Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information

March 26, 2008

Reference Number: 2008-20-071

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

March 26, 2008

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information
(Audit # 200720027)

This report represents the results of our review to determine whether controls were sufficient to detect and deter unauthorized use of Internal Revenue Service (IRS) routers and switches, two key components used to direct network traffic. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2007 Annual Audit Plan and was part of the Information Systems Programs business unit's statutory requirements to annually review the adequacy and security of IRS technology.

Impact on the Taxpayer

Because the IRS sends sensitive taxpayer and administrative information across its networks, routers on the networks must have sufficient security controls to deter and detect unauthorized use. Access controls for IRS routers were not adequate, and reviews to monitor security configuration changes were not conducted to identify inappropriate use. A disgruntled employee, contractor, or hacker could reconfigure routers and switches to disrupt computer operations and steal taxpayer information in a number of ways, including diverting information to unauthorized systems.

Synopsis

The IRS Enterprise Networks organization is responsible for installing, operating, and maintaining routers and switches for a majority of the IRS. Within the Enterprise Networks organization, the Network Management Control Center serves as the Program Management Office and central support center for the IRS network environment throughout the United States.

Its responsibilities include authorizing and authenticating persons accessing routers and switches, monitoring activity on the network, and ensuring that routers are properly configured.

The IRS uses the Terminal Access Controller Access Control System (TACACS+) to administer and configure routers and switches. Users of the TACACS+ must be authorized by managers. The IRS had authorized 374 accounts for employees and contractors that could be used to access routers and switches to perform system administration duties. Of these, 141 (38 percent) did not have proper authorization to access the TACACS+. Authorizations for 86 of the 141 employee and contractor accounts had been provided on some prior date, but the authorizations had expired at the time of our review. However, we could not find that the other 55 employee and contractor accounts had ever been authorized to access the System. We are particularly concerned that 27 of the 55 employees and contractors had accessed the routers and switches to change security configurations.

To authenticate users, the TACACS+ uses a security application that requires users to enter an account name and password. System administrators had circumvented this control by setting up 34 unauthorized accounts that appear to be shared-user accounts. Any person who knew the passwords to these accounts could change configurations without accountability and with little chance of detection. For this reason, the IRS requires that shared accounts be used only on a limited basis and that they be subjected to special authorization controls. However, during Fiscal Year 2007, 4.4 million (more than 84 percent) of the 5.2 million accesses to the TACACS+ were made by the 34 user accounts. None of the accounts were properly authorized.

In addition, the review of audit trails[1] is necessary to detect potential security events such as hacking attempts, virus or worm infections, and attempts to change or alter information. The Modernization and Information Technology Services organization Cybersecurity office has the responsibility to review audit trail information from the TACACS+, routers, and switches at least weekly. In addition, the Cybersecurity office must review audit trail logs after any security incident. Analysis of audit trail events can also allow the administrators and the Network Management Control Center to identify nonstandard configurations that could lead to security vulnerabilities or disruptions to operations.

Audit trail log reviews were not being conducted by the Cybersecurity office, and only a limited percentage of the audit trails for the IRS routers and switches were being reviewed. In addition, system administrators were not following IRS procedures that require an authoritative, IRS-wide time server for the purpose of synchronizing the system clocks of IRS systems. Correct time zone settings are critical during audit trail reviews for detecting inappropriate traffic across the

[1] An audit trail is a chronological record of activities that allows for the reconstruction, review, and examination of a transaction from inception to final results. Audit trails can be used to detect unauthorized accesses to computer systems.

IRS network and for establishing a timeline in case of a multifaceted attack on the IRS network. The time of attack can also be critical evidence in criminal proceedings.

Recommendations

We recommended the Chief Information Officer clarify responsibilities for reconciling user accounts on the TACACS+ with the system used by the IRS to authorize employee access, improve the testing of authentication controls on the TACACS+ to identify any configuration weaknesses, ensure that the TACACS+ is configured to prevent employees and contractors from gaining access to the routers and switches if they have not used the System within 90 calendar days, and eliminate unnecessary shared accounts and ensure that each account is properly authorized. In addition, the Chief Information Officer should ensure that the Enterprise Networks organization provides the audit trails for the TACACS+, routers, and switches to the Cybersecurity office for periodic reviews; audit trail information is filtered for effective analysis; and all routers and switches are configured to the same time zone.

Response

IRS management agreed with six of our recommendations and is evaluating implementation of the seventh. The IRS will begin monthly reconciliation of the TACACS+ user accounts with the system used to authorize employee access, implement testing of the authentication controls on the TACACS+, ensure that employee user accounts are locked after 45 calendar days of inactivity and removed after 90 calendar days of inactivity, and ensure that no unauthorized or unnecessary shared accounts exist on the TACACS+. In addition, audit log information will continue to be filtered in accordance with router and switch guidance, and the Enterprise Networks organization will ensure that the Cybersecurity organization has access to all audit log information for review and analysis. The IRS will evaluate our recommendation to configure all routers and switches to the same time zone to determine whether this approach is an appropriate enterprise solution. We will follow up on the adequacy of these corrective actions in future audits. Management's complete response to the draft report is included as Appendix IV.

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

Table of Contents

Abbreviations

IRS	Internal Revenue Service
TACACS+	Terminal Access Controller Access Control System

Background

Every Internal Revenue Service (IRS) site, whether it is a Computing Center,[1] campus,[2] or small field office, has a local area network interconnecting computers at the site and providing access to the other IRS networks nationwide. IRS data networks rely on thousands of routers and data switches to ensure data traffic is routed and managed effectively.

Routers are devices that determine the proper path for data to travel between different networks. They connect networks and can also direct traffic to the Internet. Routers are now available in many types, although all are fundamentally doing the same job. A modern router is essentially a small network computer with an operating system, a memory, and a small processor that does all of the work in a router. The main manufacturer of commercial-scale routers is Cisco.

In a network of any real complexity, routers will not send data directly to the destination. Instead, information will pass through a series of routers, each getting information one step closer to the destination, until it reaches the router that connects to the final destination. The term "switch" is often used interchangeably with router, but a switch is really a network hub with switched ports that might or might not also perform additional routing functions.

Because the IRS sends sensitive taxpayer and administrative information across its networks, routers must have sufficient security controls to deter and detect unauthorized use. Disgruntled employees, contractors, and hackers who gain access to routers could steal sensitive information and cause denials of service leading to lost productivity. A hacker accessing a poorly configured router could gain full control of the IRS network. For example, an unscrupulous person could divert data traffic through a third-party system on its way to the intended destination.

Denials of service can also be costly for organizations. For example, on January 23, 2001, Microsoft's web sites could not be accessed for nearly 23 hours. The next day, Microsoft attributed the failure to a configuration change to the routers on its network. In 2007, an article by Netcordia[3] stated that Gartner[4] estimated the average hourly cost of network downtime to be $42,000. The average company suffered 87 hours of network downtime annually, equaling $3.65 million in lost revenue.

---

[1] IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.
[2] IRS campuses receive, process, and archive paper and electronic tax and information returns; issue taxpayer notices; process refunds; answer taxpayers' tax law/account inquiries; and provide taxpayers with postfiling services related to collection and examination cases.
[3] *Network Downtime, the Configuration Errors*, Netcordia Whitepapers, 2007.
[4] Gartner, Inc. is a leading information technology research and advisory company.

The IRS Enterprise Networks organization is responsible for installing, operating, and maintaining routers and switches[5] for a majority of the IRS. Within the Enterprise Networks organization, the Network Management Control Center serves as the Program Management Office and central support center for the IRS network environment throughout the United States. Its responsibilities include authorizing and authenticating persons accessing routers and switches, monitoring activity on the network, and ensuring that routers are properly configured.

This review was performed at the IRS offices in New Carrollton, Maryland, within the Enterprise Networks organization during the period January through November 2007. 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.

[5] The IRS Criminal Investigation Division, Office of Chief Counsel, Office of Appeals, and Statistics of Income organization manage routers and switches for their own networks.

Results of Review

Access Controls Over Router and Switch Administration Were Not Effective to Control Unauthorized Use

Authorizing and authenticating access to routers and switches are critical for deterring unauthorized use. Fundamentally, managers must ensure that only those people who have a legitimate business need can gain access to the devices. The IRS created the Online 5081 system[6] in June 2002 to authorize employees and contractors to access its computer systems, including routers and switches. It uses the Terminal Access Controller Access Control System (TACACS+) to authenticate users on routers and switches. This System uses a security application that requires users to enter an account name and password before gaining access.

At the time of our review, the IRS had authorized 374 accounts for employees and contractors that could be used to access routers and switches to perform system administration duties. Of these, 141 (38 percent) did not have proper authorization to access the TACACS+. Authorizations for 86 of the 141 employee and contractor accounts had been provided on some prior date, but the authorizations had expired at the time of our review. However, we could not find that the other 55 employee and contractor accounts had ever been authorized to access the System. We are particularly concerned that 27 of the 55 employees and contractors had accessed the routers and switches to change security configurations.

We also identified weaknesses in the TACACS+ controls used to authenticate users. Nine accounts were still active, although the employees and contractors had not accessed the System for more than 90 calendar days. The System should have been configured to automatically prevent these users from accessing the routers and switches after 90 calendar days. In addition, the system administrators circumvented authentication controls by setting up 34 unauthorized accounts that appear to be shared-user accounts. Any person who knew the passwords to these accounts could change configurations without accountability and with little chance of detection. For this reason, the IRS requires that shared accounts be used only on a limited basis and that they be subjected to special authorization controls. However, during Fiscal Year 2007, 4.4 million (more than 84 percent) of the 5.2 million accesses to the TACACS+ were made by the 34 unauthorized user accounts. None of the accounts were properly authorized.

[6] The Online 5081 system was named after the Information System User Registration/Change Request (Form 5081) the IRS uses to request and authorize user accounts for employees on all systems. The Online 5081 system automates some of the manual processes and provides a centralized system for all system access authorizations.

We are very concerned that authorization and authentication controls are weak on devices as sensitive as routers and switches. A disgruntled employee, contractor, or hacker could reconfigure routers and switches to disrupt computer operations and steal taxpayer information in a number of ways, including diverting information to unauthorized systems. The Treasury Inspector General for Tax Administration is continuing to review security whether configuration changes were appropriate and warranted.

IRS managers of router and switch administrators did not carry out their responsibilities for authorizing access to only those employees and contractors who needed it to carry out their responsibilities. Neither the managers nor the staff at the Network Management Control Center reconciled the Online 5081 system information with TACACS+ user accounts as required. This reconciliation would have found a majority of the weaknesses we identified. None of the IRS managers we contacted stated they were responsible for administering router accounts once they forwarded authorizations to the Network Management Control Center. They stated they believed the administration of the router and switch user accounts was solely the responsibility of others.

TACACS+ administrators were able to make configuration changes to bypass the authentication controls and set up shared accounts due to a lack of oversight by their managers and the Network Management Control Center. Periodic testing of the routers and switches was insufficient to identify these weaknesses.

Recommendations

The Chief Information Officer should:

Recommendation 1: Clarify responsibilities for reconciling user accounts on the TACACS+ with the Online 5081 system and ensure that the reconciliations are conducted routinely. The results from the reconciliations should be used to ensure that only authorized employees and contractors can access the TACACS+.

> ***Management's Response:*** IRS management agreed with this recommendation. The Network Management Control Center will begin monthly reconciliation of the TACACS+ with the Online 5081 system and delete any TACACS+ accounts without an associated Online 5081 system authorization.

Recommendation 2: Improve the testing of authentication controls on the TACACS+ to identify any configuration weaknesses.

> ***Management's Response:*** IRS management agreed with this recommendation. The Enterprise Networks organization will run monthly tests of authentication controls, including the control to ensure that the system locks accounts after three failed attempts.

Recommendation 3: Ensure that the TACACS+ is configured to prevent employees and contractors from gaining access to the routers and switches if they have not used the System within 90 calendar days.

> ***Management's Response:*** IRS management agreed with this recommendation. The Network Management Control Center will ensure TACACS+ accounts are locked after 45 calendar days of inactivity and removed from the System after 90 calendar days of inactivity.

Recommendation 4: Eliminate unnecessary shared accounts on the TACACS+ and ensure that the remaining accounts are properly authorized and limited.

> ***Management's Response:*** IRS management agreed with this recommendation. The Enterprise Networks organization will ensure that no unauthorized or unnecessary shared accounts exist on the TACACS+ and will review the use of shared accounts monthly to ensure that the accounts are properly documented and authorized.

Audit Trails Are Not Being Reviewed to Identify Questionable Activity

IRS procedures provide that audit trail[7] logs for all IRS systems and applications should capture, at a minimum, the following data for each security-related event:

- Date and time the event occurred.
- Unique identifier (e.g., user name, user identification number, application name) of the user or application initiating the event.
- Type of event.
- Subject of the event (e.g., the user, file, or other resource affected) and the action taken on that subject.
- Outcome status (success or failure) of the event.

The review of audit trails is necessary to detect potential security events such as hacking attempts, virus or worm infections and propagation, attempts to change or alter information, and other threats. The Modernization and Information Technology Services organization Cybersecurity office has the responsibility to review audit trail information from the TACACS+, routers, and switches at least weekly. In addition, the Cybersecurity office must review audit trail logs after any security incident. Analysis of audit trail events can also allow the

[7] An audit trail is a chronological record of activities that allows for the reconstruction, review, and examination of a transaction from inception to final results. Audit trails can be used to detect unauthorized accesses to computer systems.

administrators and the Network Management Control Center to identify nonstandard configurations that could lead to security vulnerabilities or disruptions to operations.

For routers and switches, audit trail information is obtained from two sources. The TACACS+ records events such as password changes, failed attempts, commands entered, and configuration changes and stores them in its database, where reports can be generated and reviewed. In addition, the router and switch devices can generate daily logs on security events, such as blocked information, failed logons, and attempted exploits. The data are sent to remote servers where they are stored. The TACACS+ audit trail log reviews were not being conducted by the Cybersecurity office, and only a limited percentage of the audit trails for the IRS routers and switches were being reviewed.

In addition, system administrators were not following IRS procedures that require an authoritative IRS-wide time server for the purpose of synchronizing the system clocks of IRS systems. Correct time zone settings are critical during audit trail reviews for detecting inappropriate traffic across the IRS network and for establishing a timeline in case of a multifaceted attack on the IRS network. The time of attack can also be critical evidence in criminal proceedings. We reviewed 169 configuration error reports for routers and switches and found that 15 (9 percent) did not follow these procedures.

Inaccurate audit trails and inadequate monitoring of audit trail logs increase the likelihood that security events will not be detected and that nonstandard configurations such as the authentication weaknesses discussed earlier will not be identified. As a result, malicious persons could exploit vulnerabilities in the routers and switches to gain unauthorized access to sensitive information and disrupt computer operations with little chance of detection.

We attribute the weaknesses in controls to detect unauthorized events to three main factors.

- Audit trail logs on IRS routers and switches are capturing excessive amounts of data. The routers were set at a level that logs day-to-day activities such as network session logs. Not all logging messages at this level are necessary for detecting inappropriate activity. In addition, the data maintained at this level require a substantial amount of disk space for storage. To conduct effective reviews of audit trail logs, organizations must choose the minimum level of audit trail information that is sufficient for review. When an excessive amount of data is captured, reviewing the data can be too cumbersome.
- The Cybersecurity office did not emphasize the need to receive and review the TACACS+ audit trail logs. The Cybersecurity office did review audit trail logs for some routers and switches, but not all of the logs were being forwarded to it by the Enterprise Networks organization.
- Configurations on routers and switches were not monitored to ensure that time zone settings met IRS standards. The tool used by the IRS to test routers and switches was not configured to track time zone settings.

Recommendations

The Chief Information Officer should:

Recommendation 5: Use available filtering techniques to limit the amount of audit trail information necessary for detecting inappropriate activity.

> ***Management's Response:*** IRS management agreed with this recommendation. The IRS filters audit trail data in accordance with current guidance. The Enterprise Networks organization will coordinate with the Cybersecurity office to evaluate other filtering techniques to determine the benefit to its enterprise environment.

Recommendation 6: Ensure that the Enterprise Networks organization provides the audit trails for the TACACS+, routers, and switches to the Cybersecurity office for review and analysis.

> ***Management's Response:*** IRS management agreed with this recommendation. The Enterprise Networks organization will provide the Cybersecurity office access to the TACACS+ audit logs and ensure that all audit log information is available for review and analysis.

Recommendation 7: Ensure that all routers and switches are configured to the same time zone. The use of one time zone across the entire nation would facilitate the tracking of network activity and eliminate potential confusion due to different time zones and daylight savings time. Also, time zone setting configurations should be included in testing scripts (programs) to ensure that they are set accurately.

> ***Management's Response:*** IRS management agreed with this approach. However, the Enterprise Networks organization believes such an undertaking presents several complexities. The Enterprise Networks organization is evaluating the recommendation to configure all routers and switches to the same time zone to determine whether this approach is an appropriate enterprise solution and will document the results of the study.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether controls were sufficient to detect and deter unauthorized use of IRS routers and switches, two key components used to direct network traffic. To accomplish this objective, we:

I. Determined whether IRS guidelines, standards, and procedures are consistent with those from the National Institute of Standards and Technology and the Department of the Treasury and with industry standard practices.

II. Evaluated authorization and authentication controls for IRS routers and switches on the internal network.

   A. Determined whether all TACACS+ users had been properly authorized for access.

   B. Determined whether TACACS+ users needed access to carry out their responsibilities.

   C. Evaluated the managerial review process to ensure that all user accounts were necessary.

   D. Determined whether each system administrator had his or her own unique account and password for access to routers and switches.

   E. Determined whether passwords for user accounts met IRS standards.

III. Determined whether audit trails were created and reviewed to detect suspicious transactions on routers, switches, and the TACACS+.

   A. Reviewed the audit trail log settings on the TACACS+ to ensure that all appropriate actions were logged.

   B. Determined whether network administrators and/or the Cybersecurity office examined audit trail logs on a regular basis.

   C. Determined whether audit trail logs were securely stored.

IV. Determined whether routers and switches had been configured securely.

   A. Obtained the weekly configuration error reports from February 12 to March 12, 2007 (5 weeks) and analyzed the testing results to ensure that all devices were tested and vulnerabilities were corrected.

B. Validated the adequacy of the configuration error reports by sampling routers and switches from the March 12, 2007, error report to determine whether other significant vulnerabilities existed and were not identified. A sample of 30 routers was judgmentally selected from the 111 routers identified in the March 12, 2007, error report. Judgmental sampling was performed for ease of use in selecting the sample. All 17 switches identified in the error report were reviewed.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Thomas Polsfoot, Audit Manager
Charles Ekunwe, Senior Auditor
Cari Fogle, Senior Auditor
Esther Wilson, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Acting Chief of Staff C
Deputy Commissioner for Operations Support OS
Director, Program Oversight OS:CIO:SM:PO
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 Controls OS:CFO:CPIC:IC
Audit Liaison: Chief Information Officer OS:CIO

Appendix IV

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

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

RECEIVED
FEB 27 2008

February 27, 2008

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Arthur L. Gonzalez
Chief Information Officer

SUBJECT: Draft Audit Report – Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information (Audit #200720027) (i-trak #2008-32871)

Thank you for the opportunity to review the draft audit report and respond to the recommendations. We are committed to ensuring sufficient controls are in place to detect and deter unauthorized use of the Internal Revenue Service's routers and switches.

We have implemented a number of initiatives and continue to improve the control and monitoring of routers and switches. A few examples of these initiatives include:

- All 369 Terminal Access Controller Access Control System+ (TACACS+) users, including contractors, now have access to the Online 5081 system and have current and valid authorizations on file.
- We now provide the minimum level of permissions to routers and switches for authorized users who require such access to perform their duties.
- We have implemented configuration management and compliance initiatives using CiscoWorks, OPNET NetDoctor, and TACACS+ to ensure proper maintenance of all routers and switches and conformance of their configurations to policy standards as defined in our Guidelines, Standards, and Procedures (GSP) documents.

Enterprise Networks has reduced the number of service accounts referenced in your report from 34 to 24 and documented the use and authorization of those accounts. These service accounts are necessary for collecting data to support the functions and management of the IRS router infrastructure. Of the total 5.2 million CiscoWork transactions in fiscal year 2007, the system automatically performed 4.4 as a result of the initial set up and configuration of each CiscoWork system. After the initial CiscoWorks system setup, the TACACS+ and CiscoWorks log files track any additional system administrator initiated transactions to the individual who initiated the transaction. In March 2009, Enterprise Networks will deploy a new CiscoWorks infrastructure that will reduce the number of service accounts from 24 to 6, which in turn will reduce the number of transactions from 5.2 million to 800 thousand. Our policy has always been to prohibit shared

accounts and to require every user to have his or her own user ID and password with authorization based on a valid Online 5081.

We are evaluating your recommendation to configure all routers and switches to the same time zone, to determine whether this approach is an appropriate enterprise solution. We will document our research and keep you informed of our findings.

Thank you for your continued support and guidance. If you have any questions, please contact me at (202) 622-6800 or Perry Robinett, Director, Program Oversight, at (202) 283-6283.

Attachment

Attachment

Management Response to Draft Audit Report – Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information (Audit #200720027) (i-trak # 2008-32871)

RECOMMENDATION #1: The Chief Information Officer should clarify responsibilities for reconciling user accounts on the Terminal Access Controller Access Control System (TACACS+) with the Online 5081 system and ensure the reconciliations are conducted routinely. The results from the reconciliations should be used to ensure only authorized employees and contractors can access the TACACS+.

CORRECTIVE ACTION #1: We agree with this recommendation. The Associate Chief Information Officer, Enterprise Networks' Network Management Control Center (NMCC) Branch will begin monthly reconciliation of TACACS+ user accounts against the corresponding Online 5081 user account authorization. The NMCC will delete any accounts without an associated Online 5081. The Associate Chief Information Officer, Enterprise Networks will add this procedure to the NMCC Standard Operating Procedures (SOPs) as a monthly process.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Networks

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

RECOMMENDATION #2: The Chief Information Officer should improve the testing of authentication controls on the TACACS+ to identify any configuration weaknesses.

CORRECTIVE ACTION #2: We agree with this recommendation. The Associate Chief Information Officer, Enterprise Networks will improve the testing of the authentication process by running monthly tests in accordance with NIST SP 800-53A to ensure the system does not permit unauthorized access by locking the account after three failed attempts. The NMCC will document the results of this test. The Associate Chief Information Officer, Enterprise Networks will add this procedure to the NMCC SOPs as a monthly process.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Networks

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

Attachment

Management Response to Draft Audit Report – Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information (Audit #200720027) (i-trak # 2008-32871)

RECOMMENDATION #3: The Chief Information Officer should ensure the TACACS+ is configured to prevent employees and contractors from gaining access to the routers and switches if they have not used the system within 90 calendar days.

CORRECTIVE ACTION #3: We agree with this recommendation. The Associate Chief Information Officer, Enterprise Networks' NMCC Branch will ensure TACACS+ user accounts are locked after 45 calendar days of inactivity and removed from the system after 90 calendar days of inactivity in accordance with IRM 10.8.1. The NMCC will use this account lock-out feature and will check each TACACS+ user account monthly to ensure compliance. The Associate Chief Information Officer, Enterprise Networks will add this procedure to the NMCC SOPs as a monthly process.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Networks

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

RECOMMENDATION #4: The Chief Information Officer should eliminate unnecessary shared accounts on the TACACS+ and ensure the accounts that remain are properly authorized and limited.

CORRECTIVE ACTION #4: We agree with the recommendation. The Associate Chief Information Officer, Enterprise Networks will ensure no unauthorized or unnecessary shared accounts exist for TACACS+. Enterprise Networks' NMCC Branch will review the use of all shared TACACS+ accounts monthly to ensure the accounts are properly documented and authorized. The Associate Chief Information Officer, Enterprise Networks will add this procedure to the NMCC SOPs as a monthly process.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Networks

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

Attachment

Management Response to Draft Audit Report – Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information (Audit #200720027) (i-trak # 2008-32871)

RECOMMENDATION #5: The Chief Information Officer should use available filtering techniques to limit the amount of audit trail information necessary for detecting inappropriate activity.

CORRECTIVE ACTION #5: We agree with the value of filtering, which is the basis for this recommendation. Currently, the Associate Chief Information Officer, Enterprise Networks organization filters syslog messages at the source in accordance with the router and switch Guides, Standards, and Policies. The Computer Security Incident Response Center will continue to perform the appropriate aggregation and correlation of the audit trail data it receives using the Security Information Management (SIM) solution. The Associate Chief Information Officer, Enterprise Networks will coordinate with Cybersecurity to evaluate other filtering techniques to determine the benefit to our enterprise environment.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Networks

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #6: The Chief Information Officer should ensure the Enterprise Networks organization provides the audit trails for the TACACS+, routers, and switches to the Cybersecurity office for review and analysis.

CORRECTIVE ACTION #6: We agree with this recommendation. The Associate Chief Information Officer, Enterprise Networks will provide the Cybersecuity organization access to the TACACS+ logs and ensure all syslog messages from routers and switches are available for review and analysis. Cybersecurity will be able to access this information as needed to conduct ongoing analysis.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Networks

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

Attachment

Management Response to Draft Audit Report – Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information (Audit #200720027) (i-trak # 2008-32871)

RECOMMENDATION #7: The Chief Information Officer should ensure all routers and switches are configured to the same time zone. The use of one time zone across the entire nation would facilitate the tracking of network activity across the nation and eliminate potential confusion due to different time zones and daylight savings time. Also, time zone setting configurations should be included in testing scripts (programs) to ensure they are set accurately.

CORRECTIVE ACTION #7: We agree this would be a beneficial approach, however, the Associate Chief Information Officer, Enterprise Networks has determined such an undertaking presents several complexities due to the interdependencies of hardware and software components that rely on these infrastructure components for time synchronization. The Associate Chief Information Officer, Enterprise Networks is evaluating the recommendation to configure all routers and switches to the same time zone to determine whether this approach is an appropriate enterprise solution and will document the results of the study.

Should we decide to implement the recommendation, Enterprise Networks will test and validate time zone setting configurations monthly and will add this procedure to the SOPs as a monthly process.

IMPLEMENTATION DATE: September 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Networks

CORRECTIVE ACTION MONITORING PLAN: Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.