More Management Attention Is Needed to Protect Critical Assets

July 2005

Reference Number: 2005-20-108

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 15, 2005

MEMORANDUM FOR CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - More Management Attention Is Needed to Protect Critical Assets (Audit # 200520001)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) was making adequate progress in protecting its critical infrastructure and complying with Federal Government requirements. The audit focused on the processes and methodologies the IRS used to document and report on the status of its critical infrastructure protection.

In summary, Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection* dated December 17, 2003, established a national policy for Federal agencies to protect the United States' critical infrastructure and key resources[1] from terrorist attacks. The IRS relies upon critical computer systems to account for over $2 trillion in revenue annually.[2] The importance of these systems to our national security could make them a terrorist target.

HSPD-7 required all Federal agencies to develop plans to protect their critical infrastructure by July 31, 2004. The IRS timely provided the Department of the Treasury a list of 19 critical assets that had been identified in the latter part of 1998 in response to *The Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD-63),* dated May 1998. The Department of the Treasury also required all bureaus to update their list of critical infrastructure by September 2005. The IRS is still in the process of performing the analysis necessary to identify its critical assets and expects to have it completed by the Department of the Treasury's deadline.

---

[1] Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating affect on national security, national economic security, national public health or safety, or any combination of these matters. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy or government.
[2] *Financial Audit: IRS's Fiscal Years 2004 and 2003 Financial Statements* (GAO-05-103, dated November 2004).

Although the IRS expects to meet the goals established by the Department of the Treasury, sufficient attention has not been given to keeping the list of critical assets current. The IRS does not have a process to regularly review its inventory of critical assets to ensure it remains current and complete. To respond to the Department of the Treasury mandate, the IRS had to begin the current identification process by analyzing its complete inventory of assets rather than just adjusting it for recent year changes. The lack of a current listing increases the risks that critical assets may not be protected.

We also believe the IRS could have reacted more promptly to HSPD-7. The Directive allowed 7 months for agencies to develop and submit plans to the Office of Management and Budget that addressed the identification, prioritization, and protection of their critical assets. Based on the current schedule, the IRS will require 21 months just to finish the analysis necessary to complete an updated list of critical assets. Sufficient Mission Assurance and Security Services (MA&SS) organization resources have not been devoted to ensuring a proactive response in implementing HSPD-7. In addition, business unit owners who are most familiar with the criticality of their systems have not been involved yet in this process.

After its critical assets are identified, the IRS will need to adequately assess those assets for vulnerabilities, and then develop and implement plans to protect them. Since a new list of critical assets had not been completed yet, we reviewed the IRS' progress in securing 17 potential critical assets identified by its ongoing analysis. These assets are vital to the IRS' returns processing, law enforcement, and customer service responsibilities. Operational and technical controls for these systems have not been adequately tested and prioritized. In addition, plans for correcting the weaknesses that had been identified are not adequate. We believe business unit owners have been slow to accept responsibility for the security of their systems, and they have not devoted sufficient attention to testing and correcting security weaknesses, even for critical assets.

To ensure the IRS maintains a current and complete list of critical infrastructure assets, we recommended the Chief, MA&SS, coordinate with all business units at least annually to confirm the IRS' list of critical assets is accurate and complete. More emphasis should also be placed on completing the IRS' current efforts to identify its critical assets. Since we have previously reported deficiencies in how the IRS tested systems for vulnerabilities and how it developed corrective action plans to reduce known vulnerabilities, we are making no additional recommendations in these areas.

Management's Response: The Chief, MA&SS, concurred with our recommendations and will ensure a written survey is developed and distributed to all IRS business units possessing one or more critical assets. The results of the survey will be compiled and approved by IRS executives and will represent an updated list of critical assets. Also, the Chief, MA&SS, will coordinate with all business units, at least annually, to confirm the IRS' list of critical assets is accurate and complete. A specific timetable for this coordination is included in the response. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

More Management Attention Is Needed to Protect Critical Assets

Background

On December 17, 2003, the President signed Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection.* HSPD-7 established a national policy for Federal Government agencies to protect the United States' critical infrastructure and key resources[1] from terrorist attacks.

While an estimated 85 percent of the United States' critical infrastructure and key resources are owned and operated by the private sector,[2] the Federal Government also owns and operates critical infrastructure and key resources. The Internal Revenue Service (IRS), for example, relies upon computer systems to account for over $2 trillion in revenue annually.[3] Terrorists could attack these computer systems to gain access to taxpayers' sensitive financial information or to disrupt computer operations.

Under HSPD-7, all Federal agency heads are responsible for:

- Identifying the agency's critical infrastructure.
- Assessing and prioritizing critical infrastructure based on vulnerabilities and risks.
- Developing and implementing plans to protect critical infrastructure and using metrics to measure and communicate program effectiveness.

We conducted this review to evaluate the IRS' progress in addressing these responsibilities. The review was performed at the Mission Assurance and Security Services (MA&SS) offices in New Carrollton, Maryland, and the Enterprise Resilience and Critical Infrastructure Protection Program Office in New York, New York, during the period

---

[1] Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating affect on national security, national economic security, national public health or safety, or any combination of these matters. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

[2] *Guidance for Developing Sector-Specific Plans,* Department of Homeland Security, dated April 2, 2004.

[3] *Financial Audit: IRS's Fiscal Years 2004 and 2003 Financial Statements* (GAO-05-103, dated November 2004).

November 2004 through January 2005. 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.

The List of Critical Assets Is Not Current

The Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD-63), dated May 1998, directed Federal agencies to implement plans for protecting Federally owned critical infrastructure by May 2000. In response to PDD-63, the IRS identified 19 critical assets in November 1998.

HSPD-7 superseded PDD-63 and required the heads of all Federal agencies to submit to the Director, Office of Management and Budget (OMB), by July 31, 2004, plans for protecting their physical and cyber critical infrastructure. The Department of the Treasury is also requiring all bureaus to identify a more current set of critical assets using a tool developed by the Department of Commerce called Project Matrix. The IRS expects to complete its analyses and have a new list of critical assets by September 2005.

To update the November 1998 list of 19 critical assets, the IRS began with a universe of about 350 computer systems and 730 buildings. Next, using criteria provided by the Department of the Treasury, it identified 96 assets that were considered potential critical assets and, in March 2005, refined the list to 17 (14 systems and 3 buildings). Plans call for detailed questionnaires to be completed by the business unit owners of each of the 14 systems and reviewed by the Department of the Treasury and the IRS' MA&SS organization.

All 17 assets are vital to the IRS' returns processing, law enforcement, and customer service responsibilities. The 17 assets were previously included in the original list of critical assets identified in the list issued in November 1998.[4]

Although the IRS expects to meet the goals established by the Department of the Treasury, sufficient emphasis has not been given to maintaining a current list of critical assets.

[4] Two telecommunications assets were no longer considered critical.

The MA&SS organization did not have a process to regularly review its inventory of critical assets to ensure it remained current and complete. As a result, the IRS had to begin the current identification process by analyzing its complete inventory of assets rather than just adjusting it for recent year changes. The lack of a current listing increased the risks that critical assets may not be protected.

We also believe the IRS could have reacted more promptly to HSPD-7. The Directive allowed 7 months for agencies to develop and submit plans to the OMB to address the identification, prioritization, and protection of their critical assets. Based on the current schedule, the IRS will require 21 months just to finish the analysis necessary to complete an updated list of critical assets.

MA&SS organization management was not devoting sufficient resources to ensuring a proactive response in implementing HSPD-7. Initially, only 1 person from the MA&SS organization was assigned to evaluate the 350 systems to derive the 96 potential critical systems. Two MA&SS and 1 Department of the Treasury critical infrastructure protection program staff members worked to reduce the 96 systems to 17. In addition, business unit owners who are in the best position to determine the criticality of their systems were not scheduled to be involved until the end of the identification process. As of April 2005, questionnaires had not been issued yet to the business owners of these systems.

Identifying and maintaining a list of critical assets is the first step required in critical infrastructure protection planning. Until the IRS fully identifies its critical infrastructure and undertakes regular, repeated reviews of the list to keep it current, the IRS may not be able to ensure its critical infrastructure is adequately secured.

Recommendations

The Chief, MA&SS, should:

1. Coordinate with all business units to complete the process of identifying a current list of critical assets to comply with HSPD-7 and ensure the protection of those assets.

Management's Response: The Chief, MA&SS, will ensure a written survey is developed and distributed for completion by all IRS business units possessing critical assets. The survey results will be compiled, approved by IRS executives, and will represent an updated list of critical assets.

2. Coordinate with all business units at least annually to confirm the IRS' list of critical assets is accurate and complete.

Management's Response: The Chief, MA&SS, will coordinate with all business units, at least annually, to confirm the IRS' list of critical assets is accurate and complete. The process will include issuing a memorandum by August 15 of each year asking the business units to complete the previously mentioned survey by September 15. The results will be presented to the Chief, MA&SS, for approval no later than October 15, and submitted to the Deputy Commissioner for Operations Support for final approval. This process will be repeated annually.

Critical Assets Are Not Adequately Assessed for Vulnerabilities and Prioritized

After the IRS identifies its critical assets, it will need to adequately assess those assets for vulnerabilities. Federal Government requirements for assessing both critical and noncritical computer systems for vulnerabilities existed for many years prior to HSPD-7. OMB Circular No. A-130, *Security of Federal Automated Information Resources*, originally issued in 1985, requires agencies to secure their computer systems. Under the Federal Information Security Management Act of 2002 (FISMA)[5] and its predecessor, the Government Information Security Reform Act of 2000,[6] agencies are required to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

When security weaknesses are identified, the Department of the Treasury and the OMB require the vulnerabilities and

[5] The FISMA is part of the E-Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.
[6] National Defense Authorization, Fiscal Year 2001, § 1061, Pub L. No. 106-398 (2000), 114 Stat. 1654.

related corrective actions to be documented and tracked in Plans of Action and Milestones (POA&Ms). We reviewed the POA&Ms and other information to determine the status of security controls for the IRS' latest list of 17 potential critical assets.

According to those documents, the 17 potential critical assets were not adequately secured, making them unnecessarily vulnerable to attack. At the time of our review, the IRS reported the following vulnerabilities:

- Two critical computer systems did not have completed certifications.
- Three critical computer systems were not accredited.[7]
- Two critical computer systems did not have security plans.
- Two critical computer systems did not have contingency plans.[8]
- Seven critical computer systems did not have tested contingency plans.
- Physical security compliance reviews had not been completed at 2 of the 3 Computing Centers[9] within the last 2 years. A physical vulnerability assessment was not performed for the third Computing Center location.

In addition, the 14 potentially critical computer systems were not adequately reviewed for operational and technical security controls. Operational controls are primarily implemented and executed by people (as opposed to systems) and include, for example, personnel security and

[7] Accreditation is the official management decision to authorize the operation of a system, accepting the risk to operations based on the implementation of an agreed upon set of security controls.
[8] Contingency planning is a requirement for all general support systems and major applications. Compliance with HSPD-7 requires critical assets to have Business Continuity Plans, which include a suite of four plans: Incident Management Plan, Occupant Emergency Plan, Business Resumption Plan, and Information Technology Disaster Recovery Plan.
[9] Facilities that support tax processing and information management through a data processing and telecommunications infrastructure.

security awareness, training, and education. Technical controls are executed by computer systems and include, for example, logical access controls and audit trails. Without adequate testing, the IRS cannot determine whether security policies and procedures had been implemented effectively.

The FISMA requires that, at least annually, agency program officials (business unit owners) review the security controls of the systems they use to carry out their responsibilities. OMB guidance states the evaluations should be based on the testing of management, operational, and technical controls to determine whether policies and procedures had been developed and implemented.

Testing and prioritizing critical assets for vulnerabilities was not adequate because business unit owners had not taken responsibility for the security of their systems. Critical assets, in particular, had not received adequate attention from IRS management.

Because we have reported this condition in a recent Treasury Inspector General for Tax Administration (TIGTA) memorandum[10] to the Chief, MA&SS, regarding the IRS' compliance with the FISMA, we are making no additional recommendations.

Plans to Protect Critical Assets Are Not Complete

After vulnerabilities of critical assets have been identified, HSPD-7 requires plans be developed for correcting vulnerabilities. Even before HSPD-7, Federal laws and guidance required plans be developed and implemented to reduce security weaknesses.

In a prior review,[11] we reported that POA&Ms for both critical and noncritical systems are of limited value because they are based on the inadequate vulnerability assessments we described earlier. Implementing the corrective actions in a POA&M may not necessarily mean a system has been secured if all vulnerabilities were not identified and entered into the POA&M.

[10] Memorandum dated September 10, 2004.
[11] *The Method of Tracking Corrective Actions for Known Security Weaknesses Has Not Been Adequately Developed* (Reference Number 2005-20-027, dated January 2005).

In addition, we reported that both critical and noncritical computer systems had nearly identical milestone dates for the correction of all listed weaknesses. The corrective actions for all of the applications were identical: (1) assign accountable personnel, (2) perform gap analysis, (3) design and test process, and (4) implement solution.

Without an effective POA&M process, the IRS cannot adequately prioritize security deficiencies to ensure significant weaknesses of critical assets are timely addressed and resolved.

Since our original reporting of problems with the POA&Ms, the IRS has made a significant effort to improve them and is in the process of correcting other problems we raised with the POA&Ms. As part of our Fiscal Year 2005 FISMA evaluation, we will be assessing the adequacy of IRS management's ongoing effort to improve the POA&M process. Because we have reported these conditions and made recommendations in prior TIGTA audit reports, we are making no additional recommendations.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) was making adequate progress in protecting critical infrastructure and complying with Federal Government requirements. To accomplish our objective, we:

I. Obtained the necessary background information on protecting critical assets.

- A. Identified and reviewed critical infrastructure protection requirements set forth by the various requirement setting authorities.
- B. Obtained and reviewed the Critical Infrastructure Protection Plan the IRS submitted to the Department of the Treasury for inclusion in the Departmental Critical Infrastructure Protection Plan submitted to the Office of Management and Budget (OMB).
- C. Contacted appropriate personnel in the Department of the Treasury to obtain the instructions and guidelines issued to the bureaus.

II. Evaluated the IRS' efforts to identify its critical infrastructure.

- A. Determined the instructions, criteria, and due dates issued by the Department of Homeland Security, the OMB, and the Department of the Treasury for determining which infrastructures were critical.
- B. Obtained and reviewed the list of IRS critical infrastructure assets.
- C. Evaluated the process and criteria the IRS used to identify its critical assets.

III. Determined whether the IRS' critical assets were assessed for vulnerabilities and whether corrective actions had been taken to reduce those vulnerabilities.

- A. Determined whether testing was performed by the Modernization and Information Technology Services organization, the Mission Assurance and Security Services organization, or the business units.
- B. Determined whether the IRS used certification and accreditation results and, if so, whether the certification and accreditation was conducted within the last 12 months.
- C. Determined whether the IRS conducted annual reviews to identify and assess vulnerabilities.
- D. Reviewed Plans of Action and Milestones to determine whether vulnerabilities had been identified and corrective actions and milestones had been developed to reduce the vulnerabilities.

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
Richard Borst, Lead Auditor
Allen Gray, Senior Auditor
Jody Kitazono, Senior Auditor
Charles Ekholm, 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 Service 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
JUL 07 2005

July 6, 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Response to Draft Audit Report – More Management Attention Is Needed to Protect Critical Assets (Audit # 200520001)

Security at the Internal Revenue Service (IRS) is a top priority and we are actively engaged in efforts to adhere to Homeland Security Presidential Directive/HSPD-7, which establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. A major component of the directive requires each Federal department and agency to develop and implement a plan to protect its critical infrastructure. To comply with HSPD-7, the Department of the Treasury has developed a Treasury Cyber Critical Infrastructure Protection Plan to address threats and vulnerabilities to Treasury-owned and operated key assets and resources.

The IRS has been responsive to the Department of the Treasury's strategy and plan. Using new criteria provided by the Department of the Treasury, we identified 17 candidates for nationally critical assets. We are in the process of collecting additional information on each candidate asset from the applicable business units. The Treasury Department will analyze and score the information to obtain a prioritized composite list of Treasury's nationally critical assets. To ensure that the critical asset list is accurate and complete, we have established a process to perform an annual evaluation of the list.

We concur with both of the report recommendations on protecting critical assets. Attached are our detailed responses. If you have any questions, please contact me at (202) 622-8910 or Charles Hopkins, Director, Emergency Management Programs at (202) 622-4025.

Attachment

Attachment

Management Response to Draft Audit Report – More Management Attention Is Needed to Protect Critical Assets (Audit # 200520001)

RECOMMENDATION # 1: The Chief, Mission Assurance and Security Services should coordinate with all business units to complete the process of identifying a current list of critical assets to comply with Homeland Security Presidential Directive/HSPD-7 and ensure the protection of those assets.

CORRECTIVE ACTION TO RECOMMENDATION #1:

We concur with the recommendation. The Chief, Mission Assurance and Security Services will ensure that a written survey is developed and distributed for completion by all IRS business units possessing one or more of the IRS critical assets. The results of the survey will be compiled and approved by IRS executives and will represent the updated candidate list of IRS critical assets to comply with Homeland Security Presidential Directive/HSPD-7 and ensure the protection of those assets.

IMPLEMENTATION DATE:

November 30, 2005

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance and Security Services

CORRECTIVE ACTION MONITORING PLAN:

The Emergency Management Program Office developed a detailed Action Plan that will be monitored monthly.

Attachment

Management Response to Draft Audit Report – More Management Attention Is Needed to Protect Critical Assets (Audit # 200520001)

RECOMMENDATION # 2: The Chief, Mission Assurance and Security Services should coordinate with all business units at least annually to confirm the IRS' list of critical assets is accurate and complete.

CORRECTIVE ACTION TO RECOMMENDATION #2:

We concur with the recommendation. The Chief, Mission Assurance and Security Services (MA&SS), once the IRS receives formal notification of national critical assets owned by the IRS from Treasury, will coordinate with all business units, at least annually, to confirm the IRS' list of critical assets is accurate and complete. Specifically, the process will include MA&SS issuing a memorandum no later than August 15, of each year, to all relevant IRS business units asking them to complete the survey mentioned in response to recommendation #1, no later than September 15. The results will be compiled and presented to the Chief of MA&SS for approval no later than October 1. The Chief, MA&SS, will endorse the results no later than October 15 of each year and submit to the Deputy Commissioner for Operations Support for final approval. This process will be repeated annually to ensure the appropriate coordination with all business units is accomplished to confirm the accuracy and completion of IRS' list of critical assets.

IMPLEMENTATION DATE:

November 30, 2006

RESPONSIBLE OFFICIAL:

Chief, Mission Assurance and Security Services

CORRECTIVE ACTION MONITORING PLAN:

The Emergency Management Program Office developed a detailed Action Plan that will be monitored quarterly.