



*The Computer Security Incident Response
Center Is Effectively Performing Most of
Its Responsibilities, but Further
Improvements Are Needed*

March 12, 2012

Reference Number: 2012-20-019

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

Phone Number | 202-622-6500

E-mail Address | TIGTACommunications@tigta.treas.gov

Website | <http://www.tigta.gov>



HIGHLIGHTS

THE COMPUTER SECURITY INCIDENT RESPONSE CENTER IS EFFECTIVELY PERFORMING MOST OF ITS RESPONSIBILITIES, BUT FURTHER IMPROVEMENTS ARE NEEDED

Highlights

Final Report issued on March 12, 2012

Highlights of Reference Number: 2012-20-019 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Computer Security Incident Response Center (CSIRC) is responsible for monitoring the IRS network 24 hours a day year-round for cyberattacks and computer vulnerabilities and for responding to various computer security incidents such as the theft of a laptop computer. Taxpayers are impacted when IRS network disruptions prevent the IRS from performing vital taxpayer services such as processing tax returns, issuing refunds, and answering taxpayer inquiries.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to evaluate the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. TIGTA included this audit in its Fiscal Year 2011 Annual Audit Plan to help fulfill its statutory requirement to review the adequacy and security of IRS technology. This review addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

The CSIRC is effectively performing most of its responsibilities for preventing, detecting, and responding to computer security incidents. However, further improvements could be made. The CSIRC's host-based intrusion detection system is not monitoring 34 percent of IRS servers, which puts the IRS network and data at risk. In addition, the CSIRC is not reporting all computer security incidents to the Department of

the Treasury, as required. Finally, incident response policies, plans, and procedures are either nonexistent or are inaccurate and incomplete.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Assistant Chief Information Officer, Cybersecurity, direct the CSIRC to 1) develop its Cybersecurity Data Warehouse capability to correlate and reconcile active servers connected to the IRS network with servers monitored by the host-based intrusion detection system; 2) revise and expand the Memorandum of Understanding with the TIGTA Office of Investigations to ensure all reportable and relevant security incidents are shared with the CSIRC; 3) collaborate with the TIGTA Office of Investigations to create common identifiers to help the CSIRC reconcile its incident tracking system with the TIGTA Office of Investigations' incident system; 4) develop a standalone incident response policy or update the policy in the IRS's Internal Revenue Manual with current and complete information; 5) develop an incident response plan; and 6) develop, update, and formalize all critical standard operating procedures.

The IRS agreed with the recommendations and corrective actions are planned or in process for five of the six recommendations. Although the IRS agreed with the recommendation to correlate and reconcile active servers connected to the IRS network with servers monitored by the host-based intrusion detection system, its proposed corrective actions do not address the recommendation. Specifically, the IRS did not commit to implementing the controls we recommended.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 12, 2012

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM:

Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT:

Final Audit Report – The Computer Security Incident Response Center
Is Effectively Performing Most of Its Responsibilities, but Further
Improvements Are Needed (Audit # 201120012)

This report presents the results of our review of the Internal Revenue Service's (IRS) Computer Security Incident Response Center (CSIRC). The overall objective of this review was to evaluate the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. This audit was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2011 Annual Audit Plan and was part of our statutory requirement to annually review the adequacy and security of IRS technology. This review addresses the major management challenge of Security for Taxpayer Data and Employees.

Management's complete response to the draft report is included as Appendix VI.

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 Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.



*The Computer Security Incident Response Center Is Effectively
Performing Most of Its Responsibilities, but Further Improvements
Are Needed*

Table of Contents

| | |
|--|---------|
| Background | Page 1 |
| Results of Review | Page 3 |
| The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities and Has Sufficient Tools and Training to Accomplish Its Mission..... | Page 3 |
| The Computer Security Incident Response Center Does Not Administer and Monitor the Host-Based Intrusion Detection System for All Deployed Servers | Page 5 |
| <u>Recommendation 1:</u> | Page 7 |
| The Computer Security Incident Response Center Is Not Reporting All Computer Security Incidents to the Department of the Treasury | Page 8 |
| <u>Recommendations 2 and 3:</u> | Page 10 |
| The Computer Security Incident Response Center Has Not Developed Adequate Policies, Plans, and Procedures | Page 11 |
| <u>Recommendations 4 and 5:</u> | Page 12 |
| <u>Recommendation 6:</u> | Page 14 |
| Appendices | |
| Appendix I – Detailed Objective, Scope, and Methodology | Page 15 |
| Appendix II – Major Contributors to This Report | Page 18 |
| Appendix III – Report Distribution List | Page 19 |
| Appendix IV – Computer Security Incident Response Center Lifecycle for Managing Security Incidents..... | Page 20 |
| Appendix V – Glossary of Terms | Page 21 |
| Appendix VI – Management’s Response to the Draft Report | Page 25 |



*The Computer Security Incident Response Center Is Effectively
Performing Most of Its Responsibilities, but Further Improvements
Are Needed*

Abbreviations

| | |
|-------|---|
| CSIRC | Computer Security Incident Response Center |
| HIDS | Host-Based Intrusion Detection System |
| IRM | Internal Revenue Manual |
| IRS | Internal Revenue Service |
| MITS | Modernization and Information Technology Services |
| NIST | National Institute of Standards and Technology |
| TIGTA | Treasury Inspector General for Tax Administration |



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Background

Cybersecurity incidents are computer-related threats or attacks against an organization's computer systems.¹ The Government Accountability Office testified² to Congress that pervasive and sustained cyberattacks continue to pose a potentially devastating threat to the systems and operations of the Federal Government. Cyberthreats to Federal systems can come from a variety of sources, including criminals and foreign Nations, as well as hackers and disgruntled employees. These potential attackers have a variety of techniques at their disposal, which can enhance the reach and impact of their actions. For example, cyberattackers do not need to be physically close to the targets, their attacks can easily cross State and national borders, and cyberattackers can easily preserve their anonymity.

The U.S. Department of Energy Inspector General recently reported that exploitation of vulnerabilities could cause significant disruption to operations and increase the risk that sensitive data could be changed or stolen.³ The Department of Energy also said that recovery from cyberattacks can be very costly. For example, three recent cyberattacks at different locations cost the Department of Energy over \$2 million. In another example, a senior Department of Defense official reported that 24,000 electronic files were stolen in a cyberattack on the Pentagon in March 2011. The official said that the cyberexploitation perpetrated against the defense industry cuts across a wide swath of crucial military hardware, ranging from missile tracking systems to satellite navigation devices, and that any theft of design data or engineering information undermines the technological edge we hold over our potential adversaries.

Many cyberattacks can be traced back to the discovery of new security vulnerabilities identified by security researchers or vendors. Attackers will subsequently engineer exploit code and then launch that code against targets of interest. As a result, any significant delays in finding or fixing software with critical vulnerabilities provide ample opportunity for attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain.

To combat cyberthreats to its computer systems as well as computer-related security incidents such as loss or theft of laptop computers and employees' improper use of computers, the Internal Revenue Service (IRS) established the Computer Security Incident Response Center (CSIRC) in the Modernization and Information Technology Services (MITS) organization in February 2001.

¹ See Appendix V for a Glossary of Terms.

² Government Accountability Office, GAO-10-834T, *Continued Attention Is Needed to Protect Federal Information Systems From Evolving Threats* p. 1 (June 16, 2010).

³ U.S. Department of Energy, DOE/IG-0856, *The Department's Unclassified Cyber Security Program – 2011*, p. 8 (Oct. 2011).



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

The CSIRC's mission is to ensure the IRS has a team of capable "first responders" who are organized, trained, and equipped to identify and eradicate cyberthreats. One of the primary duties of the CSIRC is to perform 24-hour monitoring and support to IRS operations, seven days a week, 365 days a year.

Similar to what the Government Accountability Office found, the IRS has experienced an increase in the number of computer security incidents and threats. In Calendar Year 2010, the IRS detected 2,768 computer security incidents and threats, which represent a 22 percent increase over each of the past two years. The incidents and threats increase the risks to IRS operations, the administration of our Nation's tax system, and the privacy of taxpayers' sensitive information.

The IRS detected over 2,700 computer security incidents during Calendar Year 2010.

The CSIRC's 31 employees and 23 contractors are divided among three groups.

- Operations – This group monitors the network and reports security incidents. It also sends security notifications to the IRS business units and system owners.
- Technical Team – This group deploys, operates, and maintains the security tools and applications required to support the cyberincident response capabilities.
- Emerging Threats – This group helps plan for and respond to emerging threats and computer security incidents targeting information technology assets. It also identifies cyberthreats based on geographic region, country, group, and individual.

The CSIRC must also rely on employees in other MITS functions to perform critical security prevention and detection activities for the IRS. For example, the CSIRC must rely on the Enterprise Operations function to install host-based intrusion detection system (HIDS) software on servers so that the CSIRC may properly monitor all servers on the network. The Enterprise Operations function is also responsible for installing security patches on servers, which protect servers from the most up-to-date cyberthreats.

This review was performed at the offices of the MITS organization and its CSIRC in New Carrollton, Maryland. We performed the review during the period March through September 2011. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. 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 Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Results of Review

The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities and Has Sufficient Tools and Training to Accomplish Its Mission

The IRS has assigned most of the computer security incident-related services recommended by the National Institute for Standards and Technology (NIST) and the Carnegie Mellon Software Engineering Institute to the CSIRC. Other IRS functions are assigned some of the recommended services and responsibilities, which is common in large organizations according to the Carnegie Mellon Institute. For example, the Security Risk Management function in the MITS Cybersecurity office is responsible for conducting network scans that identify all missing security patches. The Security Control Testing and Evaluation group in this function conducts network vulnerability scanning at the operating system level, database scanning, and web scanning. We focused our review on the responsibilities performed by the CSIRC. These responsibilities fit into four overall categories. See Appendix IV for a chart of all functions and responsibilities assigned to the CSIRC.

- Detection – includes monitoring the network and the HIDS.
- Response – includes performing forensic analysis of security incidents and security event triage.
- Reporting – includes performing trending and analysis and reporting security incidents and events to IRS executives and the Department of the Treasury CSIRC (hereafter referred to as the Treasury CSIRC).
- Prevention – includes outreach and awareness activities to IRS business units and issuing security notifications.

Detection Responsibilities – The CSIRC is effectively performing its responsibilities to detect computer security incidents. For example, the CSIRC reviews and approves firewall change requests in accordance with IRS procedures. The CSIRC also maintains a Network-Based Intrusion Detection System that includes 27 sensors stationed throughout the IRS. Multiple sensors are placed in the IRS's three computing centers, and at least one server is located at each of the IRS's 10 campuses. CSIRC management has recognized the need for further expansion and plans to add additional sensors on the network, which will increase monitoring capability at the current sites, and expand coverage to additional office locations. The CSIRC also effectively reviews the Internet usage log files to identify violations of the IRS's Internet Usage Policy and appropriately notifies the Treasury Inspector General for Tax Administration (TIGTA) Office of



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Investigations or IRS Labor Relations when necessary. Lastly, CSIRC analysts block any malicious or inappropriate websites upon discovery.

Response Responsibilities – The CSIRC also effectively responds to computer security incidents. When addressing incidents, CSIRC employees adhere to the Department of the Treasury incident handling guidelines,⁴ which outline procedures for incident preparation, identification, containment, eradication, recovery, and follow-up. For example, when a laptop is lost or stolen, CSIRC analysts disable the employee’s grid card and ensure the employee changes his or her password. The analysts use a checklist that enumerates everything that must be completed when addressing this type of incident. Further, the CSIRC conducts post-mortems for significant events and develops corrective actions for lessons learned. For example, during the CSIRC’s response to the Conficker worm, the IRS had to remove thousands of computers from the network to contain the virus. The CSIRC recognized that the IRS helpdesk personnel needed assistance getting computers back online. To streamline this process, CSIRC analysts created a Probe and Response Guide to assist the helpdesk personnel with containing any contamination caused by the virus and restoring computers to the network. The CSIRC has implemented most of the corrective actions identified through its formal lessons-learned process, and those that remain outstanding require more complicated fixes that are still in progress, involving multiple organizations outside the CSIRC.

Prevention Responsibilities – The CSIRC effectively performs its prevention responsibilities. For example, the CSIRC timely notifies MITS’s Enterprise Operations and Security Risk Management functions when software patch notifications are received from vendors. Furthermore, the CSIRC has effective controls in place to ensure that security alerts, bulletins, and advisories are issued timely in order to help prevent computer security incidents. The CSIRC also performs outreach and awareness to IRS business units, with a presentation entitled *The Cyber Threat*. This awareness presentation includes common misconceptions about cyberthreats, the cost of inadequate security, key vulnerabilities, and the kinds of cyberthreats targeting the IRS. Lastly, the CSIRC coordinates with other MITS functions in the preparation and posting of informational security articles on the IRS’s Intranet to ensure widespread distribution.

Tools, Training, and Qualifications – The CSIRC also has sufficient tools and training to accomplish its mission. The CSIRC budget has more than doubled in the last three fiscal years, from \$11.6 million in 2009 to \$30.1 million in 2011. This increase in funds has allowed the CSIRC to procure additional equipment and analytical software to monitor and protect the IRS network. Equipment purchases alone increased from \$32,927 in 2009 to \$593,452 in 2010. The training records of CSIRC employees and contractors indicate they are provided adequate training to remain current in the rapidly changing field of cybersecurity. Training courses cover

⁴ Department of the Treasury, Treasury Directive Policy 85-01, *Department of the Treasury Incident Response Guidelines and Procedures* (Jan. 29, 2008).



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

topics such as security risk assessment and web security, software-specific certifications, and operating system administration. These resources allow the CSIRC to accomplish the services described above.

In addition to adequate tools and training, CSIRC employees and contractors have the required qualifications for their positions including a combination of appropriate experience, education, and specialized technical certifications to fulfill CSIRC roles. At the time of our review, CSIRC staff consisted of 31 Federal employees and 23 contractors who run the CSIRC 24 hours a day throughout the year, including weekends, at two different locations. CSIRC employees have advanced information technology degrees or extensive experience in computer and network security. Lastly, the IRS completed background checks for all CSIRC employees and contractors.

Although the CSIRC is effectively performing most of its prevention, detection, and responding responsibilities, we found some areas where improvements could be made to further protect the IRS network and data.

The Computer Security Incident Response Center Does Not Administer and Monitor the Host-Based Intrusion Detection System for All Deployed Servers

The CSIRC is required to detect security incidents and attacks against the IRS network by monitoring the HIDS software installed on servers. To accomplish this function, the CSIRC relies on system administrators to follow IRS procedures that require them to install and maintain HIDS software on all servers connected to the network. However, the CSIRC has not established an automated internal control to identify servers that are connected to the IRS network without the protection of a HIDS.

We found a significant number of servers deployed throughout the IRS that were operating without a HIDS installed. System administrators working in the MITS organization, which includes the Enterprise Operations, Enterprise Networks, and Applications Development functions, maintain most of these servers. However, this weakness also exists in other major IRS business units that maintain their own information technology infrastructure. Table 1 shows the number and percentage of active servers deployed on the IRS network that were operating without a functioning HIDS.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Table 1: Deployed IRS Servers Operating Without a HIDS

| Business Unit | Deployed Servers That Should Be Monitored by the CSIRC | Deployed Servers Operating Without a HIDS | Percent Not Monitored |
|------------------------------------|---|--|------------------------------|
| MITS | 6,799 | 1,898 | 28% |
| Criminal Investigation | 766 | 766 | 100% |
| Research, Analysis, and Statistics | 135 | 58 | 43% |
| Chief Counsel | 434 | 58 | 13% |
| Totals | 8,136 | 2,780 | 34% |

Source: TIGTA reconciliation of the IRS server database inventory and the HIDS monitoring system.

Included in the MITS numbers above, we also found HIDS software was not installed or functioning on 615 (29 percent) of the 2,147 servers that the IRS deployed in a virtualized environment.

Criminal Investigation servers are not protected by the HIDS. CSIRC officials are currently discussing with Criminal Investigation officials the possibility of allowing HIDS installation on the Criminal Investigation servers. For other functions, IRS officials provided several reasons why these servers were operating without the HIDS software.

- The servers were offline for maintenance on the day we conducted our test. However, the system administrators were unable to provide support for this explanation.
- The servers were retired, but the system administrators did not update the IRS asset management and inventory system. System administrators were also unable to provide support for this explanation.
- The servers were in “build” status and, therefore, were not required to have HIDS software installed. However, we found no HIDS exemption in IRS procedures for the “build” servers and believe these servers still pose risks if not monitored and protected while on the network.
- System administrators were unaware that the HIDS was not functioning on the servers.
- HIDS software was installed subsequent to our test or the HIDS is scheduled to be installed. CSIRC officials corroborated this last explanation by stating that after we forwarded identification data for the above servers to system administrators, the CSIRC’s



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

HIDS technical team noticed a significant increase in the number of servers actively monitored by the HIDS monitoring system.

A lack of coordination between the CSIRC and system administrators contributed to the significant number of servers operating without a HIDS. CSIRC officials told us their responsibility is to monitor the HIDS, and system administrators are responsible for installing and maintaining the HIDS. The CSIRC made no attempt to reconcile the active servers connected to the network with the servers the HIDS technical team monitors. However, CSIRC officials told us they are planning to enhance their Cybersecurity Data Warehouse to systemically collect and correlate active server data with data from the HIDS monitoring system. This enhancement would accomplish a reconciliation such as the one we performed and identify servers operating without a HIDS. Without adequate monitoring of IRS servers, the CSIRC may not timely detect malicious activity or cybersecurity incidents.

Recommendation

Recommendation 1: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to:

- a) Develop its Cybersecurity Data Warehouse capability to correlate and reconcile active servers connected to the IRS network with servers monitored by the HIDS.
- b) Report servers that are repeatedly found operating without a HIDS to the applicable system administrators for corrective action.

Management's Response: The IRS agreed with this recommendation. To develop the recommended HIDS correlation, reconciliation, and reporting processes, the Assistant Chief Information Officer, Cybersecurity, will 1) identify impacted IRS organizations; 2) identify applications and tools needed to provide information technology asset information, with their varying implementation dates, since the Cybersecurity Data Warehouse is not a repository of information technology asset information; and 3) initiate a stakeholder meeting to launch actions. The IRS will complete these actions by the end of Calendar Year 2012.

Office of Audit Comment: The IRS's proposed corrective actions do not address our recommendation. Specifically, the IRS did not include a commitment to implement the controls we recommended. After we issued the draft report, CSIRC officials informed us they intend to implement the controls but their dependence on another MITS function to develop an asset management system prevented the CSIRC from estimating an implementation date before the end of the calendar year. Without a control to identify and resolve servers operating without a HIDS, the IRS cannot monitor for malicious activity or cybersecurity incidents across its server environment.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

The Computer Security Incident Response Center Is Not Reporting All Computer Security Incidents to the Department of the Treasury

The Department of the Treasury requires⁵ the CSIRC to report the computer security incidents and events to the Treasury CSIRC for its analysis. Table 2 presents the incident category type and name, a description of the category, and the required reporting time period.

Table 2: Computer Security Incident and Event Categories

| CATEGORY | NAME | DESCRIPTION | REPORTING TIME PERIOD |
|----------|--|---|---|
| CAT 1 | Unauthorized Access/Physical Loss | An individual gains logical or physical access without permission to a Federal agency network, system, application, data, or other resource, including the physical loss of assets and Personally Identifiable Information. | Within one hour of discovery/detection. |
| CAT 2 | Denial of Service | An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the denial of service. | Within two hours of discovery/detection regardless of the mitigation status of the attack. |
| CAT 3 | Malicious Code | Successful installation of malicious software (e.g., virus, worm, spyware, bots, Trojan horse, or other code-based malicious entity) that is not quarantined and infects or affects an operating system or application. | Within one hour of discovery/detection if widespread across agency; otherwise, within 24 hours. |
| CAT 4 | Improper Usage | A person violates acceptable computing use policies. | Within one week of discovery/detection of the incident. |
| CAT 5 | Scans/Probes Attempted Access | Activity that seeks to access or identify a Federal agency computer, open ports, protocols, service, or any combination for later exploit. | Monthly or as activity is discovered. |
| CAT 6 | Investigation | Unconfirmed incidents under investigation that are potentially malicious or anomalous activity deemed to warrant further review. | No set time period. |

Source: Department of the Treasury Incident Reporting Guidelines and Procedures, Final Draft (May 15, 2011).

⁵ Treasury Directive TD P 85-01 Appendix G p. 13 (Jan. 29, 2008).



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

The CSIRC effectively reports the above security incidents and events when it is aware of them. However, in Calendar Year 2010, the TIGTA Office of Investigations detected 84 computer security incidents that were never forwarded to the CSIRC for reporting to the Treasury CSIRC. Sixty-five of these incidents were Internet and e-mail abuses (Category 4), 14 were misuse of Government computers or software violations not involving the Internet or e-mail (Category 4), and five were intrusion or sabotage incidents (Category 5).⁶ Since the CSIRC was not aware of these incidents, it could neither investigate nor report them to the Treasury CSIRC.

We reported this same weakness in 2009⁷ and noted the TIGTA Office of Investigations was sharing only the incidents categorized as Loss or Theft of Information Technology Assets, which omitted several reportable incident categories. At that time, we recommended the CSIRC collaborate with the TIGTA Office of Investigations to revise the Memorandum of Understanding between the two organizations.

Since we first reported this weakness, the CSIRC granted the TIGTA Office of Investigations full access to the CSIRC incident tracking system. However, the TIGTA Office of Investigations could not reciprocate due to its need to protect the confidentiality of sensitive investigative information in its own security incident tracking system. Therefore, the CSIRC still had a critical need to update the Memorandum of Understanding to define security incident referral criteria and ensure the TIGTA Office of Investigations is sharing all computer security incidents it detects during its ongoing IRS investigations and monitoring programs. However, the CSIRC did not coordinate with the TIGTA Office of Investigations to define and expand the referral criteria in the Memorandum of Understanding.

The Memorandum of Understanding was not updated because the CSIRC deferred this task to the Office of Privacy, Information Protection, and Data Security. However, that office stopped revising the Memorandum after determining its own incident tracking system, currently under development, would satisfy its needs. After the Office of Privacy, Information Protection, and Data Security determined it had no need for a revision to the Memorandum, CSIRC officials did not resume their work to revise the Memorandum.

In addition to not revising the Memorandum of Understanding to improve security incident sharing, an ineffective control in the CSIRC contributed to the CSIRC not reporting all incidents to the Treasury CSIRC. The CSIRC did not always reconcile its incident tracking system with the TIGTA Office of Investigations' tracking system to ensure the lone category of incidents that was shared, Loss or Theft of Information Technology Asset, was accounted for in the CSIRC's incident tracking system and reported to the Treasury CSIRC. Our reconciliation between the TIGTA Office of Investigations' system and the CSIRC's incident tracking system determined

⁶ At the end of our fieldwork, CSIRC officials told us they are no longer required to report Category 5 incidents to the Treasury CSIRC.

⁷ TIGTA, Ref. No. 2009-20-120, *Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices* (Aug. 2009).



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

the CSIRC did not account for 37 (12 percent) of 320 Loss or Theft of Information Technology Asset incidents that the TIGTA Office of Investigations maintained in its tracking system.

In response to our August 2009 report, CSIRC officials stated they were considering two corrective actions to improve their reconciliation process. One improvement was to develop common identifiers to help reconcile the CSIRC's incident tracking system with the TIGTA Office of Investigations' system. The second improvement was to designate the CSIRC as the central point of contact in order to reduce employee burden for making three separate contacts (manager, TIGTA Office of Investigations, and CSIRC) when a loss or theft incident occurs. However, the CSIRC did not implement either of these corrective actions that would have improved the reconciliation process.

Without an effective reconciliation process, the CSIRC does not have reasonable assurance it is fully meeting the Department of the Treasury's incident reporting requirements. In addition, the CSIRC's timely response to Loss or Theft of Information Technology Asset incidents is critical to prevent further loss of data and damage to IRS systems. Specifically, the CSIRC must determine whether the device contained Personally Identifiable Information or other sensitive data. In some cases, the CSIRC may need to remove the user's remote access account to the IRS network, disable network identification cards, or take other immediate action to protect the IRS network and data.

Recommendations

The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to:

Recommendation 2: Revise and expand the Memorandum of Understanding to require the TIGTA Office of Investigations to refer all reportable and relevant computer security incidents to the CSIRC except for those incidents that cannot be shared due to privacy or legal concerns.

Management's Response: The IRS agreed with this recommendation. Cybersecurity will revise and expand the Memorandum of Understanding to require the TIGTA Office of Investigations to refer all reportable and relevant computer security incidents to the CSIRC.

Recommendation 3: Collaborate with the TIGTA Office of Investigations to develop and use common identifiers to facilitate the reconciliation of the CSIRC's incident tracking system to the TIGTA Office of Investigations' tracking system.

Management's Response: The IRS agreed with this recommendation. Collaborative action is underway with the TIGTA Office of Investigations to develop and use common identifiers to facilitate reconciliation of CSIRC's incident tracking system with the TIGTA Office of Investigations' tracking system.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

The Computer Security Incident Response Center Has Not Developed Adequate Policies, Plans, and Procedures

The first step in establishing any program is the creation of policies and plans to implement these policies. The Department of the Treasury Incident Response Guidelines and Procedures⁸ require the IRS to implement the security requirements and controls outlined in the NIST Special Publication 800-53,⁹ which provides the elements that should be included in a bureau's incident response policy and plan. Furthermore, the Department of the Treasury also requires agencies to have "formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls." The CSIRC, however, has not prioritized its policies, plans, and procedures and has questioned whether following the NIST recommendations to develop this guidance would improve security.

The Internal Revenue Manual lacks key incident response policy details

The CSIRC has not maintained and updated its incident response policy. CSIRC officials told us that their incident response policy is included in the IRS's Internal Revenue Manual (IRM) and that the IRM provides adequate policy guidance. However, the IRM does not provide some of the key policy details recommended by the NIST and therefore required by the Department of the Treasury. The IRM lacks information about organizational structure and coordination among organizational entities; delineation of roles, responsibilities, and levels of authority; and compliance with the policy. The policy in the IRM is high level and does not contain detailed information, such as performance measures recommended by the NIST to help organizations improve their incident response capabilities.¹⁰ Furthermore, the IRM is out of date. For example, the new Office of Privacy, Information Protection, and Data Security assists CSIRC in reporting incidents involving Personally Identifiable Information to the Treasury CSIRC; however, the IRM does not provide information about these critical responsibilities. The IRM also states that the CSIRC has responsibility for conducting vulnerability assessments and network scanning but, as stated previously, the Security Risk Management function now performs these activities.

CSIRC officials told us their main priority is their mission to identify and eradicate cyberthreats 24 hours a day. However, we believe the IRS should follow the NIST recommendations, and establishing and maintaining a current and complete incident response policy will provide the program with clear direction and will assist the CSIRC with maturing its incident response capability.

⁸ Treasury Directive TD P 85-01 Appendix G p. 11 (Jan. 29, 2008).

⁹ NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations, Revision 3*, at pp. F-61 to F-65 (Aug. 2009).

¹⁰ NIST Special Publication 800-61, *Computer Security Incident Handling Guide* pp. 2-3 to 2-4 (Mar. 2008).



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Recommendation

Recommendation 4: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to develop a standalone incident response policy or update the IRM for currency and accuracy, including the NIST recommended elements that the Department of the Treasury policy requires.

Management's Response: The IRS agreed with this recommendation. The Assistant Chief Information Officer, Cybersecurity, is updating IRM 10.8.1 to include NIST guidance and Department of the Treasury requirements, as deemed appropriate.

The CSIRC has not developed an incident response plan

The CSIRC also has not developed a standalone incident response plan as recommended by the NIST and required by the Department of the Treasury. The NIST states,

...it is important that organizations have a formal, focused, and coordinated approach to responding to incidents. To effectively implement such a capability, an organization should have an incident response plan. The plan should provide a high-level approach for how the incident response capability fits into the overall organization and should lay out the resources and management support that is needed to effectively maintain and mature an incident response capability.

The CSIRC said its plan is contained within its standard operating procedures, but we determined the CSIRC's standard operating procedures lack any coherence or organization that would resemble an incident response plan and the standard operating procedures do not satisfy the NIST recommended elements for a plan. For example, the standard operating procedures do not describe the structure and organization of the incident response capability, nor do they provide a description of how this capability fits into the overall organization. The NIST also recommends that organizations review and approve their incident response plan. The CSIRC standard operating procedures have received no such review.

As stated previously, the CSIRC has not prioritized planning. We believe the IRS should comply with the Department of the Treasury requirement that bureaus implement the NIST recommended elements for incident response plans.

Recommendation

Recommendation 5: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to develop a standalone incident response plan that includes the elements recommended by the NIST.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Management's Response: The IRS agreed with this recommendation. CSIRC actions are underway to update standard operating procedures and formalize an incident response plan to include NIST guidance, as appropriate.

Standard operating procedures are not formalized and are outdated and incomplete

The CSIRC has not developed adequate standard operating procedures to guide its employees and contractors. The standard operating procedures are not formalized, and are neither current nor complete. The Department of the Treasury's "Minimum Standard Parameters" require standard operating procedures to be current and complete. The NIST also recommends standard operating procedures be tested for accuracy once developed. The CSIRC has not tested its standard operating procedures.

The CSIRC's standard operating procedures include a hodgepodge of electronic files, as follows: one basic incident response flow chart, 10 different templates that analysts may use to generate tickets in the CSIRC's tracking system, three sample e-mail formats, 29 screenshots of various online guidance ranging from a list of IRS Internet Protocol addresses to firewall administrator contacts, and one narrative standard operating procedure document. The sole narrative document contains disorganized sections that have not been updated since 2008. We also determined the single narrative document to be incomplete due to a lack of critical procedure guidance, such as how to monitor, manage, and address intrusion detection system information.

Other examples of missing guidance in the standard operating procedures include: 1) a procedure to explain how the CSIRC and the TIGTA Office of Investigations should work together to reconcile the cyberincidents in their separate tracking systems, 2) a procedure explaining how incidents must be referred to Labor Relations when Internet misuse is identified, and 3) guidance regarding the roles and responsibilities of the CSIRC and other organizations involved in maintaining the IRS network and data security.

CSIRC officials agreed with our assessment of their standard operating procedure documentation. CSIRC managers and analysts said they use an internal Wiki-page format to share information about threats and how to handle particular incidents. Operations analysts told us they use the Wiki-pages daily and that the information is easy to access and therefore effective for their purposes. However, the Wiki-pages do not satisfy the NIST recommendations and the Department of the Treasury requirements for formal, documented standard operating procedures. Any CSIRC employee or contractor can update the Wiki-pages. The procedural information on these pages does not undergo formal managerial review, and it can be inadvertently or maliciously deleted. Finally, the Wiki-pages are not always available to CSIRC analysts. When the site goes down or is otherwise unavailable, CSIRC analysts need the capability to access standard operating procedures so that they may continue to handle computer security incidents. At the beginning of our audit work, CSIRC officials told us they recently hired a technical writer to formalize the information on the Wiki-pages into standard operating procedure documents.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

As stated previously, planning and procedure documentation is not prioritized at the CSIRC. Without current and complete standard operating procedures that accurately describe how to handle computer security incidents, the CSIRC cannot be sure that employees and contractors have adequate information to appropriately address computer threats in order to protect the IRS network and data.

Recommendation

Recommendation 6: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to develop, update, and formalize all critical standard operating procedures and, once completed, test these procedures to ensure completeness and accuracy as recommended by the NIST.

Management's Response: The IRS agreed with this recommendation. Action is underway to develop, update, and formalize standard operating procedures, including coordination across the MITS organization.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of the IRS's CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. To accomplish our objective, we:

- I. Determined whether the CSIRC has established policies, plans, and procedures as recommended by the NIST and required by the Department of the Treasury by evaluating the IRM, CSIRC policy statements, incident response plans, and standard operating procedures.
- II. Determined whether the incident response services recommended by the NIST and the Carnegie Mellon Institute are performed by the CSIRC or other IRS organizations. We reviewed lists and descriptions of recommended services and interviewed officials in the CSIRC, Enterprise Operations function, and Security Risk Management function to delineate roles and responsibilities in order to ensure all recommended services are performed by the IRS.
- III. Determined whether the CSIRC is effectively performing its responsibilities for preventing, detecting, reporting, and responding to computer security incidents.
 - A. For preventing computer security incidents, we identified outreach programs the CSIRC performed during Fiscal Year 2010 and interviewed CSIRC officials to determine if the CSIRC performed any follow-up actions to evaluate the effectiveness of these programs. We also:
 1. Interviewed CSIRC officials to review the controls in place that ensure the CSIRC issues timely security alerts, bulletins, and advisories. We verified the CSIRC issued alerts and advisories timely to the appropriate IRS officials.
 2. Interviewed CSIRC officials to identify controls in place that ensure software patch notifications are distributed to the Enterprise Operations and Security Risk Management functions, and determined whether the CSIRC is distributing patches timely.
 - B. For detecting computer security incidents, we determined whether the CSIRC has an accurate server inventory and interviewed CSIRC officials to determine whether the IRS has developed procedures for notifying the CSIRC of changes that would affect its ability to detect unauthorized access. We also:



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

1. Evaluated the effectiveness of the Internet usage logs and determined whether the CSIRC reported Internet misuse and improper software downloads to appropriate IRS or TIGTA offices.
 2. Evaluated the effectiveness of the intrusion detection system operations. We reviewed the adequacy of Network-based Intrusion Detection System devices deployed throughout the IRS network. To evaluate the effectiveness of HIDS operations, we compared the Enterprise Server Database inventory of active deployed servers to the list of servers with HIDS software functioning properly in order to determine how many servers were operating without HIDS.
- C. For reporting computer security incidents, we evaluated the trending and analysis performed by the CSIRC and determined whether the CSIRC is reporting all security attacks and incidents to the Treasury CSIRC. We also:
1. Interviewed Office of Privacy, Information Protection, and Data Security, and TIGTA Office of Investigations officials to determine how computer security incidents are shared and tracked between organizations.
 2. Determined whether the CSIRC reconciles its incident tracking system with the TIGTA Office of Investigations' incident tracking system to ensure all known incidents are accounted for and reported. To accomplish this, we used all TIGTA Office of Investigations computer security incident records in Calendar Year 2010 and matched them against records in the CSIRC's incident tracking system.
- D. For responding to computer security incidents, we determined the CSIRC's process for handling incidents and determined whether the CSIRC conducted post-mortems, developed lessons learned, and performed recovery operations and other services. We interviewed CSIRC officials and operations analysts to determine whether they follow the Department of the Treasury incident handling guidelines. We also observed CSIRC operations analysts while they handled incidents and mitigated computer threats on site for three business days.
- IV. Determined whether a lack of resources, qualified staff, or training was affecting the CSIRC mission. We reviewed resumes, technical qualifications, and employment records for all CSIRC employees and contractors and verified background checks were conducted. We interviewed the MITS training coordinator about training received and reviewed training records for all CSIRC personnel. Finally, we reviewed the CSIRC's budget for the past three fiscal years.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: the NIST standards and related IRM guidelines and the processes followed by the CSIRC to protect the IRS network and data. We evaluated these controls by conducting interviews and meetings with management and staff, observing operations analysts on site, and reviewing documentation such as standard operating procedures.



*The Computer Security Incident Response Center Is Effectively
Performing Most of Its Responsibilities, but Further Improvements
Are Needed*

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
W. Allen Gray, Audit Manager
Charles O. Ekunwe, Lead Auditor
George L. Franklin, Senior Auditor
Bret Hunter, Senior Auditor
Jena R. Whitley, Senior Audit Evaluator
Monique Queen, Information Technology Specialist



*The Computer Security Incident Response Center Is Effectively
Performing Most of Its Responsibilities, but Further Improvements
Are Needed*

Appendix III

Report Distribution List

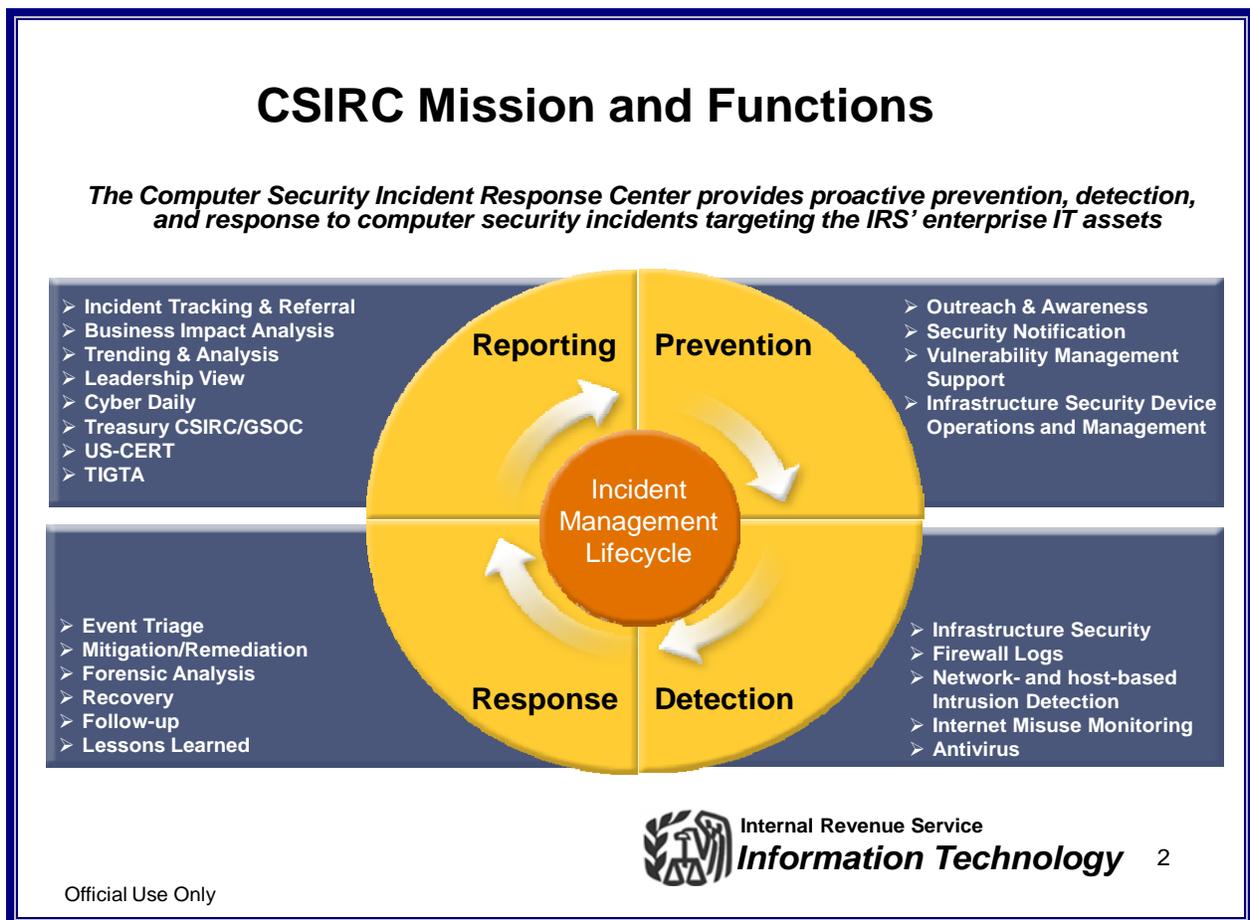
Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Chief Counsel CC
Chief, Criminal Investigation SE:CI
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Research, Analysis and Statistics RAS
Director, Office of Program Evaluation and Risk Analysis RAS:O
Director, Statistics of Income RAS:S
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM
Deputy Inspector General for Investigations IG:I



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Appendix IV

Computer Security Incident Response Center Lifecycle for Managing Security Incidents



Source: IRS CSIRC Overview and Status Presentation (September 2010), slide 2. GSOC is the acronym for Government Security Operations Center, IT is the acronym for Information Technology, and US-CERT is the acronym for United States Computer Emergency Readiness Team.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Appendix V

Glossary of Terms

| Term | Definition |
|--|--|
| Campus | 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. |
| Carnegie Mellon Software Engineering Institute | A Federally funded research and development center operated by Carnegie Mellon University and sponsored by the Department of Defense. |
| Conficker Worm | A computer worm targeting operating systems that was first detected in October 2008. It used flaws in software to propagate and was unusually difficult to counter because of its combined use of many advanced malware techniques. |
| Cyber | Cyber is often used for “electronic” or “computer-related.” |
| Exploit Code | A piece of software or sequence of commands that takes advantage of a bug, glitch, or vulnerability in order to cause unintended behavior on computer software or hardware. Exploit code frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial-of-service attack. |
| Grid Card | One component of the IRS’s two-factor authentication process to validate remote users on the network. |
| Host-Based Intrusion Detection System | A host-based intrusion detection system is a type of intrusion detection system that monitors and analyzes the computing system as well as (in some cases) the network packets on its network interfaces. |



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

| Term | Definition |
|----------------------------|---|
| Incident | An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. |
| Incident Handling | The mitigation of violations of security policies and recommended practices. |
| Incident Response Plan | The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyberattacks against an organization's information system(s). |
| Information Security | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. |
| Information Technology | Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. |
| Internet Protocol | The Internet Protocol is the principal communications protocol used for relaying packets of information across the Internet. Responsible for routing packets across network boundaries, it is the primary protocol that establishes the Internet. |
| Intrusion Detection System | Provides an organization the ability to monitor activity on its computer network and look for suspicious or unauthorized actions from both external and internal threats. |



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

| Term | Definition |
|--|--|
| Malware | Malicious code, software, or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. |
| National Institute of Standards and Technology | The NIST, 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. |
| Network-Based Intrusion Detection System | Devices that are appliance-based components residing on specific network environments to monitor traffic originating from or destined for protected segments of the network. |
| Patch | Software vendors issue patches to fix flaws that become apparent after their software has been released to the public. |
| Personally Identifiable Information | Personally Identifiable Information includes the personal information of taxpayers, employees, contractors, and visitors to the IRS. Examples include: name, home address, Social Security Number, home telephone number, biometric data, and other numbers and information that alone or in combination with other data can identify an individual. |
| Risk | The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals that results from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. |
| Server | A physical computer dedicated to running one or more services as a host to serve the needs of users of other computers on the network. |
| System | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people. |



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

| Term | Definition |
|----------------------|--|
| System Administrator | A person who manages the technical aspects of a system. |
| Threat | Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service. Also, the potential for a threat-source to successfully exploit an information system vulnerability. |
| Virus | 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 to automatically spread to other computer users. |
| Vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. |
| Wiki-Page | Website allowing creation and editing of any number of interlinked web pages used collaboratively by multiple users. |



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Appendix VI

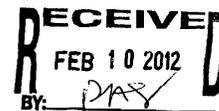
Management's Response to the Draft Report



CHIEF TECHNOLOGY OFFICER

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

FEB 7 2012



MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland *Terence V. Milholland*
Chief Technology Officer

SUBJECT: Draft Audit Report – The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed - (Audit # 201120012) (e-trak #2012-28058)

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss earlier draft report observations. We appreciate that the report acknowledged that the Internal Revenue Service's (IRS's) Computer Security Incident Response Center (CSIRC) is effectively performing most of its responsibilities to prevent, detect, and respond to cyber threats against IRS computer systems and data. We also thank you for acknowledging that CSIRC has sufficient tools and training to accomplish its mission.

The IRS's Modernization and Information Technology Services organization is committed to continuously improving its security posture, and your report recommendations will further improve our security program. We concur with the six report recommendations. The attachment to this memo details our planned corrective actions to the recommendations.

If you have any questions, please contact me at (202) 622-6800 or David W. Stender, Associate Chief Information Officer for Cybersecurity, at (202) 622-8910.

Attachment



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Draft Audit Report –The Computer Security Incident Response Center (CSIRC) Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed
(Audit # 201120012) e-trak # 2012-28058

RECOMMENDATION #1 The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to:

- a) Develop its Cybersecurity Data Warehouse capability to correlate and reconcile active servers connected to the IRS network with servers monitored by the HIDS.
- b) Report servers that are repeatedly found operating without a HIDS to the applicable system administrators for corrective action.

CORRECTIVE ACTION #1: We concur with the recommendation. To develop the recommended HIDS correlation, reconciliation and reporting processes, the ACIO Cybersecurity will:

- Identify impacted IRS organizations;
- Identify IRS applications and tools needed to provide IT asset information, with their varying implementation dates, since the Cybersecurity Data Warehouse is not a repository of IT asset information; and
- Initiate stakeholder meeting to launch actions.

IMPLEMENTATION DATE: 12/31/2012

RESPONSIBLE OFFICIAL: ACIO Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to revise and expand the Memorandum of Understanding (MOU) to require the TIGTA Office of Investigations to refer all reportable and relevant computer security incidents to the CSIRC except for those incidents that cannot be shared due to privacy or legal concerns.

CORRECTIVE ACTION #2: The IRS concurs with the recommendation. Cybersecurity will revise and expand the MOU to require TIGTA Office of Investigations to refer all reportable and relevant computer security incidents to CSIRC.

IMPLEMENTATION DATE: 12/31/2012

RESPONSIBLE OFFICIAL: ACIO Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Draft Audit Report –The Computer Security Incident Response Center (CSIRC) Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed
(Audit # 201120012) e-trak # 2012-28058

RECOMMENDATION #3: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to collaborate with the TIGTA Office of Investigations to develop and use common identifiers to facilitate the reconciliation of the CSIRC’s incident tracking system to the TIGTA Office of Investigations’ tracking system.

CORRECTIVE ACTION #3: The IRS concurs with the recommendation. Collaborative action with TIGTA Office of Investigations to develop and use common identifiers to facilitate reconciliation of CSIRC’s incident tracking system with TIGTA Office of Investigation’s tracking are underway, and scheduled to be completed calendar year ending 2012.

IMPLEMENTATION DATE: 12/31/2012

RESPONSIBLE OFFICIAL: ACIO Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to develop a standalone incident response policy or update the IRM for currency and accuracy, including the NIST recommended elements that the Department of the Treasury policy requires.

CORRECTIVE ACTION #4: The IRS concurs with the recommendation. The ACIO Cybersecurity is updating IRM 10.8.1 to include NIST guidance and Treasury requirements, as deemed appropriate.

IMPLEMENTATION DATE: 12/31/2012

RESPONSIBLE OFFICIAL: ACIO Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #5: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to develop a standalone incident response plan that includes the elements recommended by the NIST.



The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed

Draft Audit Report –The Computer Security Incident Response Center (CSIRC) Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed
(Audit # 201120012) e-trak # 2012-28058

CORRECTIVE ACTION #5: CSIRC actions are underway to update standard operating procedures and formalize an incident response plan to include NIST guidance, as appropriate. The scheduled completion is calendar year ending 2012.

IMPLEMENTATION DATE: 12/31/2012

RESPONSIBLE OFFICIAL: ACIO Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #6: The Assistant Chief Information Officer, Cybersecurity, should direct the CSIRC to develop, update, and formalize all critical standard operating procedures and, once completed, test these procedures to ensure completeness and accuracy as recommended by the NIST.

CORRECTIVE ACTION #6: The IRS concurs with the recommendation. Action to develop, update and formalize standard operating procedures, including coordination across Modernization and Information Technology Services is underway, and to be completed by calendar year ending 2012.

IMPLEMENTATION DATE: 12/31/2012

RESPONSIBLE OFFICIAL: ACIO Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.