TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Full Compliance With Trusted Internet Connection Requirements Is Progressing; However, Improvements Would Strengthen Security

September 17, 2013

Reference Number: 2013-20-107

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.treasury.gov/tigta

FULL COMPLIANCE WITH TRUSTED INTERNET CONNECTION REQUIREMENTS IS PROGRESSING; HOWEVER, IMPROVEMENTS WOULD STRENGTHEN SECURITY

Highlights

Final Report issued on September 17, 2013

Highlights of Reference Number: 2013-20-107 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Trusted Internet Connection (TIC) initiative is one of the Administration's three priorities to improve cybersecurity and the security of Federal information systems. The TIC initiative aims to improve agencies' security posture and incident response capabilities through enhanced monitoring and situational awareness of all external network connections. The IRS has progressed steadily towards implementing TIC requirements; however, additional improvements could strengthen the security posture of its TICs. Security weaknesses within these TICs could expose taxpayer data to unauthorized access or loss.

WHY TIGTA DID THE AUDIT

This audit was included in our Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The objective of this audit was to evaluate the IRS's three TICs to ensure that the connections comply with Department of Homeland Security requirements. The Administration expects Federal agencies to achieve 100 percent compliance with TIC requirements by Fiscal Year 2014.

WHAT TIGTA FOUND

Although the IRS has made good progress implementing the TIC requirements, our review revealed areas where improvements could strengthen the security posture of the TICs. For example, the IRS was not logging administrative activity on TIC equipment, had not completed actions to fully implement TIC requirements for a Data Loss Prevention program, did not have sufficient staff with the required security clearance and proper locations for handling classified information, and was not regularly scanning TIC equipment to ensure timely discovery and mitigation of vulnerabilities or misconfigurations.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure that the IRS: 1) implements the capture and review of administrator activity on TIC devices; 2) fully implements the selected tool for the Data Loss Prevention program upon successful testing; 3) obtains Top Secret Sensitive Compartmented Information clearances for IRS operational employees who can receive and react to classified information on a 24/7 basis; 4) completes implementation of proper locations for handling classified information at TIC locations; 5) implements vulnerability and configuration management scanning on TIC equipment and mitigates reported findings; and 6) updates all TIC equipment to the most current operating systems approved for use within the IRS.

The IRS agreed with all of our recommendations and has planned appropriate corrective actions to address them. The IRS plans to implement audit logging and review administrator activity on TIC devices. The IRS also plans to fully implement TIC requirements related to Data Loss Prevention, obtain security clearances for operational employees, and complete implementation of proper locations for handling classified information at TIC locations. In addition, the IRS plans to implement vulnerability scanning on TIC equipment and update all TIC equipment to the most current operating systems.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 17, 2013

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Full Compliance With Trusted Internet Connection Requirements Is Progressing; However, Improvements Would Strengthen Security (Audit # 201320005)

This report presents the results of our review of the Internal Revenue Service's three Internet connections to ensure compliance with the Department of Homeland Security requirements for Trusted Internet Connections. This review is part of the Treasury Inspector General for Tax Administration's Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Abbreviations

DHS	Department of Homeland Security
DLP	Data Loss Prevention
IRS	Internal Revenue Service
OMB	Office of Management and Budget
SCIF	Sensitive Compartmented Information Facility
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Response Team

Background

In November 2007, the Office of Management and Budget (OMB) issued Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*, which introduced the TIC initiative, one of the Administration's three priorities[1] for improving cybersecurity and the security of Federal information systems. The primary goals of the TIC initiative are (1) to consolidate and secure Federal agency external connections using a common set of security controls and (2) to improve the Federal Government's incident response capability. To achieve these goals, the initiative has the following objectives:

The TIC initiative is an Administration priority for improving the security of Federal information systems.

- Reduce and consolidate external connections, including connections to the Internet, across the Federal Government.
- Define and maintain baseline security capabilities at TIC access points.
- Establish a compliance program to monitor agency adherence to TIC policy.

The Administration expects executive branch departments and agencies to achieve 100 percent compliance with TIC requirements by the end of Fiscal Year[2] 2014. In Memorandum M-08-27,[3] the OMB stated that to be considered compliant with the TIC initiative, Federal agencies that implement TICs must:

- Comply with the capabilities published by the OMB as part of the TIC initiative.[4]
- Continue the reduction and consolidation of external network connections.
- Participate in the National Cyber Protection System[5] program.

[1] The other two are continuous monitoring of Federal information systems and strong authentication with Homeland Security Presidential Directive 12–compliant credentials for logical access control.

[2] A 12-consecutive-month period ending on the last day of any month. The Federal Government's fiscal year begins on October 1 and ends on September 30.

[3] OMB M-08-27, *Guidance for Trusted Internet Connection Compliance* (Sept. 30, 2008), provides additional guidance and clarification to Federal departments and agencies on compliance with the TIC initiative requirements.

[4] The Department of Homeland Security, in collaboration with Federal agencies, developed the TIC Reference Architecture v2.0, which introduces new capabilities and clarifies existing mandatory critical capabilities. In addition to mandatory critical capabilities, the TIC Reference Architecture v2.0 includes recommended capabilities based on evolving technologies and threats.

[5] The National Cyber Protection System (operationally known as Einstein) is a Governmentwide intrusion detection system deployed at TIC access points.

The Department of Homeland Security (DHS) has been tasked with managing and overseeing the OMB's TIC initiative for the Federal Government and ensuring that Federal agencies reduce their total number of external Internet connections and consolidate them through approved TIC access points.[6] The DHS Federal Network Resilience Division's Cybersecurity Assurance Branch annually assesses the state of operational readiness and cybersecurity risk of unclassified networks and systems across the Federal civilian executive branch. The Cybersecurity Assurance Branch is responsible for coordinating annual Cybersecurity Capability Validations[7] using an objective, repeatable, and consistent validation assessment method to measure the degree of adherence to the TIC initiative and OMB-published Federal cybersecurity requirements.

The DHS conducted its most recent annual Cybersecurity Capability Validations on the Department of the Treasury's various TICs in February 2013. The Department of the Treasury has implemented seven TICs, three of which were implemented by the Internal Revenue Service (IRS) at its computing centers in Detroit, Michigan; Memphis, Tennessee; and Martinsburg, West Virginia. During its 2013 review, the DHS reported that the Department of the Treasury's composite score for meeting TIC technological compliance was 92 percent, that it had consolidated 64 percent of its connections, and that it had consolidated 81 percent of its total external traffic flow through an approved TIC access point.

This review was performed with information obtained from the IRS Information Technology organization located in New Carrollton, Maryland; Detroit, Michigan; Memphis, Tennessee; and Martinsburg, West Virginia, during the period December 2012 through July 2013. 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 that 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.

[6] As a follow-up, OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security* (July 6, 2010), further defined the DHS's responsibility, in coordination with the OMB, to certify and enforce agency implementation of network security operational standards and best practices and to ensure that agencies comply with Federal standards and policies.

[7] In 2009-2010, the DHS's Federal Network Resilience Division launched the TIC Cybersecurity Capability Validations to assess and report agency compliance with OMB-directed guidance and criteria.

Results of Review

Full Compliance With Trusted Internet Connection Requirements Is Progressing

Agencies that implement TICs must ensure that each TIC meets the security and technological capabilities specified in the TIC Reference Architecture v2.0 that was issued by the DHS. The IRS has progressed steadily towards full compliance with TIC Reference Architecture v2.0 requirements in its three TICs, which are located at the IRS computing centers in Detroit, Michigan; Memphis, Tennessee; and Martinsburg, West Virginia. In February 2013, the DHS conducted a Cybersecurity Capability Validation assessment of two of the IRS TICs, located at Memphis, Tennessee, and Martinsburg, West Virginia, and reported that each met 68 (92 percent) of the 74 capabilities required. The TIC capabilities that the IRS had not met related to requirements for:

- Multi-factor authentication for administrative access to TIC devices.
- Having at least two physically separate points of entry and separate cabling paths to external Internet service providers, rather than a single Internet service provider using a single circuit.
- Filtering inbound traffic to Web servers to protect from attacks.
- Validating domain signatures[8] of e-mails received from external institutions, and supporting the domain-level signing of outbound e-mail.

The IRS continues to work to address gaps in order to comply with the TIC initiative's mandated requirements. The IRS has taken steps to correct previous gaps in meeting TIC Reference Architecture v2.0 capabilities, such as implementing external Domain Name System Security Extensions[9] validation to protect against manipulation of Domain Name System[10] data and installing Einstein probes[11] at its TIC access points to comply with intrusion detection standards.

[8] A domain signature is a digital signature added to the header of e-mail messages which allows the recipient of the message to validate that it is from the actual sender.
[9] A technology that protects against attacks that use forged or manipulated Domain Name System data by digitally "signing" the data to ensure that they are valid.
[10] The Domain Name System translates Internet domain and host names to Internet Protocol addresses and implements a distributed database to store this name and address information for all public hosts on the Internet.
[11] Intrusion detection sensors that can alert the U.S. Computer Emergency Response Team in real time to the presence of a malicious or potentially harmful activity in the Federal network traffic and provide correlation and visualization of the derived data.

In addition, the IRS has taken appropriate steps to identify all external connections in order to ensure that those connections which were required to go through a TIC were in fact going through a TIC.

Additional Improvements Would Strengthen Security

Although the IRS has made good progress implementing the TIC requirements, our review revealed areas where improvements could strengthen security over the TICs. Specifically, the IRS should implement audit logging of administrator activity on TIC equipment to ensure that accountability can be established for any actions that are taken. In addition, while the IRS is working towards compliance, actions are still needed to complete TIC requirements related to implementing a Data Loss Prevention (DLP) program and ensuring that the IRS has sufficient personnel in place with the required clearance and the proper locations for handling classified information. Finally, the IRS must implement regular scanning or other automated checks to ensure that vulnerabilities or misconfigurations are timely discovered and mitigated on TIC equipment.

Audit logging of administrator activity on TIC devices was not occurring

The IRS was not capturing audit logs of administrator activity on TIC servers, firewalls, or routers. Because logs were not being captured, activity by administrators on TIC devices was not being reviewed. Audit trails maintain a record of user activity and provide a means to establish individual accountability. TIC specifications require the IRS to maintain the logs needed to establish an audit trail of administrator activity on TIC systems and components. IRS policy requires administrators of IRS systems to ensure that systems are logging in compliance with requirements. In addition, IRS policy requires Information Technology organization security specialists to review audit logs at least weekly. Our interviews with the staff within the IRS's Computer Security Incident Response Capability and User and Network Services organizations revealed confusion over who had responsibility for capturing and reviewing this specific type of audit log. Without an effective system for the capture and review of administrator activity, accountability for actions taken on TIC equipment cannot be established and unauthorized activity may go undetected.

A DLP program was not in place

The DLP program is a system that is designed to detect potential data breach transmissions and prevent them by monitoring, detecting, and blocking sensitive data while **in use** (endpoint actions), **in motion** (network traffic), and **at rest** (data storage). In data loss incidents, sensitive data are disclosed to unauthorized personnel either by malicious intent or inadvertent mistake. Such sensitive data can come in the form of private or company information, intellectual property, financial or patient information, credit card data, and other information depending on the business and the industry. TIC specifications in accordance with OMB Memorandums

M-06-16, M-06-19, and M-07-16[12] recommend the IRS implement a DLP program for safeguarding Personally Identifiable Information and other sensitive information that is in the possession of the Government and preventing its breach.

Although the IRS has a plan in place, it has not yet implemented its DLP program.[13] The IRS intends to implement a DLP solution that is able to identify, log, track, monitor, alert on, report on, and protect sensitive agency information and Personally Identifiable Information. The IRS has planned three releases. Release 1 will address data in motion through monitoring data moving across the IRS information technology perimeter and identifying Personally Identifiable Information, specifically Social Security Numbers. Release 2 will address data-at-rest by detecting sensitive data stored on IRS databases or fileservers. Release 3 will address data-in-use by deploying an end-user client that will allow monitoring of data being created or manipulated on user workstations and preventing its distribution, storage, or alteration.

The IRS has selected a DLP tool and initiated testing of this tool. However, its deployment that was scheduled for the end of Calendar Year 2013 will not be met due to funding issues. Without an effective DLP solution in place, the IRS cannot detect potential data breaches or exfiltration transmissions,[14] putting IRS data at risk of unauthorized disclosure and loss.

A sufficient number of operational employees did not have appropriate security clearances for handling classified information

The IRS currently does not have sufficient personnel in place with the required clearance for handling classified information. TIC specifications require the IRS to have personnel with Top Secret Sensitive Compartmented Information clearance. This clearance provides the individual with the authority to report, acknowledge, and initiate actions based on ongoing cyber investigations, intrusions, incidents, and operations that are classified at the Top Secret Sensitive Compartmented Information level with the U.S. Computer Emergency Response Team (US-CERT) and other cleared operational cyber components. The intent is to have at least one qualified person with this clearance always available (on call, including weekends and holidays) to exchange classified communications within two hours. During off hours, TICs may have reduced staffing. Network operations center personnel working after hours may need to escalate an incident to on-call personnel with Top Secret Sensitive Compartmented Information clearance. While some IRS executives have the required clearance, employees at the operational level who are available to address TIC security issues do not. The IRS had not yet requested the

[12] OMB M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006), OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 6, 2006), and OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

[13] A prior report, Treasury Inspector General for Tax Administration, Ref. No. 2011-20-012, *Additional Security Is Needed for the Taxpayer Secure Email Program* (Feb. 2011), recommended that the IRS deploy a data leakage prevention system to prevent sensitive data, such as Social Security Numbers, from leaving the IRS domain.

[14] The unauthorized transmission of data from a computer to the external world.

security clearances through the Department of the Treasury due to other priorities. Without these security clearances at the operational level, the IRS may be unable to receive and react to classified TIC security issues in a timely manner.

Sensitive Compartmented Information Facilities were not available for IRS TICs

The IRS does not have a Sensitive Compartmented Information Facility (SCIF) at any of its three TIC locations. A SCIF[15] is a secured area within a building that is used to process sensitive compartmented information. Sensitive compartmented information is classified secret or top secret information that is derived from intelligence sources, methods, or analytical processes. All sensitive compartmented information must be processed, stored, used, or discussed in an accredited SCIF.

TIC specifications require accredited SCIFs to be maintained within 30 minutes of each TIC management location in order for authorized personnel to exchange classified information, evaluate the recommendations, initiate the response, and report operational status with the US-CERT within two hours of the notification. For example, the IRS may need to report to or receive from the US-CERT information regarding cyberattacks, threats, or incidents that are classified at the sensitive compartmented information level and must be handled in a properly secured area. While the Department of the Treasury maintains a SCIF at its headquarters building located in Washington, D.C., this facility is not within 30 minutes of the IRS TICs. The IRS is in the process of implementing this requirement. The IRS indicated that it has encountered challenges to implementing SCIFs that include working with the General Services Administration to identify suitable space, selecting a contractor to complete the work, and working with the Department of the Treasury to provide final approval after the construction is complete. Without fully compliant SCIFs at each TIC location, the IRS may be unable to receive and react to top secret security issues in a timely and secure manner.

Implementing required scans can further secure TIC firewalls and routers

Although the IRS has generally configured TIC firewalls and routers securely, we found instances where firewalls or routers were not configured in compliance with required baseline configuration settings. The IRS was not regularly scanning its TIC firewalls and routers to identify vulnerabilities or misconfigurations. Both TIC specifications and IRS policy require that firewalls and routers be scanned monthly to ensure that vulnerabilities or misconfigurations are timely discovered and mitigated.

We reviewed all 38 firewalls deployed within IRS's TIC environments and their related 66 routers. The firewalls and routers are used to move network traffic between the Internet

[15] Office of the Director of National Intelligence, Intelligence Community Directive Number 705, *Sensitive Compartmented Information Facilities* (May 26, 2010), established the uniform physical and technical requirements with which facilities must comply in order to be accredited as a SCIF.

access provider and the IRS internal network. We found the following instances of noncompliance.

- Administrator accounts on two of 38 firewalls did not have a password, allowing direct access at the highest privilege without a password. IRS policy requires all systems to have passwords that meet minimum requirements. Administrative accounts without passwords can be accessed by anyone and would provide unrestricted access to everyone on the computer as well as a jumping point to access other systems, increasing the risk of unauthorized access and exposure to sensitive data.

- Administrator passwords on 20 of 66 routers were not securely encrypted within the router configuration files. These routers had the "enable password" encryption scheme that the manufacturer had stated in 2008 should no longer be used. Passwords encrypted with the "enable password" scheme can readily be decrypted if access was gained to the configuration file or a stored copy of the configuration file. Instead, the manufacturer stated that all passwords on routers should use the "enable secret" routine that utilizes a stronger encryption routine. IRS policy requires passwords to be protected through encryption that meets Federal standards when stored or transmitted. Weak encryption of administrator passwords increases the risk of unauthorized access and disclosure of taxpayer data.

- Time zone configurations on two of 66 routers were not properly configured. IRS policy requires that routers be time-synchronized with the IRS's authoritative time server. Without proper time synchronization, events that occur on these routers may not be accurately time stamped, making it difficult to detect attacks or investigate suspicious user activity.

- The system-use notification/warning banner in use on 10 of 38 firewalls and 52 of 66 routers did not meet the IRS-approved notification/warning banner text. IRS policy specifies the approved text that must be displayed before granting access to an IRS system. The warning banner text was modified to include appropriate legal citations in May 2012. Not displaying the approved banner could result in authorized and unauthorized users not being aware that they have accessed a U.S. Government system that requires prior authorization and that they have forfeited their rights to privacy when using the specified system.

- A "deny all" rule is typically placed at the end of each Access Control List to specifically deny traffic that has not been permitted or denied earlier within that Access Control List. On two of 66 routers we reviewed, a "deny all" rule was misplaced in the middle of an Access Control List. This misplacement prevented legitimate traffic from reaching the rule that would have permitted the traffic to transit the router.

The IRS informed us that it corrected the misconfigurations on the routers and devices that we reported. The lack of regular scanning or other means for automated checks to verify compliance on firewalls and routers led to the incorrect configurations we found. Without regular scanning or automated checks, vulnerabilities may not be timely discovered and fixed, ultimately decreasing the security posture of the IRS network.

Operating systems were outdated on certain TIC servers

The IRS has eight TIC servers running outdated versions of the Linux Red Hat operating system. IRS policy requires that equipment be maintained at proper configuration baselines. However, the IRS organization responsible for updating these systems did not sufficiently monitor them to ensure that operating systems were updated in a timely manner. Outdated operating systems increase the risk of attacks that exploit known vulnerabilities, resulting in unauthorized access or loss of IRS data.

Recommendations

The Chief Technology Officer should ensure that the IRS:

Recommendation 1: Implements the capture and review of administrator activity on TIC devices, including users accessing these devices, logon and logoff times, and activities conducted during access.

> **Management's Response:** The IRS agreed with this recommendation. The User and Network Services organization will engage the Cybersecurity Enterprise Security Audit Trail team to facilitate gap analysis of existing Enterprise Security Audit Trail audit and review capabilities and fully implement the capture and review of administrator activity on TIC devices.

Recommendation 2: Fully implements the selected DLP tool upon successful testing.

> **Management's Response:** The IRS agreed with this recommendation. The IRS's current implementation of the DLP tool to monitor outbound e-mail and web traffic is scheduled to be completed in December 2014.

Recommendation 3: Obtains Top Secret Sensitive Compartmented Information clearances for IRS operational employees who can receive and react to classified information on a 24/7 basis.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity Computer Security Incident Response Center requires access to Top Secret Sensitive Compartmented Information on specific ongoing real-world classified cyber investigations, intrusions, incidents, and operations and will continue to work with the Department of the Treasury to obtain and clear appropriate staff.

Recommendation 4: Completes implementation of the SCIFs at TIC management locations.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity organization understands the importance of appropriate classified facilities and previously initiated planning and design work with the Real Estate and Facilities Management organization at the two primary IRS Security Operations Centers which also serve as TIC management locations. The Cybersecurity organization will monitor the progress and work with the Real Estate and Facilities Management organization to complete the implementation of the SCIFs at these locations.

Recommendation 5: Implements vulnerability and configuration management scanning on firewalls and routers and mitigates reported findings.

> **Management's Response:** The IRS agreed with this recommendation. The User and Network Services organization will engage the Cybersecurity organization to perform vulnerability scanning on TIC firewalls and routers. Additionally, the User and Network Services organization will verify that all TIC routers, switches, and firewalls are currently reporting to Hewlett Packard Network Automation for biweekly Guidelines, Standards, and Procedures compliance validation checking.

Recommendation 6: Updates all TIC equipment to the most current operating systems approved for use within the IRS.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will review TIC inventory and current operating system releases and identify any systems that are not running the current release approved for use within the IRS. Following the review of the systems, the User and Network Services organization will engage the system vendor to analyze TIC components for any known vulnerabilities and recommend updated releases for any systems running outdated software.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of our review was to evaluate the IRS's three TICs to ensure that the connections complied with the Department of Homeland Security requirements. To accomplish this objective, we:

I. Determined the effectiveness of IRS efforts to identify all existing external connections and route those connections through the TICs.

   A. Assessed whether the IRS is properly applying the definition of "external connection" in accordance with the TIC Reference Architecture v2.0.

   B. Assessed whether the IRS effectively identified all of its external connections.

   C. Determined whether any criteria exist that allows certain external connections to not go through a TIC.

II. Determined the effectiveness of IRS efforts to comply with TIC Reference Architecture v2.0 requirements as well as selected security controls protecting the TICs.

   A. Identified Federal requirements for implementation and configuration of each TIC component.

   B. Reviewed the Cybersecurity Capability Validation Report issued by the DHS in March 2013 that provided an assessment of TIC compliance for two of the IRS TICs. We did not verify or validate the reported results.

   C. Determined the effectiveness of security controls over TIC components.

      1. Verified whether operating systems had been properly updated.

      2. Verified whether access controls were in place.

      3. Verified whether audit trails were captured and reviewed.

      4. Reviewed all 38 TIC firewalls and their 66 related routers to verify whether they were properly configured. Because scanning reports were generally not available, we extracted and reviewed configuration files directly from the firewalls and routers.

5. Verified whether Domain Name System Security Extensions[1] was in place.
6. Verified whether a network intrusion detection system was in place and reports and logs were reviewed.
7. Determined whether a DLP program was in place.

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 for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: IRS policies and procedures for the identification and control of external network connections and for ensuring required security controls are implemented on TIC equipment. We evaluated these controls by reviewing IRS, DHS, and OMB policies; interviewing IRS personnel; and reviewing IRS TIC documentation and device configurations.

[1] A technology that protects against attacks that use forged or manipulated Domain Name System data by digitally "signing" the data to ensure that they are valid.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Bret Hunter, Senior Auditor
Sam Mettauer, Information Technology Specialist
Larry Reimer, Information Technology Specialist

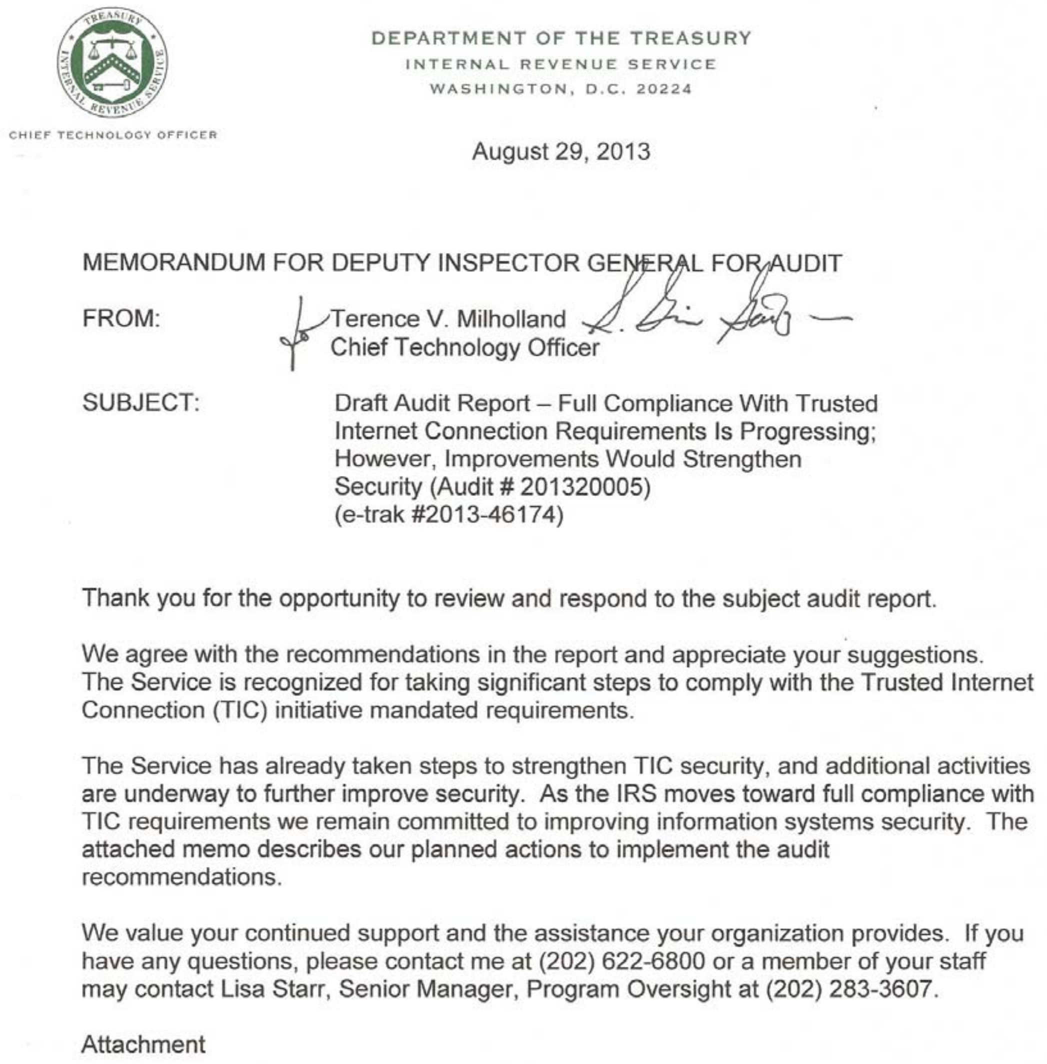
Appendix III

Report Distribution List

Acting Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Office of the Deputy Commissioner for Services and Enforcement SE
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
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 Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Management's Response to the Draft Report



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

CHIEF TECHNOLOGY OFFICER

August 29, 2013

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Full Compliance With Trusted Internet Connection Requirements Is Progressing; However, Improvements Would Strengthen Security (Audit # 201320005)
(e-trak #2013-46174)

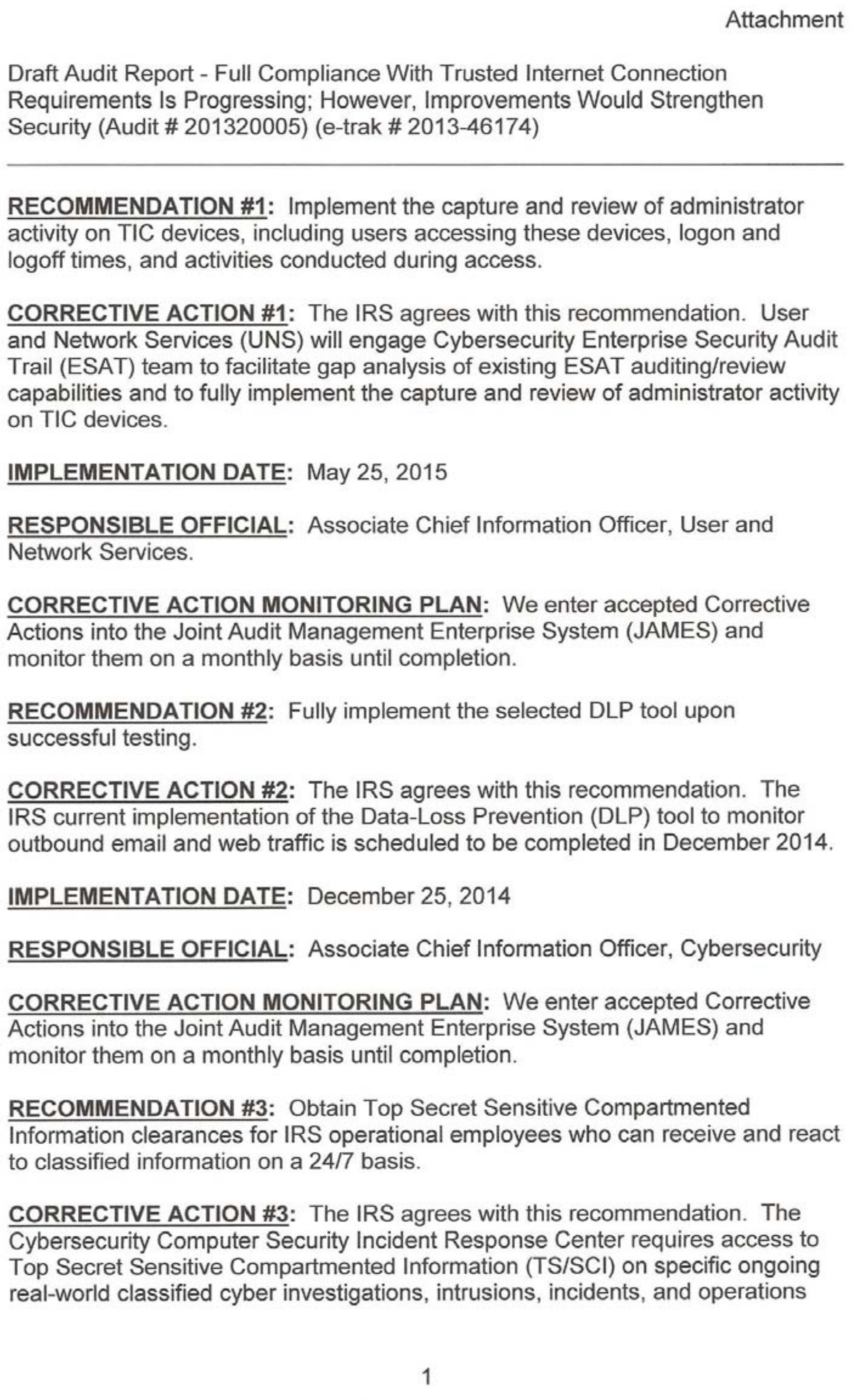
Thank you for the opportunity to review and respond to the subject audit report.

We agree with the recommendations in the report and appreciate your suggestions. The Service is recognized for taking significant steps to comply with the Trusted Internet Connection (TIC) initiative mandated requirements.

The Service has already taken steps to strengthen TIC security, and additional activities are underway to further improve security. As the IRS moves toward full compliance with TIC requirements we remain committed to improving information systems security. The attached memo describes our planned actions to implement the audit recommendations.

We value your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 622-6800 or a member of your staff may contact Lisa Starr, Senior Manager, Program Oversight at (202) 283-3607.

Attachment



Attachment

Draft Audit Report - Full Compliance With Trusted Internet Connection Requirements Is Progressing; However, Improvements Would Strengthen Security (Audit # 201320005) (e-trak # 2013-46174)

RECOMMENDATION #1: Implement the capture and review of administrator activity on TIC devices, including users accessing these devices, logon and logoff times, and activities conducted during access.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. User and Network Services (UNS) will engage Cybersecurity Enterprise Security Audit Trail (ESAT) team to facilitate gap analysis of existing ESAT auditing/review capabilities and to fully implement the capture and review of administrator activity on TIC devices.

IMPLEMENTATION DATE: May 25, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User and Network Services.

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: Fully implement the selected DLP tool upon successful testing.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. The IRS current implementation of the Data-Loss Prevention (DLP) tool to monitor outbound email and web traffic is scheduled to be completed in December 2014.

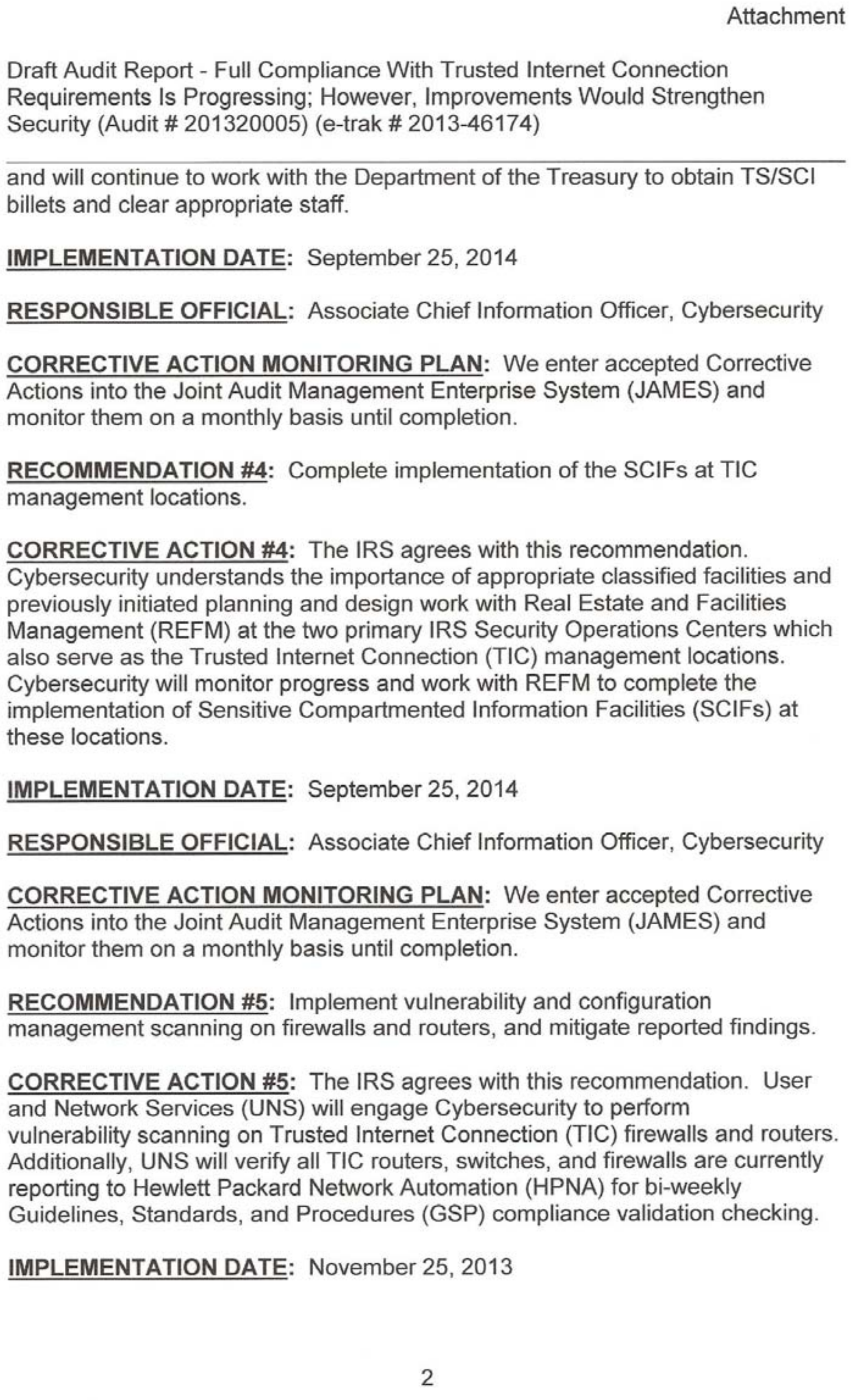
IMPLEMENTATION DATE: December 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, 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 #3: Obtain Top Secret Sensitive Compartmented Information clearances for IRS operational employees who can receive and react to classified information on a 24/7 basis.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The Cybersecurity Computer Security Incident Response Center requires access to Top Secret Sensitive Compartmented Information (TS/SCI) on specific ongoing real-world classified cyber investigations, intrusions, incidents, and operations



and will continue to work with the Department of the Treasury to obtain TS/SCI billets and clear appropriate staff.

IMPLEMENTATION DATE: September 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, 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: Complete implementation of the SCIFs at TIC management locations.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. Cybersecurity understands the importance of appropriate classified facilities and previously initiated planning and design work with Real Estate and Facilities Management (REFM) at the two primary IRS Security Operations Centers which also serve as the Trusted Internet Connection (TIC) management locations. Cybersecurity will monitor progress and work with REFM to complete the implementation of Sensitive Compartmented Information Facilities (SCIFs) at these locations.

IMPLEMENTATION DATE: September 25, 2014

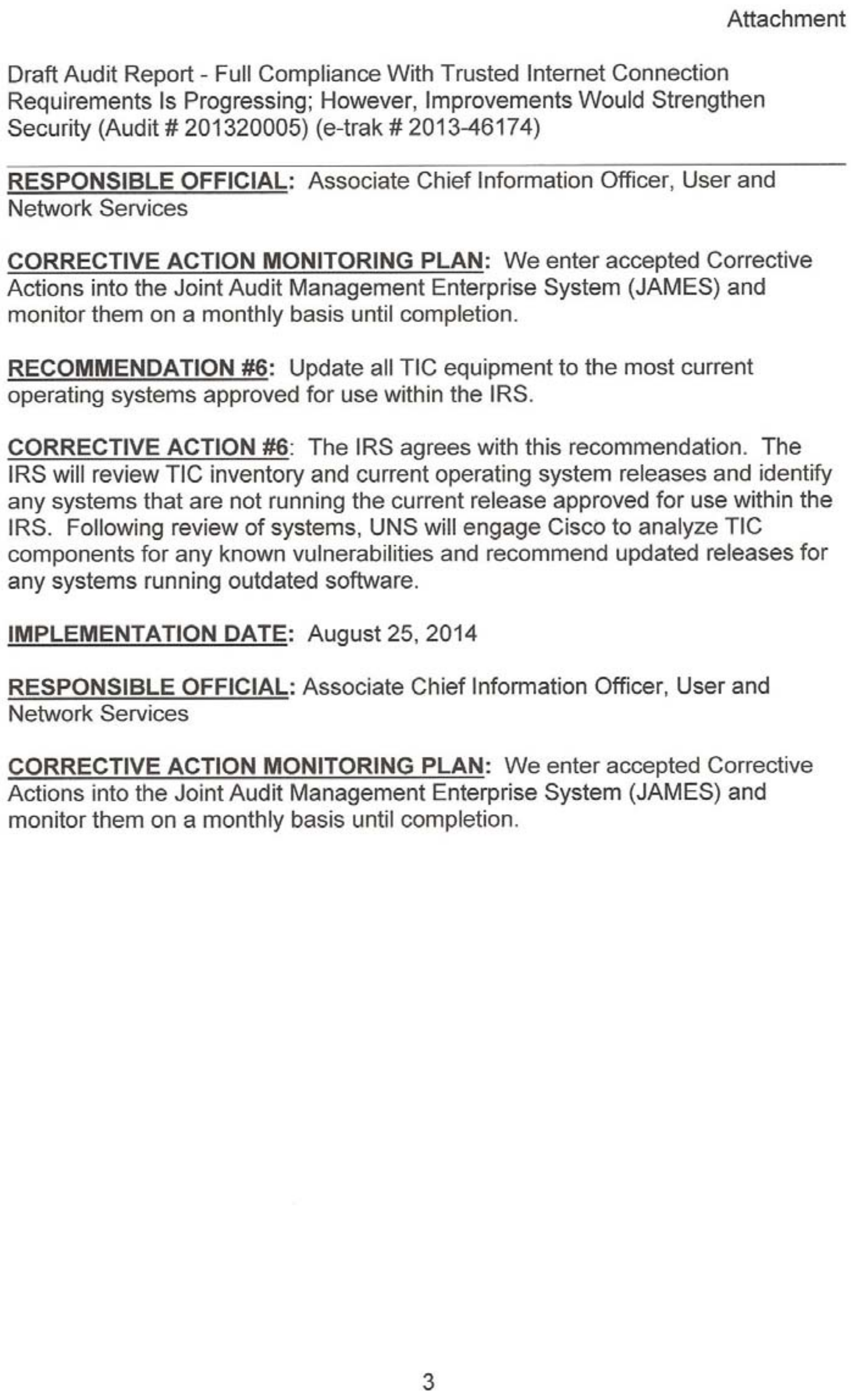
RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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: Implement vulnerability and configuration management scanning on firewalls and routers, and mitigate reported findings.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation. User and Network Services (UNS) will engage Cybersecurity to perform vulnerability scanning on Trusted Internet Connection (TIC) firewalls and routers. Additionally, UNS will verify all TIC routers, switches, and firewalls are currently reporting to Hewlett Packard Network Automation (HPNA) for bi-weekly Guidelines, Standards, and Procedures (GSP) compliance validation checking.

IMPLEMENTATION DATE: November 25, 2013



Attachment

Draft Audit Report - Full Compliance With Trusted Internet Connection Requirements Is Progressing; However, Improvements Would Strengthen Security (Audit # 201320005) (e-trak # 2013-46174)

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User and Network Services

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: Update all TIC equipment to the most current operating systems approved for use within the IRS.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. The IRS will review TIC inventory and current operating system releases and identify any systems that are not running the current release approved for use within the IRS. Following review of systems, UNS will engage Cisco to analyze TIC components for any known vulnerabilities and recommend updated releases for any systems running outdated software.

IMPLEMENTATION DATE: August 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, User and Network Services

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.