TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made

September 2005

Reference Number: 2005-20-143

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 30, 2005

MEMORANDUM FOR CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

Pamela J Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made (Audit # 200520007)

This report presents the results of our review of the effectiveness of the Internal Revenue Service's (IRS) Computer Security Incident Response Center (CSIRC) at preventing, detecting, and responding to computer security incidents targeting IRS computers and data. As a part of its mission, the CSIRC provides assistance and guidance in incident response and provides a centralized approach to incident handling across the IRS enterprise.

Synopsis

The CSIRC is effective at preventing, detecting, and responding to computer security incidents. In particular, it:

- Manages entry points into the IRS computer architecture to ensure computer networks are secure against external intruders.
- Monitors entry points into the IRS computer architecture and major connections within the computer network to ensure suspicious activities are detected and reviewed.
- Reports and helps investigate computer and physical security incidents detected in the IRS.
- Identifies and refers Internet misuse by employees to appropriate authorities.

- Implements processes to rate security patches[1] related to software used by the IRS and inform system administrators of the vulnerabilities involved.
- Performs vulnerability scanning along with penetration tests of IRS computers.

We identified two areas where improvements could be made. First, the CSIRC has been operating under draft patch management procedures since November 2003. The lack of formal guidance can hinder the CSIRC and system administrators in the Modernization and Information Technology Systems organization in timely installing software patches on all appropriate computers. As an example, the draft guidance requires the CSIRC to conduct periodic follow-up to ensure patches are installed. We found the CSIRC did not regularly perform follow-up activities on patches. The installation of patches is critical in deterring unauthorized accesses and minimizing disruptions of service from internal and external threats to known weaknesses. The importance of timely installing patches can be illustrated when the IRS did not timely install patches on all computers that were vulnerable to the SASSER worm.[2] About 19 days after notification about the patch, the SASSER worm had spread throughout the IRS' internal computer network. The IRS believed it sustained several million dollars in lost productivity and potential losses of about $50 million in tax assessments and collections.

Second, problems identified during vulnerability scans and penetration tests were not formally provided to the business owners, and corrective actions were not documented in Plans of Action and Milestones (POA&M)[3] as required by the Federal Information Security Management Act (FISMA).[4] In addition, unless requested by the business unit, the CSIRC did not always follow up to ensure corrective actions were implemented. As a result, vulnerabilities may not be corrected or sufficiently reduced.

Recommendations

We recommended the Chief, Mission Assurance and Security Services, ensure the draft patch management guidance is finalized, ensure business units include security weaknesses identified from vulnerability scans and penetration tests in POA&Ms, and implement procedures to

[1] Vendors issue software security patches to correct flaws identified after their software has been released to the public.

[2] The SASSER worm exploited a flaw in the Local Security Authority Subservice System on Microsoft Windows computers and transferred additional exploit code to the computers. It also probed for other computers to infect. This worm rendered computers inoperable.

[3] A POA&M is a tool that identifies tasks that need to be accomplished and includes documenting resources required to accomplish the element of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The purpose of POA&Ms is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

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

formally share results with the head of the requesting office and routinely follow up to ensure corrective actions are taken and effective.

Response

The Chief, Mission Assurance and Security Services, concurred with our findings and recommendations, which will further assist the CSIRC in preventing, detecting, and responding to computer security incidents. The Mission Assurance and Security Services organization will finalize the patch management guidance manual, document vulnerability assessment and penetration test findings in a memorandum to the respective FISMA project office and the Executive in charge, ensure planned corrective actions to findings are reported through the FISMA process, and re-run scans and penetration tests to ensure vulnerabilities were effectively reduced. 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

Appendices

Background

The Internal Revenue Service's (IRS) Computer Security Incident Response Center (CSIRC) was designed to ensure the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify, contain, and eradicate cyber threats targeting IRS computers and data. The CSIRC provides a single clearinghouse of information and centralized pool of highly specialized expertise to detect and respond to computer attacks against the IRS.

The activities under the CSIRC program include:

- Firewall Administration and Management.
- Intrusion Detection.
- Incident Response, Recovery, and Reporting.
- Internet Misuse Monitoring.
- Security Patch Identification and Applicability to the IRS.
- Vulnerability Scanning and Penetration Testing.

This review was performed at the IRS' CSIRC National Headquarters in New Carrollton, Maryland, during the period December 2004 through May 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.

Results of Review

Firewall Administration and Management Were Effective

The primary function of firewalls is to keep a computer or computer network secure from intruders. Firewalls can be hardware or software and are typically installed at entry points into a network. They evaluate all traffic coming into and leaving the network based on configurations established by the organization. The effectiveness of firewalls depends on the placement, configurations, and configuration change management process of the firewalls.

The IRS installed firewalls at all connection points from the Internet and business partners[1] into the IRS' internal computer network. At the highest risk connections, a two-tier firewall scheme was implemented. The two-tier approach leverages the two firewall technologies[2] to more completely protect each connection point. This approach significantly reduces the likelihood of an improper access because a configuration error or security flaw on one of the firewalls is not likely to exist on the other firewall.

Overall, the configurations on the firewalls we reviewed were effective at protecting the IRS' internal computer network. We identified configuration errors where disallowed traffic could have been allowed to pass through the firewall. For example, one firewall erroneously allowed all external users to have full access to a portion of the IRS' internal computer network. However, the two-tier firewall approach prevented successful attacks because the second firewall did not contain the same configuration error. The CSIRC immediately corrected these weaknesses when we brought them to its attention.

Overall, the configurations on the firewalls we reviewed were effective at protecting the IRS' internal computer network.

In addition, the CSIRC has implemented a change management process for firewall configurations that is web based and implements all requirements from the Department of the Treasury security directives. Changes to the firewalls are installed when necessary by the

[1] Business partners refer to those organizations that need connectivity to do business with or for the IRS. Examples include financial institutions and other Federal Government agencies.

[2] The two firewall technologies are packet filtering and application firewalls. Packet-filtering firewalls review the source and destination addresses of the network traffic along with the type of traffic to a set of rules to decide whether the traffic should be allowed to proceed intact. Application firewalls stop all traffic coming to the firewall and repackage the traffic data for delivery on the other side while reviewing its contents. While this is more secure, it uses more resources of the firewall computer.

CSIRC staff and contractors and require approval by the CSIRC manager before implementation. Our review found this process is working as intended.

The IRS is moving the responsibility for maintaining firewalls from the CSIRC to the Information Technology Service Enterprise Networks organization.[3] This change is to be in place at the beginning of Fiscal Year 2006.

Intrusion Detection Systems Were Effective

Intrusion detection systems provide an organization the ability to monitor the activity of its computer network and look for suspicious or unauthorized actions from both external and internal threats. The Federal Information Security Management Act (FISMA)[4] specifically requires Federal Government agencies to develop procedures to detect, report, and respond to security computer incidents. Similar to the firewall architecture, an effective detection program depends on the placement, configuration, and maintenance of intrusion detection sensors. The sensors record traffic data, and the servers collect all data from the sensors and evaluate the traffic for patterns or characteristics of known attack scenarios.

The placement of sensors throughout the IRS' internal computer network was sufficient and effective. Sensors were deployed at perimeter connections of the computer network and at the major internal network connections at the campuses[5] and Computing Centers.[6] In addition, sensors were installed on many of the major servers throughout the IRS infrastructure. The CSIRC plans to add more sensors throughout the network as soon as funding is available, which will allow the CSIRC to more completely monitor traffic moving within the IRS campus networks.

The sensors we reviewed were well configured, maintained, and monitored by the CSIRC staff and contractors. The sensors were using up-to-date configurations to detect known cyber attacks and automatically sent alerts to the CSIRC staff for analysis as questionable incidents were detected. The CSIRC facility is staffed 24 hours per day, 7 days a week, using both contractors and employees.

Intrusion detection sensors were well configured, maintained, and monitored by the CSIRC staff 24 hours per day, 7 days a week.

[3] The mission of the Enterprise Networks organization is to positively satisfy IRS business units' requirements by providing all forms of electronic communications in the most efficient and effective manner and by managing the day-to-day operations of the telecommunications environment.

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

[5] Campuses are the data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.

[6] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

We performed our own scanning activities of a portion of the IRS architecture over a 2-week period. During that period, the sensors inside the IRS network detected and recorded our activities.

Incident Response, Recovery, and Reporting Were Effective

If a hacker, disgruntled employee, or contractor attempts an unauthorized access, or a virus enters the IRS internal computer network, the IRS must respond quickly. Once an incident has been detected, the CSIRC must determine the scope of the incident, determine how best to contain the damage, and develop plans to recover from the incident. The CSIRC is also required to report significant incidents to the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations and the Department of the Treasury CSIRC function.

As part of its incident response program, the CSIRC maintains an incident response database to track an incident from the time it is reported until it is closed. The database includes who reported the incident, the point of contact, notes on email and telephone contacts during the incident review, corrective actions that were taken and, if necessary, results of any follow-up tests.

The CSIRC followed procedures, which are based on guidance from the Department of the Treasury and the National Institute of Standards and Technology,[7] to effectively identify and respond to cyber and physical security incidents. In addition, it properly referred significant incidents to the TIGTA when necessary, assisted in the subsequent investigations, and properly reported results to the Department of the Treasury CSIRC function. Between January 1, 2004, and March 3, 2005, the CSIRC recorded 1,361 incidents in its database, which consisted of:

The CSIRC followed procedures to effectively identify and respond to cyber and physical security incidents.

- Violations of the IRS' personal use policies (512).[8]

[7] The National Institute of Standards and Technology, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

[8] The IRS' policy on limited personal use of Government Information Technology equipment/resources defines acceptable use of the Internet by IRS employees.

- Malicious code that turned out to be mainly worms, viruses, and phishing emails (413).[9]
- Questionable computer scans of the IRS infrastructure from both internal and external entities (264).
- Unauthorized access attempts (61).
- Theft of computer equipment or data (29).
- Miscellaneous incidents, such as denial of service attempts and noncompliance with security policies (82).

Internet Misuse Monitoring Was Effective

The Internet is an excellent research resource for employees to better perform their jobs. Providing access to the Internet for business purposes, however, has also created the opportunity for abusive Internet browsing habits. As a result, the IRS created a policy on limited personal use of electronic communications, which specifically states what an employee can and cannot do on the Internet. The IRS policy specifically prohibits:

- Accessing, creating, downloading, viewing, storing, copying, or transmitting sexually explicit material.
- Creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling or any other illegal activity.
- Using Federal Government equipment/resources for commercial purposes or in support of “for profit” activities or in support of other outside employment or business activity.

In June 2003, we issued a report on the IRS Internet policy and employee usage of the Internet.[10] This report stated that, although the IRS had an Internet usage policy that was comprehensive and widely distributed, a substantial number of IRS employees continued to access prohibited sites that put IRS computer systems at risk. During a 1-week period almost 6 months after the policy was implemented, over 1 million questionable accesses to web sites were made from approximately 19,000 computer addresses. These accesses were linked to seven categories of

[9] A virus is a piece of programming code usually disguised as something else that causes some unexpected and, for the victim, usually undesirable event and which is often designed so it is automatically spread to other computer users. A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Phishing is the illegal act of sending an email to a user under the false pretense of being a legitimate enterprise such as a bank or online retailer with the intent of having the user disclose his or her account number and/or password.

[10] *Inappropriate Personal Use of the Internet Jeopardizes the Security and Privacy of Taxpayer Data* (Reference Number 2003-20-133, dated June 2003).

sites specifically listed in the policy as inappropriate: sexually explicit web sites, personal email accounts, chat rooms, games, music, instant messaging, and sites from which programs were downloaded.

The current CSIRC Internet misuse monitoring program consists of two mechanisms to deter and detect employee Internet violations to the IRS' policy. First, the CSIRC uses commercial software that is designed to block certain Internet accesses from connecting to those web sites deemed inappropriate. Second, the CSIRC reviews Internet access log files to identify questionable Internet accesses that were not blocked by the commercial blocking software. If necessary, these sites are then added to the software's forbidden site list so they will be blocked in the future.

When access to a web site that violates the IRS policy is detected, the CSIRC determines if the access is by a user who is a "first-time violator." If so, and the access does not involve sexually explicit web sites or criminal activity, the user will be sent an email explaining the access violated the IRS policy and he or she should not attempt to access the web site again. For sexually explicit web sites and possible criminal activity, the user's Internet activity will be reviewed for the prior 3 months. If the access was isolated, the user is treated as a first-time violator and sent a courtesy email. Repeated attempts will result in referrals to appropriate authorities based on the severity of the violations.

In Fiscal Year 2004, the CSIRC made 53 referrals. Specifically, these consisted of 34 employees referred to the IRS Human Resources organization for administrative handling, 10 employees referred to the TIGTA for criminal investigation, and 9 contractors referred to the IRS Personnel Security and Investigations office.[11]

The CSIRC has developed effective procedures and practices to monitor and identify Internet misuse by IRS employees. Because strong controls and procedures exist, we limited our test to a 1-day sample of employee Internet use and determined that significant Internet misuse did not exist.

Security Patches Were Properly Identified and Evaluated for Applicability, but Follow-Up Is Needed to Ensure Patches Are Timely Installed

The CSIRC is responsible for providing warnings and intelligence information on vulnerabilities, threats, and incidents that affect IRS computers and data. A key component of these duties is to

[11] The mission of the Personnel Security and Investigations office, under the Mission Assurance and Security Services organization, is to ensure the employment or retention of employment in the IRS is consistent with the interests of national security, the efficiency of the Federal Government service, and the integrity of the tax system.

review security alerts from various industry and vendor sources and determine if related patches are applicable to the IRS. Vendors issue patches to fix flaws that become apparent after their software has been released to the public. These fixes may be to correct one of the features of the program or a security weakness not known at the time of the software's release. The installation of patches generally prevents these weaknesses from being exploited.

The CSIRC properly identified relevant security alerts and patches applicable to the IRS. To identify security alerts, the CSIRC regularly reviewed web sites maintained by vendors, the Federal Government, and security organizations. In addition, the CSIRC is included on mailing lists to receive current vulnerability announcements.

The CSIRC evaluated the risks affecting the IRS infrastructure and appropriately assigned severity levels for security patches based on the exploit, the software involved, and how widely the software was in use within the IRS. Patches were assigned one of four levels: red (critical risk), orange (high risk), yellow (medium risk), and green (low risk). Each level has its own installation requirements. For example, a critical patch must be installed within 72 hours.

After the CSIRC evaluates patches for applicability, patches are tested by the Modernization and Information Technology Services (MITS) organization to determine if the installation of the patch will adversely affect existing computer operations, such as stopping certain parts of programs from working. If no conflicts are identified, system administrators in the MITS organization are notified to install the patches.

While the CSIRC has effectively identified security alerts affecting the IRS, it currently does not follow up to ensure patches are installed. As a result, the IRS has no assurance that even critical patches are implemented timely and effectively.

The importance of verifying that patches have been installed timely and effectively can be illustrated by the SASSER worm[12] incident in 2004. On April 13, 2004, Microsoft Corporation notified certain customers, including the IRS, of a patch to correct the underlying problem exploited by the SASSER worm. On that date, the CSIRC issued a critical alert to the MITS organization. The MITS organization installed patches to its servers but did not install patches to all vulnerable computers, such as employee workstations. By May 1, 2004, the SASSER worm was quickly spreading across the Internet. By May 2, 2004, the SASSER worm had penetrated the IRS' internal computer network primarily because the patch had not been installed on all applicable computers. The IRS estimated the SASSER worm outbreak cost the various business units

The IRS estimated the SASSER worm potentially caused $50 million of tax assessments and collections to be lost.

[12] The SASSER worm exploited a flaw in the Local Security Authority Subservice System on Microsoft Windows computers and transferred additional exploit code to the computers. It also probed for other computers to infect. This worm rendered computers inoperable.

several million dollars in lost productivity from May 2 through May 10 due to the loss of connectivity caused by the SASSER worm. The IRS also estimated the SASSER worm potentially caused $50 million of tax assessments and collections to be lost during this time period.

Although the CSIRC has the responsibility for identifying security patches that should be installed, it currently has no authority to verify the patches are installed. The draft patch management guidance, dated November 2003, addresses this procedural weakness, as it contains a requirement stating the CSIRC will implement periodic widespread enterprise network and host vulnerability and security compliance scans to detect and report on deficiencies in the security patch management process. However, the draft procedures do not specifically state when these scans should be performed.

Recommendation

Recommendation 1: The Chief, Mission Assurance and Security Services, should ensure the draft patch management guidance is finalized and include a requirement for the CSIRC to conduct vulnerability scans across the IRS enterprise to ensure security patches have been timely installed. The procedures should require the CSIRC to conduct these scans within an appropriate time period based on the severity level of the security patch.

> ***Management's Response:*** The Director, CSIRC, will finalize the patch management guidance manual, which includes the requirement that the CSIRC will perform routine and ongoing security assessments to identify systems that have failed to implement patches or correct identified security vulnerabilities, to the extent possible.

Vulnerability Scanning and Penetration Testing Were Performed, but Follow-Up Was Not Always Conducted

The CSIRC conducts scans and penetration tests on IRS computers to find and reduce exploitable vulnerabilities. Scanning consists of using automated tools to review the computer resources on the internal network for known vulnerabilities. The automated tools usually target specific computers on the network with the full knowledge of the users. Penetration testing is similar to scanning but is usually done from an external perspective (e.g., a hacker attempting to attack the perimeter of an organization) without the full knowledge of the users.

The FISMA requires agencies to prepare Plans of Action and Milestones (POA&M)[13] for security weaknesses at the program and system levels. The POA&Ms are to be updated as new vulnerabilities are identified regardless of how the vulnerabilities were identified (e.g., an internal security review, business unit self-assessments, or an external security audit).

Scanning and penetration testing efforts were largely conducted on an ad hoc basis, when requested by the business units. During Calendar Year 2004, the CSIRC conducted 17 vulnerability scans and 2 penetration tests. We reviewed 13 of the scans and the 2 tests and determined the CSIRC had identified significant security weaknesses on the systems reviewed. Security weaknesses from these scans included 11 incidents involving authentication controls and 15 different types of vulnerabilities (316 incidents) that can be exploited to render the computer useless or to run malicious commands to take over control of the computer.

The CSIRC shared its results with the requesting office, although this was done on an informal basis. Generally, the person conducting the scan provided the results to the point of contact within the requesting office. There was no assurance that the head of the requesting office received the results of the scans or knew what the results were.

In addition, the CSIRC did not always follow up to determine if the vulnerabilities identified had been corrected. Follow-up reviews were conducted only when requested by the business units. CSIRC officials cited a lack of staffing as the main reason for not being able to follow up with requesting offices. We contacted several of the individuals who had requested the vulnerability scanning to determine the actions taken to address weaknesses identified. They indicated the results were disseminated down to the local managers for corrective actions, but the POA&Ms were not updated with the vulnerabilities identified by the CSIRC. The business units we contacted stated the problems were local and not national and, therefore, should not be added to the POA&Ms. We disagree with this rationale since the FISMA clearly requires all security weaknesses to be included in the POA&Ms for accountability and resolution purposes.

The CSIRC did not always follow up to determine if vulnerabilities identified had been corrected.

By not formally sharing results of tests with the heads of office, documenting results in POA&Ms, and following up, the IRS is not assured that identified vulnerabilities have been corrected or sufficiently mitigated.

[13] A POA&M is a tool that identifies tasks that need to be accomplished and includes documenting resources required to accomplish the element of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The purpose of POA&Ms is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Recommendations

The Chief, Mission Assurance and Security Services, should:

Recommendation 2: Require the CSIRC to formally provide scanning and penetration testing results to the business units in the form of a memorandum from the Office of the Chief, Mission Assurance and Security Services, to the Executive in charge of the requesting office.

> ***Management's Response:*** The Director, CSIRC, will document the findings from vulnerability assessments and penetration tests in a memorandum to the respective FISMA project office via the Executive in charge.

Recommendation 3: Ensure the business units document results and planned corrective actions from vulnerability scans and penetration tests in the POA&Ms, as required by the FISMA.

> ***Management's Response:*** The Director, CSIRC, will ensure all findings yielded from vulnerability assessments are documented and referred to the appropriate FISMA project office within the respective business units. The FISMA project office will accept and document the report findings for tracking corrective actions.

Recommendation 4: Require the CSIRC or another office to follow up on high-risk vulnerabilities identified from scanning and penetration testing to ensure vulnerabilities are corrected or properly reduced.

> ***Management's Response:*** The Chief, Mission Assurance and Security Services, will ensure the business units' FISMA project offices monitor, track, and report on findings from vulnerability assessments through closure. Upon notification from the FISMA project office of closure, the CSIRC will re-run scans and penetration tests to ensure vulnerabilities were effectively reduced.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of the Internal Revenue Service's (IRS) Computer Security Incident Response Center (CSIRC) at preventing, detecting, and responding to computer security incidents targeting IRS computers and data. To accomplish this objective, we:

I. Evaluated the security provided by the firewalls maintained by the CSIRC.

  A. Reviewed the configurations of a judgmental sample of 13 firewalls from the 67 firewalls installed on the IRS infrastructure. The sample selected was representative of the firewalls installed, the Computing Centers[1] where they were located, and the connection points being protected. A judgmental sample was used because we were not planning to project the results.

  B. Reviewed a random sample of 28 firewall configuration change management requests made between January 1, 2004, and February 28, 2005. During this period, we found 373 change management requests.

  C. Reviewed the process to accumulate and review the logs generated by the firewalls.

II. Evaluated the effectiveness of intrusion detection systems operations.

  A. Reviewed the configurations of a judgmental sample of 10 intrusion detection sensors from the 67 sensors installed on the IRS infrastructure. The sample selected was representative of the types of sensors installed, where they were located, and the connection points being protected. A judgmental sample was used because we were not planning to project the results.

  B. Reviewed how the intrusion detection sensors were deployed within the IRS.

  C. Reviewed all 68 intrusion detection change requests made from January 2004 through February 2005.

  D. Scanned the IRS network from April 20, 2005, to May 2, 2005, and verified with the CSIRC that this scanning activity was identified and logged.

[1] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

III. Evaluated the adequacy of the incident response and recovery actions.

A. Evaluated the processes and procedures for determining the nature of incidents, the containment of the incidents, remediation of the issues or causes, recovery or reconstitution of the systems for return to operational status, and education of personnel on lessons learned.

B. Identified 1,361 incidents reported on the CSIRC's incident response database between January 1, 2004, and March 3, 2005, and categorized the incidents by incident type.

C. Reviewed the reports from 12 incidents, including postmortem reports and reports to IRS management, the Department of the Treasury, and the Treasury Inspector General for Tax Administration (TIGTA).

IV. Evaluated the effectiveness of the security alert and patch process.

A. Evaluated the sources used to generate alerts, the process for determining their criticality, and the processes for issuing alerts and any follow-up regarding corrections based on the alerts.

B. Reviewed the 44 alerts for Microsoft Windows issued by the IRS during Fiscal Year 2004 and compared them to the related Microsoft Corporation security bulletins to ensure the alerts were coded correctly for their level of criticality.

V. Evaluated the effectiveness of the vulnerability scans and penetration tests conducted by the CSIRC.

A. Ascertained that 17 vulnerability scans and 2 penetration tests were performed during Calendar Year 2004.

B. Reviewed the results of 13 of the 17 vulnerability scans and the 2 penetration tests and determined what security vulnerabilities were identified, to whom the results were reported, and if follow-up scans were performed. Due to time constraints, we did not evaluate four of the scans.

VI. Evaluated the adequacy of the Internet usage log file reviews.

A. Reviewed the procedures for monitoring Internet usage by employees and contractors and for referring inappropriate Internet accesses to IRS management and the TIGTA.

B. Reviewed a random sample of 384 Internet firewall log entries from the 1,671,452 log entries for transactions of 5,000 bytes or more that went through the Martinsburg Computing Center Internet firewall on March 23, 2005. The sample was selected through interval selection.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
David Brown, Senior Auditor
William Lessa, Senior Auditor
Larry Reimer, Senior Auditor
Esther Wilson, Senior Auditor

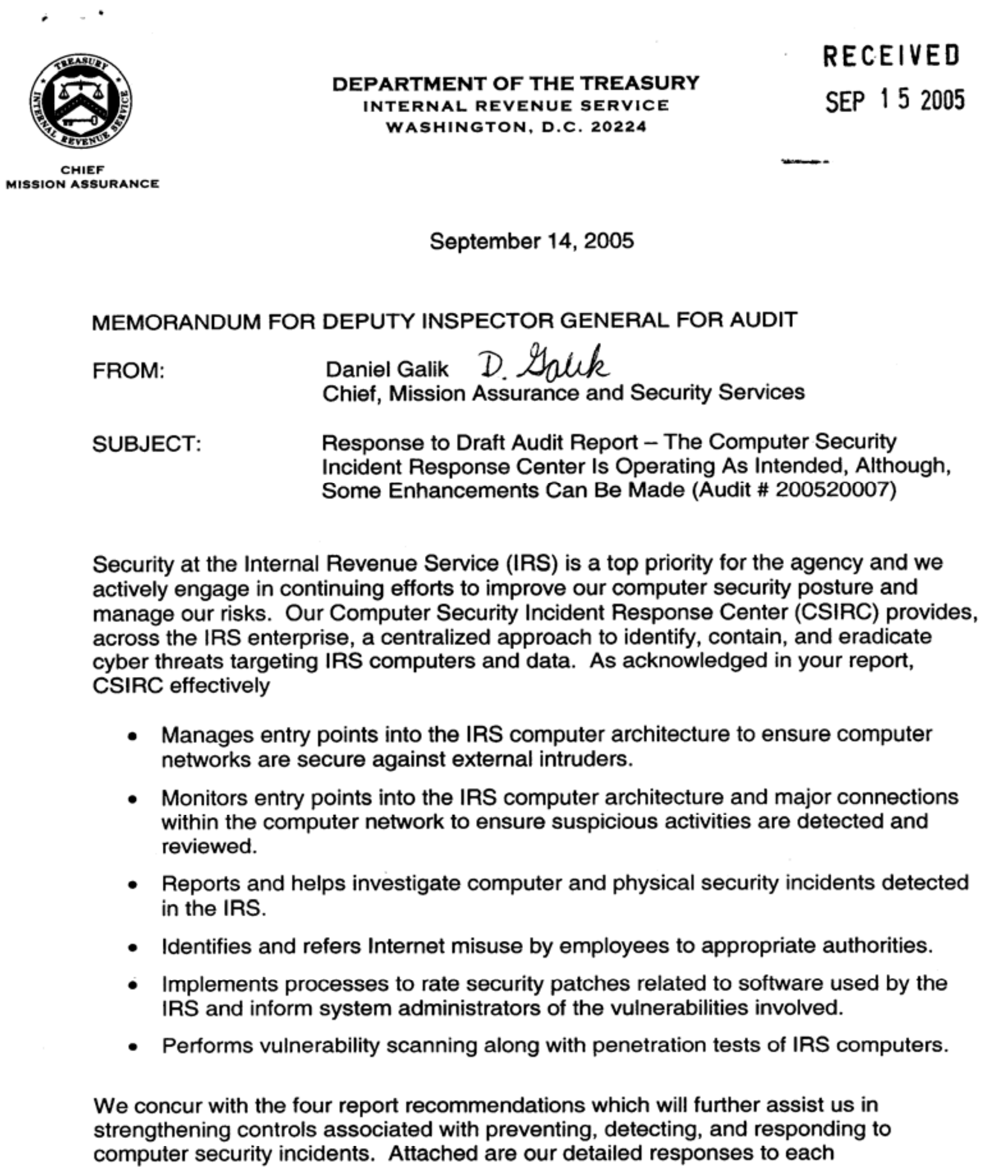
Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Director, Assurance Programs OS:MA:AP
Deputy Director, Information Technology Security Program Office OS:MA:AP
Chief, Computer Security Incident Response Center OS:MA:AP
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 and Security Services OS:MA

Appendix IV

Management's Response to the Draft Report



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

CHIEF
MISSION ASSURANCE

September 14, 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

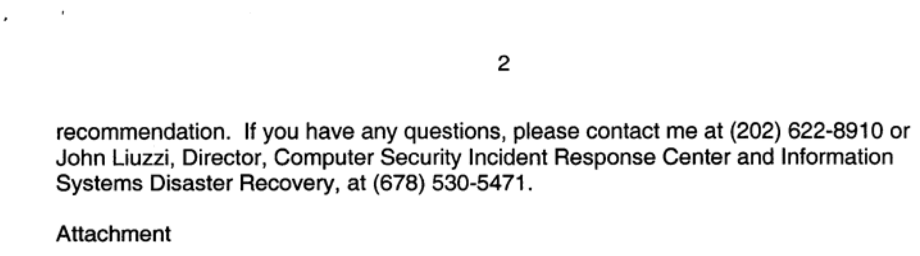
FROM: Daniel Galik D. Galik
Chief, Mission Assurance and Security Services

SUBJECT: Response to Draft Audit Report – The Computer Security Incident Response Center Is Operating As Intended, Although, Some Enhancements Can Be Made (Audit # 200520007)

Security at the Internal Revenue Service (IRS) is a top priority for the agency and we actively engage in continuing efforts to improve our computer security posture and manage our risks. Our Computer Security Incident Response Center (CSIRC) provides, across the IRS enterprise, a centralized approach to identify, contain, and eradicate cyber threats targeting IRS computers and data. As acknowledged in your report, CSIRC effectively

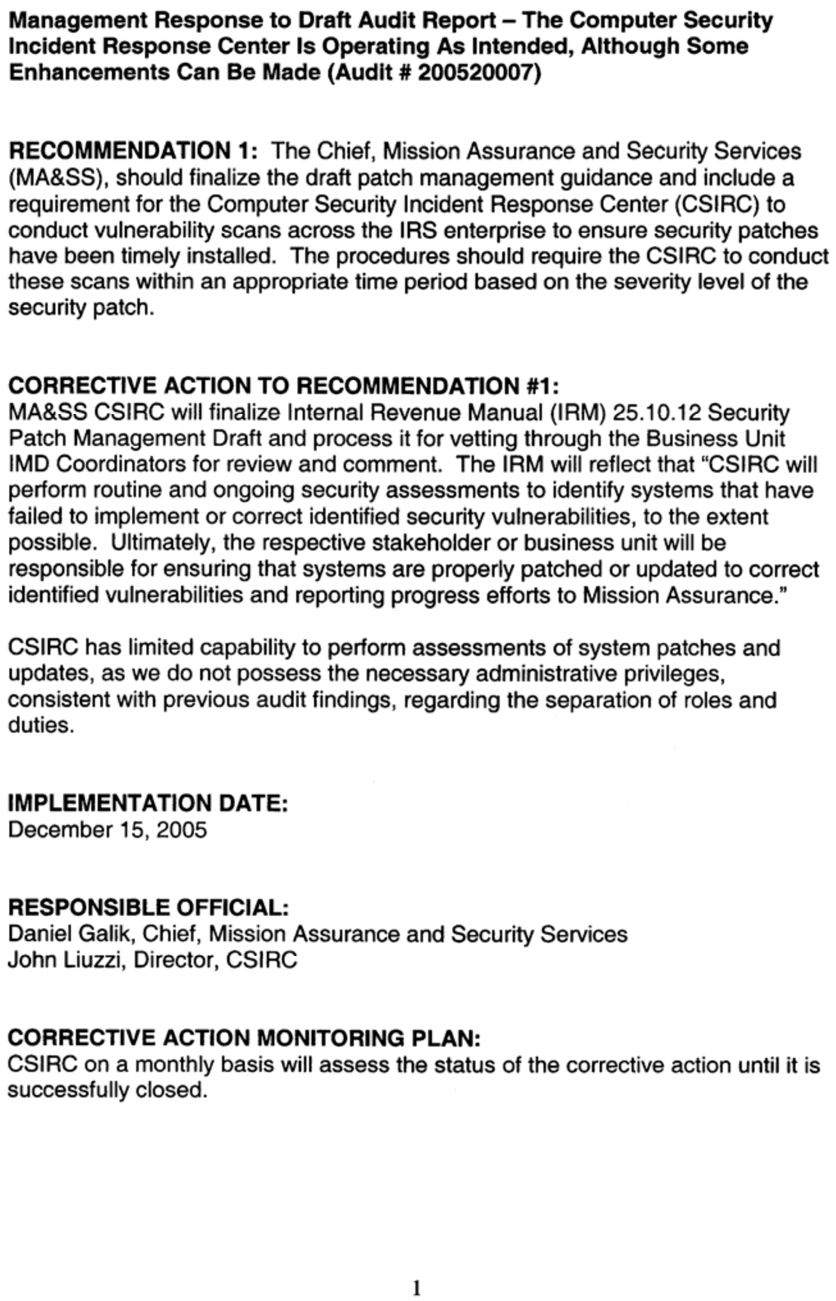
- Manages entry points into the IRS computer architecture to ensure computer networks are secure against external intruders.
- Monitors entry points into the IRS computer architecture and major connections within the computer network to ensure suspicious activities are detected and reviewed.
- Reports and helps investigate computer and physical security incidents detected in the IRS.
- Identifies and refers Internet misuse by employees to appropriate authorities.
- Implements processes to rate security patches related to software used by the IRS and inform system administrators of the vulnerabilities involved.
- Performs vulnerability scanning along with penetration tests of IRS computers.

We concur with the four report recommendations which will further assist us in strengthening controls associated with preventing, detecting, and responding to computer security incidents. Attached are our detailed responses to each



recommendation. If you have any questions, please contact me at (202) 622-8910 or John Liuzzi, Director, Computer Security Incident Response Center and Information Systems Disaster Recovery, at (678) 530-5471.

Attachment



Management Response to Draft Audit Report – The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made (Audit # 200520007)

RECOMMENDATION 1: The Chief, Mission Assurance and Security Services (MA&SS), should finalize the draft patch management guidance and include a requirement for the Computer Security Incident Response Center (CSIRC) to conduct vulnerability scans across the IRS enterprise to ensure security patches have been timely installed. The procedures should require the CSIRC to conduct these scans within an appropriate time period based on the severity level of the security patch.

CORRECTIVE ACTION TO RECOMMENDATION #1:
MA&SS CSIRC will finalize Internal Revenue Manual (IRM) 25.10.12 Security Patch Management Draft and process it for vetting through the Business Unit IMD Coordinators for review and comment. The IRM will reflect that "CSIRC will perform routine and ongoing security assessments to identify systems that have failed to implement or correct identified security vulnerabilities, to the extent possible. Ultimately, the respective stakeholder or business unit will be responsible for ensuring that systems are properly patched or updated to correct identified vulnerabilities and reporting progress efforts to Mission Assurance."

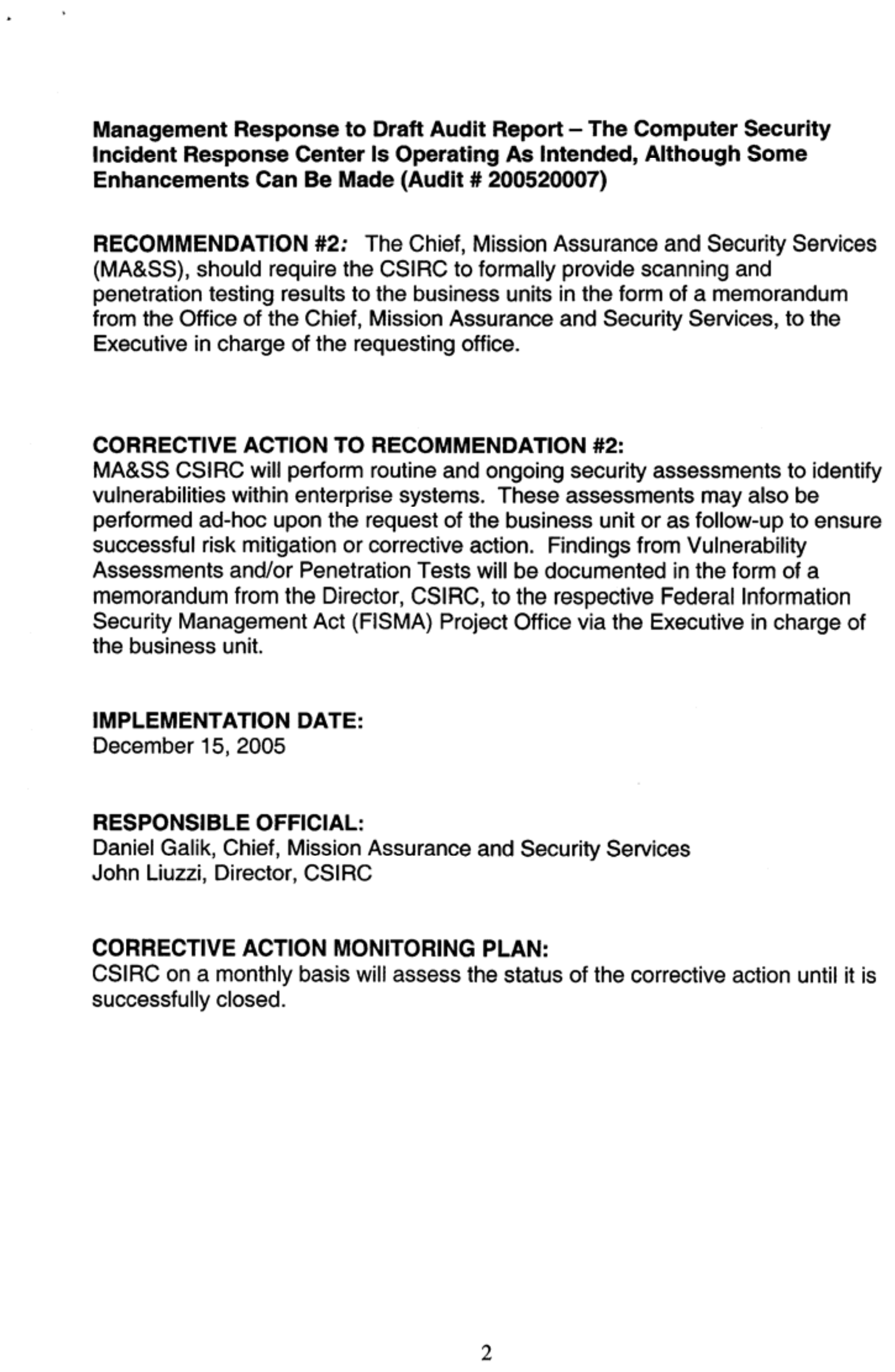
CSIRC has limited capability to perform assessments of system patches and updates, as we do not possess the necessary administrative privileges, consistent with previous audit findings, regarding the separation of roles and duties.

IMPLEMENTATION DATE:
December 15, 2005

RESPONSIBLE OFFICIAL:
Daniel Galik, Chief, Mission Assurance and Security Services
John Liuzzi, Director, CSIRC

CORRECTIVE ACTION MONITORING PLAN:
CSIRC on a monthly basis will assess the status of the corrective action until it is successfully closed.

1



Management Response to Draft Audit Report – The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made (Audit # 200520007)

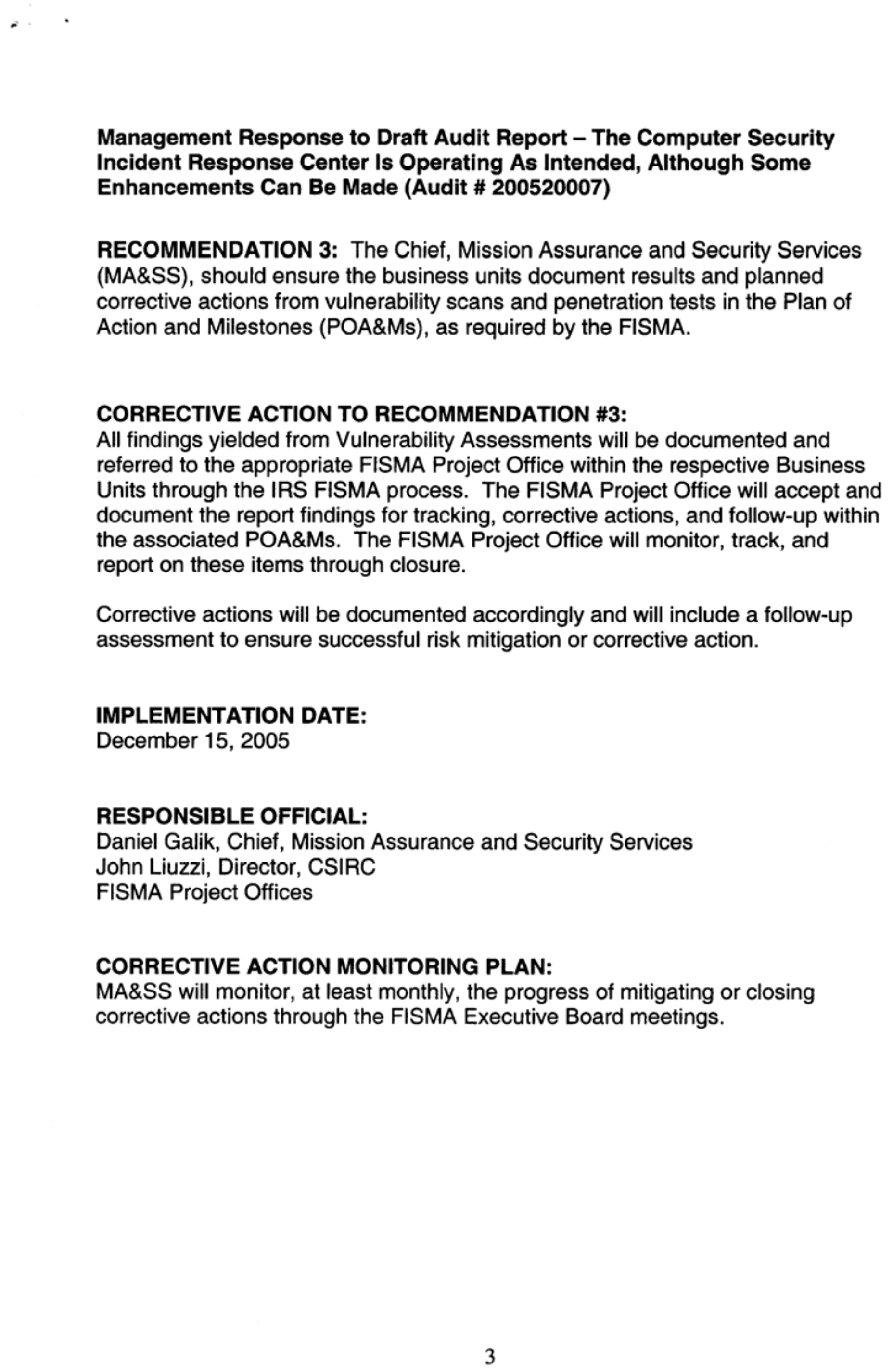
RECOMMENDATION #2*:* The Chief, Mission Assurance and Security Services (MA&SS), should require the CSIRC to formally provide scanning and penetration testing results to the business units in the form of a memorandum from the Office of the Chief, Mission Assurance and Security Services, to the Executive in charge of the requesting office.

CORRECTIVE ACTION TO RECOMMENDATION #2:
MA&SS CSIRC will perform routine and ongoing security assessments to identify vulnerabilities within enterprise systems. These assessments may also be performed ad-hoc upon the request of the business unit or as follow-up to ensure successful risk mitigation or corrective action. Findings from Vulnerability Assessments and/or Penetration Tests will be documented in the form of a memorandum from the Director, CSIRC, to the respective Federal Information Security Management Act (FISMA) Project Office via the Executive in charge of the business unit.

IMPLEMENTATION DATE:
December 15, 2005

RESPONSIBLE OFFICIAL:
Daniel Galik, Chief, Mission Assurance and Security Services
John Liuzzi, Director, CSIRC

CORRECTIVE ACTION MONITORING PLAN:
CSIRC on a monthly basis will assess the status of the corrective action until it is successfully closed.



Management Response to Draft Audit Report – The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made (Audit # 200520007)

RECOMMENDATION 3: The Chief, Mission Assurance and Security Services (MA&SS), should ensure the business units document results and planned corrective actions from vulnerability scans and penetration tests in the Plan of Action and Milestones (POA&Ms), as required by the FISMA.

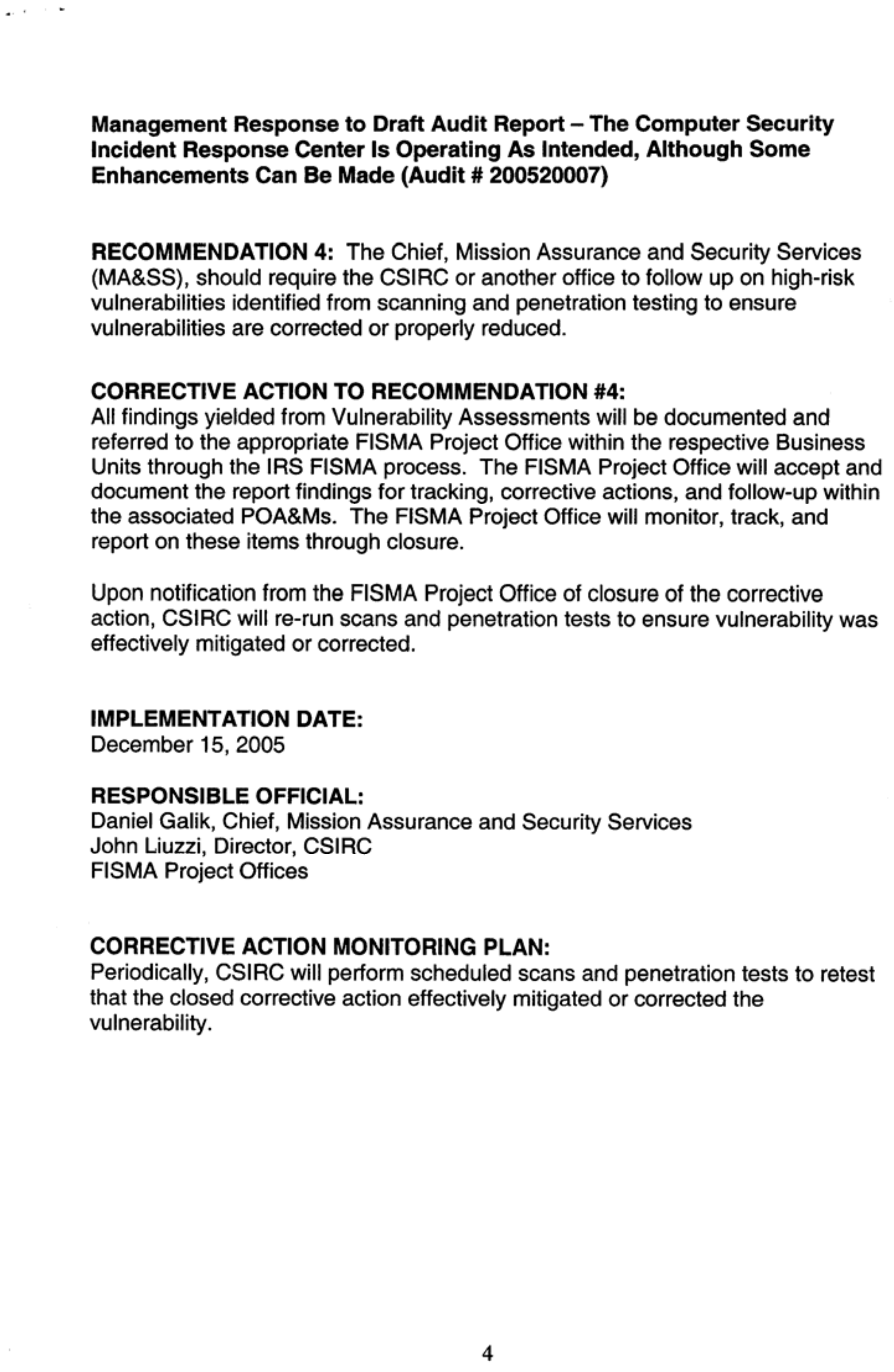
CORRECTIVE ACTION TO RECOMMENDATION #3:
All findings yielded from Vulnerability Assessments will be documented and referred to the appropriate FISMA Project Office within the respective Business Units through the IRS FISMA process. The FISMA Project Office will accept and document the report findings for tracking, corrective actions, and follow-up within the associated POA&Ms. The FISMA Project Office will monitor, track, and report on these items through closure.

Corrective actions will be documented accordingly and will include a follow-up assessment to ensure successful risk mitigation or corrective action.

IMPLEMENTATION DATE:
December 15, 2005

RESPONSIBLE OFFICIAL:
Daniel Galik, Chief, Mission Assurance and Security Services
John Liuzzi, Director, CSIRC
FISMA Project Offices

CORRECTIVE ACTION MONITORING PLAN:
MA&SS will monitor, at least monthly, the progress of mitigating or closing corrective actions through the FISMA Executive Board meetings.



Management Response to Draft Audit Report – The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made (Audit # 200520007)

RECOMMENDATION 4: The Chief, Mission Assurance and Security Services (MA&SS), should require the CSIRC or another office to follow up on high-risk vulnerabilities identified from scanning and penetration testing to ensure vulnerabilities are corrected or properly reduced.

CORRECTIVE ACTION TO RECOMMENDATION #4:
All findings yielded from Vulnerability Assessments will be documented and referred to the appropriate FISMA Project Office within the respective Business Units through the IRS FISMA process. The FISMA Project Office will accept and document the report findings for tracking, corrective actions, and follow-up within the associated POA&Ms. The FISMA Project Office will monitor, track, and report on these items through closure.

Upon notification from the FISMA Project Office of closure of the corrective action, CSIRC will re-run scans and penetration tests to ensure vulnerability was effectively mitigated or corrected.

IMPLEMENTATION DATE:
December 15, 2005

RESPONSIBLE OFFICIAL:
Daniel Galik, Chief, Mission Assurance and Security Services
John Liuzzi, Director, CSIRC
FISMA Project Offices

CORRECTIVE ACTION MONITORING PLAN:
Periodically, CSIRC will perform scheduled scans and penetration tests to retest that the closed corrective action effectively mitigated or corrected the vulnerability.