Performance Data for the Security Program Should Be Corrected

April 2004

Reference Number: 2004-20-093

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

April 27, 2004

MEMORANDUM FOR COMMISSIONER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Performance Data for the Security Program Should Be Corrected (Audit # 200420001)

This report presents the results of our review of the Internal Revenue Service (IRS) security program performance data. The overall objective of this review was to validate performance measure data reported by the IRS to the Department of the Treasury related to the number of systems that underwent a security self-assessment in Fiscal Year (FY) 2003. This report is being furnished to you since protection of taxpayer information is the ultimate responsibility of all IRS executives and managers.

The Federal Information Security Management Act (FISMA)[1] requires Federal Government agencies to annually assess the security controls in place to protect the information and systems that support their operations and to report those results to the Office of Management and Budget (OMB). To ensure sensitive taxpayer information is adequately and appropriately protected, business unit leaders must take ownership of the security of their assigned systems and integrate security into daily program responsibilities.

In summary, we found that the information provided by the Chief Information Officer (CIO) to the Department of the Treasury in September 2003 was inaccurate. Neither the IRS business unit managers nor the CIO's staff tested security controls for the 352 applications that required a security self-assessment. Specifically, the CIO's staff sorted the 352 applications into 10 groups, 1 group for each of the 10 operating systems. All applications assigned to an operating system were given the same assessment as each of the other applications for that operating system. Apparently, the CIO's staff assumed every application running on an operating system had the same controls. The business unit managers who own the applications were asked to validate

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

that the assessments for the operating systems were accurate for the respective applications, even though no testing of the application controls was conducted.

While we agree it is important for the Information Technology organization to test operating system controls, it is also important for business unit managers to ensure application security controls are tested. Application security controls are critical for providing adequate security over taxpayer data. Application security controls often provide the last defense against a disgruntled employee or contractor who may wish to inappropriately access sensitive information or disrupt computer operations.

The OMB did not issue instructions to Federal Government agencies for completing the FY 2003 FISMA reports until August 2003. However, self-assessments have been required since October 2000 by the Government Information Security Reporting Act.[2] The IRS did not begin to conduct its self-assessments until the summer of 2003. As a result, it rushed to answer the required questionnaire and jeopardized the credibility of the assessment process by claiming that all applications running on a specific operating system had the same level of controls.

We recommended the Commissioner hold business unit managers accountable for the security of their applications and ensure annual self-assessments of their applications are conducted in accordance with the FISMA requirements. To ensure accurate information is reported in compliance with the FISMA, we recommended the Chief, Mission Assurance, amend the IRS information provided to the Department of the Treasury in September 2003 and resubmit the corrected information. We also recommended the Chief, Mission Assurance, coordinate with business unit managers to define the roles and responsibilities for assessing the security of all sensitive applications for the FY 2004 self-assessments required by the FISMA.

Management's Response: IRS management agreed that business unit managers should be held accountable for ensuring annual self-assessments of their systems are conducted. The response stated that actions have already been taken to address this issue and provided no further corrective actions.

Management disagreed with our recommendation that the Chief, Mission Assurance, revise the number of systems reported to the Department of the Treasury to reflect that the IRS assessed 10 operating systems but did not review any sensitive applications. They stated that all systems/applications were reviewed to determine the managerial, technical, and operational security measures in place. Management also stated that managerial and operational controls were reviewed through methods other than the FISMA self-assessments.

Finally, management agreed with our recommendation that the Chief, Mission Assurance, coordinate with business unit managers to help define the roles and responsibilities for assessing the security of all sensitive applications during FY 2004 in accordance with the FISMA. Corrective actions are in process. Management's complete response to the draft report is included as Appendix V.

---

[2] FY 2001 Defense Authorization Act (P.L. 106-398).

Office of Audit Comment: Management actions taken to ensure business unit managers are accountable for the security of their systems and annual tests of their applications are conducted have not been effective. To adequately protect information, business unit managers must understand the current status of their security programs and the security controls planned or in place in order to make informed judgments and investments that appropriately reduce risk. As we reported, the IRS has yet to conduct self-assessments of any of its applications, other than those that have undergone certification and accreditation. Without annual testing as required by the FISMA, management has no means to fully understand the current status of their security controls. Signing a form that presents an assessment of an operating system does not, in our view, provide management with an adequate basis for understanding the security of its applications.

We continue to maintain the validity of our recommendation that the IRS revise the number of systems reviewed as reported to the Department of the Treasury. It is inaccurate for the IRS to state that 569 systems/applications were reviewed. As stated in our report, all applications assigned to an operating system were given the same assessment as each of the other applications for that operating system, thus indicating that operating systems were assessed but applications were not. We also maintain the identical assessments indicate that reviews of managerial and operational controls in the applications were not conducted through other methods.

In addition, the Chief, Mission Assurance, stated that the IRS has revised its categorization of systems/applications for certification and accreditation activities as well as for vulnerability tracking and FISMA reporting. Initially, 87 general support systems, major applications, and applications of interest have been identified and will be used as the basis for FY 2004 FISMA reporting. The Chief, Mission Assurance, is attempting to bundle or associate the remaining low-impact applications with those 87 systems and applications scheduled for certification. This approach seems to be consistent with guidance from the National Institute of Standards and Technology (NIST) for certification and accreditation activities.[3] However, to fully comply with the guidance, the IRS must conduct at least some testing based on risk on the low-impact applications, not just the 87 major systems and applications.

While we still believe our recommendation is worthwhile, we do not intend to elevate our disagreement concerning this matter to the Department of the Treasury for resolution. Department of the Treasury and IRS officials are currently seeking clarification regarding the NIST guidance as it relates to the IRS' certification and accreditation activities. We will continue to monitor this issue in relation to the IRS' compliance with the FISMA requirements for FY 2004. 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 your staff may call Margaret E. Begg,

[3] Final Draft Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (dated April 2004).

Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Background

On December 17, 2002, the President signed the Electronic Government Act, which includes Title III, the Federal Information Security Management Act (FISMA).[1] The FISMA and Office of Management and Budget (OMB) guidance provide a framework for annual information technology (IT) security reviews, reporting, and remediation planning to assist Federal Government agencies in meeting their IT security responsibilities.

The FISMA requires that Federal Government agencies annually evaluate and report on the security of their information systems. To promote standardization among the agencies, the OMB requires responses to specific requests for information. Inspectors General are required to respond independently to most of the items requested. Agencies then submit both sets of responses to the OMB with their annual budget requests.

As required by the FISMA, the Treasury Inspector General for Tax Administration and the Internal Revenue Service (IRS) each prepared responses to the information requested by the OMB on the status of security in the IRS for Fiscal Year (FY) 2003. Some of the responses required empirical information for the entire fiscal year, but the responses had to be forwarded to the Department of the Treasury in August 2003 so they could be consolidated with other bureaus and submitted timely to the OMB. None of the IRS system reviews had been completed by August 2003. As a result, the IRS projected results for the number of systems reviewed and submitted an updated report on September 30, 2003.

Guidance from the OMB states that all systems (applications), other than those that have been certified during the current year, must be reviewed. The necessary depth and breadth of an annual review depend on several factors such as the potential risk and magnitude of harm to the system or data, the relative comprehensiveness of last year's review, and the adequacy and successful implementation of planned corrective actions. The salient point is that an effective security program requires maintaining sound and effective computer security practices

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

and demands a comprehensive and continuous understanding of program and system weaknesses.

The OMB requires Federal Government agencies to use the National Institute for Standards and Technology (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, to conduct their annual reviews. The NIST Self-Assessment Guide lists 17 control topics categorized into 3 major control areas: management, operational, and technical. See Appendix IV for further details regarding the three major control areas.

We initiated this review to validate the accuracy of the information reported to the Department of the Treasury regarding the number of systems and applications reviewed. We evaluated the methodology used by the IRS for the security self-assessments and interviewed management from the Large and Mid-Size Business (LMSB), Small Business/ Self-Employed (SB/SE), Tax Exempt and Government Entities (TE/GE), and Wage and Investment (W&I) Divisions who own the majority of IRS systems.

We conducted our audit from October 2003 through January 2004 at the Office of Mission Assurance in New Carrollton, Maryland. The audit was performed 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.

The Internal Revenue Service Did Not Conduct Security Self-Assessments of Its Applications

To maintain adequate security in a network environment, controls are required for each sensitive application and for the operating systems on which the applications run. Operating system controls help ensure only authorized persons have access to the network. Application controls help deter disgruntled employees and contractors who already have access to the network from inappropriately accessing sensitive information and disrupting computer operations.

For the FY 2003 FISMA reporting period covering October 2002 through September 2003, the IRS Security Services function within the Chief Information Officer (CIO) organization was responsible for reviewing security controls for each of the operating systems used in the IRS. The FISMA requires that agency program officials

(business unit managers) annually review the applications supporting their programs. The CIO's staff took the responsibility of providing guidance to business owners and for accumulating and reporting the results to the Department of the Treasury. Beginning in October 2003, the Chief, Mission Assurance, assumed these responsibilities.

For several years, the IRS has struggled to identify the total number of systems and applications and is not yet confident that the total number is accurate. The IRS is working with the Department of the Treasury to identify an accurate inventory of systems and applications, and we are addressing this issue in another review for which we will issue an audit report later this year.

As of September 30, 2003, the IRS reported an inventory of 10 operating systems and 424 sensitive applications. It also reported that 72 sensitive applications had been certified or recertified during FY 2003 and that it had completed self-assessments on the remaining 352 applications.

The information provided by the CIO to the Department of the Treasury in September 2003 was inaccurate. Neither the IRS business unit managers nor the CIO's staff tested security controls for the 352 applications. Instead, the CIO's staff prepared assessments for the 10 operating systems and sorted the 352 applications into 10 groups, 1 group for each of the 10 operating systems. All applications assigned to an operating system were given the same assessment as each of the other applications for that operating system. Apparently, the CIO's staff assumed all applications running on a particular operating system had the same controls.

The business unit managers who own the applications were asked by the CIO's staff to validate that the assessments for the operating systems were accurate for the respective applications, even though no testing of the application controls was conducted. Business unit managers made minimal changes to only 8 (2 percent) of the 352 assessments.

The OMB did not issue instructions to Federal Government agencies for completing the FY 2003 FISMA reports until August 2003. However, self-assessments have been required since October 2000 by the Government

Information Security Reporting Act.[2] The IRS did not begin to conduct its self-assessments until the summer of 2003. As a result, it rushed to answer the NIST questionnaire and jeopardized the credibility of the assessment process by claiming that all applications running on a specific operating system had the same level of controls.

We spoke to representatives of the LMSB, SB/SE, TE/GE, and W&I Divisions to determine the extent of their input to the FY 2003 assessment process. Collectively, these business units own the majority of IRS applications. The representatives stated that they did not have the knowledge or expertise to comment on or validate assessments of the operating systems, nor did they review the current risk assessments and security plans for the applications.

In addition, business unit managers expressed confusion regarding what is expected of them and their roles in meeting the FISMA requirements. They were not sure if they were supposed to partner with the IT organization to gain the necessary expertise or how they would obtain the resources for such an effort. Some were understandably confused as to how an assessment of an operating system could be used to assess an application.

In lieu of providing feedback on the assessments, business unit managers focused their attention on validating application ownership and the assigned risk level for each application. They did sign a statement acknowledging that assessments were completed and that they understood the risks associated with the applications.

Business unit managers also expressed apprehension with the overall assessment process and suggested a need for the Office of Mission Assurance to provide a clear vision and define objectives and expectations, to assist them in executing their responsibilities with the process. They also expressed concern that preparations for the FY 2004 assessment have not been communicated. Because activities for FY 2003 were centered on application ownership and application risk levels, they do not have a clear understanding of what their roles will be in subsequent FISMA initiatives.

---

[2] FY 2001 Defense Authorization Act (P.L. 106-398).

Recommendations

To ensure adequate security of information and systems, the Commissioner should:

1. Hold business unit managers accountable for the security of their applications and ensure annual self-assessments of their sensitive applications are conducted in accordance with the FISMA.

Management's Response: Management agreed with this recommendation. Management cited actions taken during FY 2003 but provided no further corrective actions.

During implementation of the FISMA in 2003, the Office of Mission Assurance conducted numerous briefings and discussions to communicate FISMA requirements and provide guidance to business unit staffs and other senior IRS officials to assist them in completing all required FISMA program reviews or security controls testing. A FISMA Service Level Agreement, which supported the implementation of the FISMA Security Assessments, was approved and signed by the Acting Chief, Security Services, on September 3, 2003.

Office of Audit Comment: The actions taken to ensure business unit managers are accountable for the security of their systems and annual tests of their applications are conducted have not been effective. Business unit managers must understand the current status of their security programs and the security controls planned or in place to protect their information, in order to make informed judgments and investments that appropriately reduce risk.

As we reported, the IRS has yet to conduct self-assessments of any of its applications, other than those that have undergone certification and accreditation. Without annual testing as required by the FISMA, management has no means to understand the current status of their security controls. Signing a form that presents an assessment of an operating system does not, in our view, provide management with an adequate basis for understanding the security of its applications.

To ensure accurate information is reported in compliance with the FISMA, the Chief, Mission Assurance, should:

2. Revise the number of systems reported to the Department of the Treasury to reflect that the IRS assessed only 10 operating systems and did not include reviews of any sensitive applications.

Management's Response: Management disagreed with this recommendation and its related finding. They stated that each of 569 systems/applications was reviewed to determine the managerial, technical, and operational security measures in place. Management also stated that managerial and operational controls were reviewed through methods other than the FISMA self-assessments.

Office of Audit Comment: We maintain it is inaccurate to state that 569 systems/applications were reviewed. As stated in our report, all applications assigned to an operating system were given the same assessment as each of the other applications for that operating system, thus indicating that operating systems were assessed but applications were not. We also maintain the identical assessments indicate that reviews of managerial and operational controls in the applications were not reviewed through other methods.

In addition, the Chief, Mission Assurance, stated that the IRS has revised its categorization of systems/applications for certification and accreditation activities as well as for vulnerability tracking and FISMA reporting. Initially, 87 general support systems, major applications, and applications of interest have been identified and will be used as the basis for FY 2004 FISMA reporting. The Chief, Mission Assurance, is attempting to bundle or associate the remaining low-impact applications with those 87 systems and applications scheduled for certification. This approach seems to be consistent with guidance from the NIST for certification and accreditation activities.[3] However, to fully comply with the guidance, the IRS must conduct at least some testing based on risk on the low-impact applications, not just the 87 major systems and applications.

[3] Final Draft Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (dated April 2004).

3. Coordinate with business unit managers to help define the roles and responsibilities for assessing the security of all sensitive applications during FY 2004 in accordance with the FISMA.

Management's Response: Management agreed with this recommendation and corrective actions are in process. The Office of Mission Assurance will be providing updated guidance to assist the business units and other senior officials in more clearly understanding FISMA requirements and associated roles and responsibilities.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to validate performance measure data reported by the Internal Revenue Service (IRS) to the Department of the Treasury related to the number of systems that underwent a security self-assessment in Fiscal Year 2003. To accomplish this objective, we:

I. Reviewed self-assessments for each of the 352 sensitive applications. We sorted the 352 self-assessments by the operating system to which they were assigned and compared the results. All applications assigned to an operating system were given the same assessment as each of the other applications for that operating system. We confirmed with representatives of the Chief, Mission Assurance, that this was the approach taken. Since tests had not been performed for applications, no further review of the assessments was necessary.

II. Interviewed contact points in the four business units to determine if they had conducted any testing to support the self-assessments assigned to their business units and to discuss their understanding of what their roles will be in subsequent Federal Information Security Management Act[1] self-assessments.

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

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
Abraham Millado, Senior Auditor
Joan Raniolo, Senior Auditor
Charles Ekholm, Auditor

Appendix III

Report Distribution List

Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Commissioner, Large and Mid-Size Business Division SE:LM
Commissioner, Small Business/Self-Employed Division SE:S
Commissioner, Tax Exempt and Government Entities Division SE:T
Commissioner, Wage and Investment Division SE:W
Chief Information Officer OS:CIO
Chief, Mission Assurance OS:MA
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 Liaison: Chief, Mission Assurance OS:MA

Appendix IV

Methodology Required for Self-Assessments

The Office of Management and Budget (OMB) requires Federal Government agencies to use the National Institute for Standards and Technology (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, to conduct their annual reviews. The NIST Self-Assessment Guide lists 17 control topics categorized into 3 major control areas: management, operational, and technical.

Management controls focus on the management of the security system and the management of risk. Management controls include ensuring security plans are current and certifications are performed timely.

Operational controls are primarily implemented and executed by people (as opposed to systems). Some require technical expertise, but many can and should be assessed by operations managers who have no technical expertise.

Technical controls are performed by computer systems. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Each of the 17 control topics in the NIST Self-Assessment Guide has several questions that must be answered by providing the level of effectiveness as follows:

- Level 1 – Control objective documented in a security policy.
- Level 2 – Security controls documented as procedures.
- Level 3 – Procedures have been implemented.
- Level 4 – Procedures and security controls are tested and reviewed.
- Level 5 – Procedures and security controls are fully integrated into a comprehensive program.

The questions should be answered by examining relevant documentation and conducting a rigorous examination and test of controls. The OMB suggests that the General Accounting Office's Federal Information System Controls Audit Manual provides techniques that can be used to test the control objectives.

Appendix V

Management's Response to the Draft Report

CHIEF
MISSION ASSURANCE

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

RECEIVED
APR 05 2004

April 5, 2004

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: Daniel Galik Daniel Galik
Chief, Mission Assurance

SUBJECT: Response to Draft Audit Report – Performance Data Security Program Should Be Corrected (Audit # 200420001)

Thank you for the opportunity to review this draft report entitled, "Performance Data for the Security Program Should Be Corrected". We are attaching a detailed response to each of the three report recommendations in which we concur with two of the recommendations. Information technology (IT) security is a shared responsibility for all senior officials at IRS, and a number of initiatives were pursued in 2003 (and also planned for 2004) to ensure that the appropriate level of emphasis and accountability are in place, and that IRS major systems are compliant with the requirements of the Federal Information Security Management Act. Since the implementation of FISMA in December 2002, various briefings and presentations were conducted at various IRS leadership forums and meetings to inform and provide guidance to the Business Unit Executive team. As indicated in our response, this information was shared at the Technology Security Committee and Security Executive Steering Committee meetings respectively. Additionally, during the implementation of the FISMA, a Service Level Agreement was implemented by Mission Assurance (formally the Office of Security Services) to provide technical security support to the business and functional organizations in completing the required FISMA security assessments.

We disagree with Recommendation 2 regarding revising the number of systems reported to the Treasury. The draft audit report does not accurately reflect the review activities performed in 2003 to identify and validate IRS systems. However, in February 2004, the IRS conducted an evaluation of its overall approach to information systems categorization, and security certification and accreditation. As a result of the evaluation, the IRS developed a comprehensive information security program strategy that will validate the IRS inventory of systems, and provide a new, practical and cost effective certification and accreditation approach that will be fully compliant with the FISMA, National Institute of Security and Technology (NIST), and Office of Management and Budget (OMB) guidance. The IRS strategy is consistent with FISMA, which requires the agency to utilize a risk management approach that properly balances business

requirements and risks, in providing appropriate information security protections and utilizing cost effective security processes. The IRS revised strategy and supporting details related to the total number of major systems was reported to Treasury, and forwarded to OMB in February 2004.

We do agree with Recommendation 3 regarding defining the roles and responsibilities for assessing compliance with FISMA, and corrective actions are in process. The new approach to the categorization of IRS major systems has required us to redefine our FISMA implementation process. Mission Assurance will be providing updated guidance to assist the business units and other senior officials in more clearly understanding all FISMA requirements, and associated roles and responsibilities.

If you have any questions, please contact me at (202) 622-8910, or Colleen Murphy, Director, Assurance Programs at (202) 283-4500.

Attachment

Attachment

Management Response to Draft Audit Report –Performance Data for the Security Program Should Be Corrected (Audit # 200420001)

RECOMMENDATION # 1: To ensure adequate security of information and systems, the Commissioner should hold business unit managers accountable for the security of their applications and ensure that annual self-assessments of their sensitive applications are conducted in accordance with the Federal Information Security Management Act (FISMA).

CORRECTIVE ACTION TO RECOMMENDATION #1:

We agree with the recommendation. The Commissioner recognizes that the security of IRS information and information systems is a shared responsibility for all IRS senior officials. A number of initiatives and activities summarized below were completed in 2003, (and continue in 2004), to ensure that the business unit managers and other senior IRS officials are appropriately engaged in ensuring that the information systems that support their programs and operations are secure, and also compliant with the requirements of FISMA. The technical details associated with activities such as the annual systems security review and system security controls testing, typically require that business unit staffs be provided extensive help and support from expert security staff. The new Mission Assurance organization has been tasked with providing that support to the business units and other senior IRS officials in 2004, to assist them in completing all required FISMA security program reviews or security controls testing.

During the implementation of FISMA in 2003, detailed briefings were presented to the IRS Leadership Team. These briefings were presented at various Technology Security Committee (TSC), and Security Executive Steering Committee (SESC) meetings. The purpose of these Committees was to (1) help ensure that security issues having a significant impact on IRS business practices were resolved on a consistent national basis, with input from all appropriate IRS organizations; and (2) oversee two subordinate committees within the governance structure and serve as an IRS-wide senior leadership forum for security matters. Additionally, briefing sessions and distribution of information regarding FISMA roles, responsibilities and requirements were presented to all IRS-wide FISMA Points of Contact. Further, a FISMA Service Level Agreement, which supported the implementation of the FISMA Security Assessments was approved and signed by the Acting Chief, Security Services on September 3, 2003. Prior to the signing of this document, members of the SESC were briefed on the SLA in June 2003. This document outlined MITS Services and their customers (the Business Operating Divisions (BODs)) FISMA self assessment

actions and responsibilities. The following FISMA briefings and discussions were conducted:

Title	Date	Audience
The FISMA of 2002	1/13/02	SESC
The IRS Implementation of the FISMA of 2002	2/3/03	SESC
IRS Material Weakness/FISMA Management Process	2/19/03	TSC
IRS Material Weakness/FISMA Management Process	3/3/03	SESC
FISMA Implementation NIST 800-26 Questions	3/3/03	SESC
FISMA Discussion	3/3/03	SESC
FISMA Discussion	3/19/03	TSC
2003 Security Data Requests- A Strategic Approach	5/14/03	
FISMA Implementation	6/18/03	TSC
FISMA Systems Security Reviews	8/15/03	IRS FISMA POCs

Upon completion of the FISMA self assessment each Business Unit Executive reviewed and approved a FISMA Systems Security Assessment Validation form indicating that assessments had been completed. All assessments were completed by October 2003.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A

Management Response to Draft Audit Report – Performance Data for the Security Program Should Be Corrected (Audit # 200420001)

RECOMMENDATION # 2: To ensure that accurate information is reported in compliance with the FISMA, the Chief, Mission Assurance, should revise the number of systems reported to the Department of the Treasury to reflect that the IRS assessed only 10 operating systems and did not include reviews of any sensitive applications.

CORRECTIVE ACTION TO RECOMMENDATION #2:

We disagree with this recommendation and its related finding. The recommendation is inconsistent with FISMA reporting guidelines and it does not accurately reflect the review activities that were performed for IRS systems.

The IRS used National Institute for Standards and Technology (NIST) Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, to conduct the annual FISMA review in accordance with OMB requirements. IRS identified 569 systems/applications for review and reporting purposes for FY 2003. Each of the 569 was reviewed to determine the managerial, technical, and operational security measures in place.

The facility location for each of the 569 was identified as well as the operating system platform. The managerial, technical, and operational security measures were reviewed using a variety of methods including online auditing; onsite visits to field offices, service center campuses, and computing centers; interviews with managers, system administrators, security administrators, and operational staffs; use of automated scanning and reporting tools; etc.

The 569 systems/applications may use only 10 different operating systems; however, there are multiple occurrences of each. Each occurrence exists as a separate environment and must be reviewed to ensure that the technical systemic controls provided by the operating system are in place for each of its resident applications, databases, etc. Managerial and operational controls generally exist outside the operating system (e.g., access approvals, review of audit trails, separation of critical functions, etc.) and are reviewed through other methods.

IRS has recently revised its categorization of systems/applications for certification and accreditation activities as well as for vulnerability tracking and FISMA reporting. OMB guidance focuses FISMA reporting activities on "major systems", with no specific detailed guidance for "sensitive" systems. IRS systems/applications will be identified as major applications, applications of interest, or as part of a general support system. Such determinations are in accordance with OMB A-130, NIST Special Publication 800-26, and Treasury

Directive TDP 85-01. The initial identification of 87 total general support systems, major applications, and application of interest has already been submitted to, and reviewed by the Treasury Department and OMB. Preliminary feedback is that they are satisfied with our revised strategy and approach for system categorization, validating our system inventory, and for completing system security certification and accreditation activities. These 87 applications and systems will serve as the basis for FISMA reporting for FY 2004. Each of the previous 569 items will be associated with one of the inventory categories. As the FISMA 2004 annual reviews are completed with each office, Mission Assurance will re-validate the re-categorization of these systems with the business units and other system systems.

IMPLEMENTATION DATE:

N/A

RESPONSIBLE OFFICIAL:

N/A

CORRECTIVE ACTION MONITORING PLAN:

N/A

Management Response to Draft Audit Report – Performance Data for the Security Program Should Be Corrected (Audit # 200420001)

RECOMMENDATION # 3: To ensure that accurate information is reported in compliance with the FISMA, the Chief, Mission Assurance, should coordinate with business unit managers to help define the roles and responsibilities for assessing the security of all sensitive applications during FY 2004 in accordance with the FISMA.

CORRECTIVE ACTION TO RECOMMENDATION #3:

In February 2004, the IRS performed a re-evaluation of its overall approach to information systems security certification and accreditation. As a result, the IRS developed a comprehensive information security program strategy that would validate IRS inventory of systems, and provide a new, practical and cost effective certification and accreditation approach that would be fully compliant with the Federal Information Security Management Act (FISMA), NIST and OMB guidance. This approach was embraced by both Treasury and OMB. As a result, the IRS's FISMA Quarterly Report, dated March 1, 2004 reflected the changes made to the plan and provided a clearer and more concise depiction of the IRS's systems inventory. The FISMA Report addressed the 87 Major Applications (MAs), general support systems (GSS) and applications of interest (AOI) as well as the other applications associated with a GSS. Mission Assurance's, Information Security Program is developing and implementing a communication plan that will be used to provide information, direction and guidance to the Business Unit Executives for assessing the security of their MAs, GSSs, and AOIs for FY 2004.

IMPLEMENTATION DATE:

4/30/04

RESPONSIBLE OFFICIAL:

Director, Assurance Programs OS:MA:AP

CORRECTIVE ACTION MONITORING PLAN:

1. Provide Business Unit Executives with results of the revised Information Systems Security and Certification & Accreditation (C&A) Plan.

2. Provide Business Unit Executives with a copy of the March 1, 2004 FISMA Quarterly Report.

3. Provide Business Unit POCs with briefing to address and discuss FISMA roles and responsibilities.