process employed by the IRS and determine whether the POA&M process satisfies the Office of Management and Budget (OMB) requirements and assists the agency in managing its risk and vulnerabilities.

OMB regulations state Information Technology (IT) security is one of several critical components agencies must meet to achieve a green or yellow status for the E-Government Scorecard. To achieve either status for the IT security component of the E-Government Scorecard, agencies must demonstrate consistent progress in reducing IT security weaknesses through their POA&Ms, and the Inspectors General must verify whether the process is effective.

In summary, the IRS has prepared POA&Ms to track both program-level and system-level weaknesses. However, the process it uses to identify weaknesses and report progress is flawed and ineffective. As a result, information provided to the Department of the Treasury and the OMB has been inaccurate and misleading.

The program-level POA&M identified the number of security reports issued by the Government Accountability Office and the Treasury Inspector General for Tax Administration, but it did not identify the specific weaknesses reported. As a result, the number of program-level weaknesses was significantly understated.

The system-level POA&Ms did not accurately and completely describe the security weaknesses and milestones, understated the number of weaknesses, and overstated

progress in addressing the weaknesses. The IRS prepared almost identical POA&Ms for each system, noting only broad control topics rather than specific weaknesses. Specific actions aimed at correcting the weaknesses were not detailed, and responsible individuals were not identified. Essentially, the POA&Ms were so vague they could not be used in managing and overseeing the security program.

For the most recent POA&M submission to the Department of the Treasury, dated September 2004, the IRS reported 319 system-level weaknesses for its 80 major systems. This number is understated because it represents only management control weaknesses such as lack of a certification and accreditation, security plan, or tested contingency plan. Generally, operational and technical control weaknesses were not reported.

Progress in addressing the weaknesses was overstated. The IRS assumed if a system had been certified and accredited, then nearly all weaknesses noted on the system's POA&M could be closed. This assumption is not valid since certified and accredited systems can still have security weaknesses. We know of no testing that was done to identify security weaknesses or to ensure weaknesses were corrected.

To ensure an effective system is in place to monitor security weaknesses, we recommended the Chief, Mission Assurance and Security Services (MA&SS), coordinate with the Chief Information Officer (CIO) and business unit owners to develop POA&Ms that specifically identify all known security weaknesses. The POA&Ms should contain details sufficient to allow oversight of the IRS security program. The Chief, MA&SS, should also accurately report the results of efforts to correct security weaknesses. Testing should be conducted to ensure the weaknesses have been corrected before the POA&Ms are closed.

Management's Response: The Chief, MA&SS, agreed with our recommendations and has initiated a number of corrective actions. The Chief, MA&SS, has established a Federal Information Security Management Act (FISMA)[1] working group of executives and senior staff from the business units and from the Modernization and Information Technology Services organization to develop and implement an approach to managing the POA&M process. In coordination with the CIO and business unit owners, the Chief, MA&SS, will develop a matrix to allow the reconciliation and validation of corrective actions through the testing process. 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.

[1] The FISMA is part of the E-Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.

Table of Contents

The Method of Tracking Corrective Actions for Known Security Weaknesses Has Not Been Adequately Developed

Background

The Office of Management and Budget (OMB) requires all Federal Government agencies to identify and track their progress in correcting computer security weaknesses. Specifically, the OMB requires each agency to develop Plans of Action and Milestones (POA&M) for identifying and managing weaknesses in its security programs and systems. Plans should be developed to correct the weaknesses, milestones should be provided for monitoring actions, and completion dates should be set.

Each quarter, the Internal Revenue Service (IRS) must submit its current list of security weaknesses to the Department of the Treasury to demonstrate whether it is effectively managing its security program. The Department of the Treasury then combines these results with those from the other bureaus and provides the results to the OMB.

The OMB directs Inspectors General (IG) to assess, using specific criteria,[1] whether the agencies have developed, implemented, and managed an agency-wide POA&M process. IGs are required to report to the OMB annually on whether agencies have an effective process for monitoring security weaknesses.

OMB regulations state Information Technology (IT) security is one of several critical components agencies must meet to achieve a green or yellow status for the E-Government Scorecard. To achieve either status for the IT security component of the E-Government Scorecard, agencies must demonstrate consistent progress in reducing IT security weaknesses through their POA&Ms.

This review was performed in the Office of Mission Assurance and Security Services (MA&SS) at the IRS Headquarters in New Carrollton, Maryland, during April and May 2004. We delayed issuing this report so we could include modifications the IRS was making to the POA&M process for its Fiscal Year (FY) 2004 Federal Information Security Management Act (FISMA)[2] report for the period ending August 31, 2004. The audit was conducted in

[1] OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Actions and Milestones, dated October 17, 2001.
[2] The FISMA is part of the E-Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.

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.

The Current Method to Track Security Weaknesses Is Not Reliable or Effective

The IRS has prepared POA&Ms to track both program-level and system-level weaknesses. However, the process it uses to identify weaknesses and report progress is flawed and ineffective. As a result, information provided to the Department of the Treasury and the OMB has been inaccurate and misleading.

Without an effective POA&M process, the IRS cannot identify and monitor security weaknesses to ensure the most significant weaknesses are timely addressed. In addition, the Department of the Treasury is developing a central database to track POA&Ms for all its bureaus. It envisions using this database to generate quarterly reports for the OMB. As the Department of the Treasury's largest bureau, the IRS must maintain an adequate POA&M process if the database is to be reliable. Also, without an effective POA&M process, the IRS will be unable to achieve either a green or yellow status on the E-Government Scorecard.

In our opinion, the IRS has not provided sufficient emphasis and instilled the discipline necessary to ensure it has a system in place to monitor security weaknesses. Consequently, it has reported only general weaknesses for its systems and overstated the actions it has taken to improve the security program.

The program-level POA&M cannot be used to monitor progress in addressing program-level weaknesses

The program-level POA&M addresses weaknesses that may affect security IRS-wide. Generally, the Chief, MA&SS, is responsible for preparing the POA&M and resolving these weaknesses.

For the quarter ending June 2004, the IRS reported nine computer security weaknesses on one program-level

POA&M. The nine weaknesses coincided with the nine security issues of the computer security material weakness.[3]

In August 2004, the IRS modified the program-level POA&M. It now includes 86 security weaknesses (1 plan for all 9 material weakness areas and 85 new computer security program-level weaknesses). The new weaknesses relate to the 85 Government Accountability Office (GAO) and Treasury Inspector General for Tax Administration (TIGTA) audit reports with open recommendations. These weaknesses had not been reported on prior submissions of the program-level POA&M.

However, the program-level POA&M cannot yet be used as a tool to track and monitor the IRS' progress in addressing its security program weaknesses. We have the following concerns:

- The number of program-level weaknesses reported to the Department of the Treasury is significantly understated. The IRS considered each GAO and TIGTA audit report to be one weakness, listing only the title of the report as the weakness. Since GAO and TIGTA reports generally identify more than 1 weakness, the actual number is several times the 85 weaknesses reported by the IRS.
- The POA&M indicates the status of all milestones is ongoing and does not reflect interim corrective actions that may have already been taken. The completion date for all program-level weaknesses is September 2005, which does not coincide with the corrective actions provided to the TIGTA reports.

[3] The IRS currently reports computer security as a material weakness. This material weakness is comprised of nine component security areas: 1) network access controls, 2) system and application access controls, 3) configuration management, 4) delineation of security roles and responsibilities, 5) segregation of system and security administration duties, 6) disaster recovery, 7) audit trails, 8) security training, and 9) certification and accreditation.

System-level POA&Ms cannot be used to monitor progress in identifying and correcting security weaknesses in the IRS' major systems

System-level POA&Ms address weaknesses that are specific to individual systems. Generally, the owner of the system, either the business unit owner or the Chief Information Officer (CIO), is responsible for preparing system-level POA&Ms and resolving these weaknesses.

The system-level POA&Ms the IRS prepared did not accurately and completely describe security weaknesses and milestones and understated the number of system-level weaknesses reported to the Department of the Treasury. The IRS stated the system security self-assessments it conducted in 2003 were the basis for identifying weaknesses included in the POA&Ms. In an earlier report,[4] we took exception to the approach taken by the IRS in conducting the self-assessments because the assessments did not include testing security controls.

In June 2004, the IRS provided the Department of the Treasury and the OMB with system-level POA&Ms for 92 major systems. The POA&Ms showed almost all of the systems had identical weaknesses. These weaknesses coincided with the 17 control topics provided by the National Institute of Standards and Technology (NIST) in its *Security Self-Assessment Guide for Information Technology Systems*[5] (5 management control weaknesses, 9 operational control weaknesses, and 3 technical control weaknesses).

The milestones for each system were also nearly identical, indicating certification and accreditation activities as the corrective actions. Milestones for each of the general support systems were identical.

In August 2004, the IRS revised the system-level POA&Ms. There are now 80 system-level POA&Ms, 1 for each of the revised number of systems in the major systems inventory. However, the number of weaknesses is understated, and the information provided on the system-level POA&Ms is still

[4] *Performance Data for the Security Program Should Be Corrected* (Reference Number 2004-20-093, dated April 2004).
[5] SP 800-26, dated November 2001.

so general and vague that the IRS, TIGTA, GAO, Department of the Treasury, and OMB could not use them to monitor the progress of the IRS security program. For example:

- The weaknesses are still based on insufficient self-assessments because, as was true for FY 2003, the FY 2004 self-assessments did not include testing of security controls. We know of no testing that was done to identify specific security weaknesses.
- The weaknesses are still nearly identical for each system and are stated in terms of the NIST control areas rather than as specific security weaknesses.
- The milestones for all of the applications are identical: (1) assign accountable personnel, (2) perform gap analysis, (3) design and test process, and (4) implement solution.
- The IRS claims system-level POA&Ms must be vague to preclude an unauthorized or inadvertent disclosure of sensitive information. We disagree with this assertion. Oversight officials authorized to review POA&Ms must see the detailed weaknesses and milestones to be able to monitor progress on the corrective actions.
- The number of system-level weaknesses reported to the Department of the Treasury is understated. In September 2004, the IRS reported only 319 system-level weaknesses at the beginning of the quarter. This number is understated because it represents only 3 of the 17 NIST security controls for each system such as the lack of certification and accreditation, or the lack of a security plan or tested contingency plan. Generally, operational and technical control weaknesses were not reported. Without reliable self-assessment results, as reported earlier, we cannot determine the actual number of weaknesses for each system; however, we estimate that it would be many times more than the number reported to the Department of the Treasury if all 17 NIST control areas were included.
- The number of TIGTA-identified weaknesses is also understated in the system-level POA&Ms. The TIGTA report titles are listed as the weaknesses rather than

listing the specific management, operational, and technical control weaknesses described in the reports.

- The system-level POA&Ms do not include the names of individuals responsible for correcting the security weaknesses. Instead, only the responsible organizational units are named.

Progress in addressing the weaknesses was overstated. Weaknesses were closed off the system-level POA&Ms when a system was certified and accredited. No testing was done to evaluate specific security weaknesses. Instead, the IRS assumed if a system had been certified and accredited, then all weaknesses noted on the system's POA&M could be closed. The only exception was that a weakness would remain open on the POA&M for any certified and accredited systems that did not have a tested contingency plan.

The IRS apparently assumed certification and accreditation meant all weaknesses had been addressed. This assumption is not valid since certified and accredited systems can still have security weaknesses. We know of no testing that was conducted to ensure all specific security weaknesses were, in fact, corrected before the system-level POA&Ms were closed.

Recommendations

The Chief, MA&SS, should coordinate with the CIO and business unit owners to:

1. Develop POA&Ms that specifically identify known security weaknesses, provide detailed corrective actions, and identify responsible officials. All known weaknesses should be included in either program-level or system-level POA&Ms, and the POA&Ms should contain details sufficient to allow oversight of the IRS security program.

Management's Response: The Chief, MA&SS, has established a FISMA working group of executives and senior staff from the business units and the Modernization and Information Technology Services organization. The group will develop and implement an

enterprise approach to managing the IRS' POA&M process. This approach will ensure that POA&Ms include all known security weaknesses, provide detailed corrective actions, and identify responsible officials.

2. Accurately report the results of efforts to correct security weaknesses for both program-level and system-level weaknesses. Testing should be conducted to ensure weaknesses have been corrected before the POA&Ms are closed.

Management's Response: To ensure weaknesses are corrected before being reported as closed, the Chief, MA&SS, in coordination with the CIO and business unit owners, will develop a matrix to allow the reconciliation and validation of corrective actions through the testing process.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of the Internal Revenue Service's (IRS) process for monitoring security weaknesses. The purpose of the review was to evaluate the Plans of Action and Milestones (POA&M) process employed by the IRS and determine whether the POA&M process satisfies the Office of Management and Budget (OMB) requirements and assists the agency in managing its risk and vulnerabilities. We also wanted to establish the method used to track vulnerabilities identified by various oversight sources. To accomplish this objective, we:

I. Determined the method used by the Office of Mission Assurance and Security Services to track known security vulnerabilities.

II. Determined whether the sources used to track these vulnerabilities included the following information, as required by the OMB, in order to prepare a POA&M:

   A. Type of weakness.

   B. Office or organization responsible for resolving the weakness.

   C. Key milestones with completion dates.

   D. Source of the identified weakness (e.g., Treasury Inspector General for Tax Administration, Government Accountability Office, internal functions).

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Gerald Horn, Audit Manager
Joan Raniolo, Senior Auditor
William Simmons, Senior Auditor
Charles Ekholm, Auditor
George Franklin, 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 Management Controls OS:CFO:AR:M
Audit Liaisons:
- Chief Information Officer OS:CIO
- Chief, Mission Assurance and Security Services OS:MA

Appendix IV

Management's Response to the Draft Report

CHIEF
MISSION ASSURANCE

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

RECEIVED
JAN 05 2005

January 5, 2005

MEMORANDUM FOR TREASURY ACTING DEPUTY INSPECTOR GENERAL
FOR AUDIT

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

SUBJECT: Response to Draft Audit Report – The Method of Tracking Corrective Actions for Known Security Weaknesses Has Not Been Adequately Developed (Audit # 200420030)

This is in response to your memorandum of November 29, 2004 on the above subject. Mission Assurance and Security Services (MA&SS) has also recognized the process for managing known computer security weaknesses, identified in your draft report, as needing improvement. Our office has already initiated a number of activities related to correcting this problem, including:

- Integrating all Government Accountability Office (GAO) Limited Official Use (LOU) recommendations into Treasury's Joint Audit Management Enterprise Systems (JAMES) to allow one source for tracking Planned Corrective Actions (PCA) related to TIGTA and GAO audit findings and recommendations.

- Establishing a Federal Information Security Management Act (FISMA) working group, consisting of executives and senior staff from each of the business units and from Modernization and Information Technology Services (MITS), to develop an enterprise approach to instituting FISMA as a core organizational process. One of the major action items of that working group is to develop and implement an enterprise approach to managing the IRS's Plan of Action and Milestones (POA&M) process. Consistent with the FISMA guidelines, all security weaknesses identified from internal or external audits, self-assessments or controls testing, will be addressed within the risk-based/cost-effective model that is being developed by a sub-group of the FISMA working group.

- Teaming with the Department of Treasury in the procurement of an automated tool to standardize and streamline, department-wide, the POA&M reporting and tracking processes. The current Treasury Federal Manager's Financial Integrity Act (FMFIA) processes for tracking and reporting material weaknesses via the Treasury JAMES database is being addressed to synchronize the reporting under this process with Treasury's overall FISMA POA&M process.

My staff has also partnered with the Chief Information Officer (CIO) and the business units and developed the attached corrective action plan for each of your report recommendations. We will use this plan to ensure we have a more effective process to manage our POA&M.

If you have any questions, please contact me at (202) 622-8910 or Ellen Pieklo, Deputy Director, Certification Testing, Evaluation, and Assessment at (585) 262-1185.

Attachment

Management Response to Draft Audit Report – The Method of Tracking Corrective Actions for Know Security Weaknesses Has Not Been Adequately Developed (Audit # 200420030)

RECOMMENDATION #1:

The Chief, Mission Assurance & Security Services (MA&SS), should coordinate with the Chief Information Officer (CIO) and business unit owners to develop Plan of Action and Milestones (POA&Ms) that specifically identify known security weaknesses, provide detailed corrective actions, and identify responsible officials. All known weaknesses should be included in either program-level or system-level POA&Ms, and the POA&Ms should contain details sufficient to allow oversight of the IRS security program.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The IRS has established a Federal Information Security Management Act (FISMA) Working Group of executives and senior staff from the business units and from Modernization and Information Technology Services (MITS) to develop an enterprise approach to instituting FISMA as a core organizational process. One of the major action items of that working group is to develop and implement an enterprise approach to managing the IRS's POA&M process. Consistent with the FISMA guidelines, all security weaknesses identified from internal or external audits, self-assessments or controls testing, will be addressed within the risk-based/cost-effective model that is being developed by a sub-group of the FISMA working group.

The Chief, MA&SS, will coordinate with the CIO and business unit owners to ensure all system POA&Ms, generated currently as part of the certification Security Test and Evaluation process, are included in the FISMA POA&M to specifically identify known security weaknesses. The FISMA POA&M will provide detailed corrective actions and identify responsible officials.

In addition, the IRS will ensure the FISMA POA&M consistently identifies corrective actions by line-item, rather than grouping certain corrective actions by external audit reports, to ensure there is not a perception of an underreporting of corrective actions.

IMPLEMENTATION DATE:

10/18/05

RESPONSIBLE OFFICIAL:

OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:

The Chief, MA&SS, will develop a reconciliation process to ensure all POA&M items are recorded in the FISMA POA&M, for system level weaknesses. In addition, MA&SS will monitor and review the POA&M, at least quarterly, to ensure all corrective actions are being developed and that progress toward correcting deficiencies is being accomplished.

RECOMMENDATION #2:

The Chief, Mission Assurance & Security Services (MA&SS), should coordinate with the Chief Information Officer (CIO) and business unit owners to accurately report the results of efforts to correct security weaknesses for both program-level and system-level weaknesses. Testing should be conducted to ensure weaknesses have been corrected before the Plan of Action and Milestones (POA&Ms) are closed.

CORRECTIVE ACTION TO RECOMMENDATION #2:

The Chief, MA&SS will coordinate with the CIO and business unit owners to accurately report the results of efforts to correct security weaknesses for both program-level and system-level weaknesses. A matrix will be developed to allow the reconciliation and validation of corrective actions through the testing process. The supporting process will enable cross-referencing of corrective actions with testing efforts. This will ensure the actions are validated as corrected before the planned corrective actions are closed.

IMPLEMENTATION DATE:

10/18/05

RESPONSIBLE OFFICIAL:

OS:MA:CT

CORRECTIVE ACTION MONITORING PLAN:

The management process will integrate a monitoring process to verify, at least quarterly, that testing of corrective actions is taking place for closing of corrective actions.