

# DEPARTMENT OF HOMELAND SECURITY

## Office of Inspector General

### Improved Security Required For Transportation Security Administration Networks (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552(b)(2). A review under the Freedom of Information Act will be conducted upon request.

**Office of Information Technology**

**OIG-05-31**

**August 2005**

*Office of Inspector General*

**U.S. Department of Homeland Security**  
Washington, DC 20528



**Homeland  
Security**

## Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared by our office as part of our DHS oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report assesses the strengths and weaknesses of controls over network security at the Transportation Security Administration (TSA). It is based on interviews with employees and officials of the TSA, direct observations, technical scans, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner  
Inspector General

# Table of Contents/Abbreviations







---

Executive Summary .....	1
Background.....	2
Results of Audit .....	4
TSA Does Not Have a Comprehensive Network Security Testing Program .....	4
Recommendation .....	5
TSA Needs Further Improvements to Secure its Network .....	5
Recommendation .....	11
Audit Trails Are Not Regularly Reviewed and Maintained .....	11
Recommendation .....	12
Contingency Plan Has Not Been Completed .....	12
Recommendation .....	13

## Appendices

Appendix A: Purpose, Scope, and Methodology .....	14
Appendix B: Management Response To Draft Report .....	15
Appendix C: NIST’s Recommended Testing Schedule .....	18
Appendix D: Vulnerabilities Detected by Location .....	19
Appendix E: Major Contributors to This Report.....	20
Appendix F: Report Distribution.....	21

## Abbreviations

	
CIO	Chief Information Officer
DHS	Department of Homeland Security
DoS	Denial of Service
FISMA	Federal Information Security Management Act
FSD	Federal Security Director
	
IDS	Intrusion Detection System
ISS	Internet Security Systems
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
	
TSA	Transportation Security Administration
WAN	Wide Area Network

# OIG

*Department of Homeland Security  
Office of Inspector General*

---

## **Executive Summary**

The Office of Inspector General (OIG) audited the security program of the Department of Homeland Security (DHS) and its organizational components to evaluate the effectiveness of controls implemented on selected wired-based sensitive but unclassified networks. This audit included a review of applicable DHS and Transportation Security Administration (TSA) security policies, procedures, and other appropriate documentation. In addition, we performed vulnerability assessments to evaluate the effectiveness of controls implemented on selected network devices.

Our overall objective was to determine whether TSA has implemented adequate controls for protecting its networks. To address our objective, we: (1) interviewed personnel at TSA Headquarters, [REDACTED]; [REDACTED]; [REDACTED]; (2) reviewed DHS and TSA's policies and procedures; and (3) conducted vulnerability assessments for a select sample of network devices at three TSA locations [REDACTED].

TSA has taken actions and made progress in securing its networks. TSA has strengthened the security configurations on its servers and workstations. As a result, we have detected significantly fewer security vulnerabilities compared to the vulnerability assessment results reported in a prior OIG audit report<sup>1</sup>.

However, TSA can make further improvements to secure its networks. For example, TSA has not developed adequate policies and procedures and fully implemented processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. In addition, the contingency plan for the TSANet has not been finalized and tested to ensure that critical operations could be restored in the event of emergency.

---

<sup>1</sup> *DHS Needs to Strengthen Controls For Remote Access to Its Systems and Data*, dated November 2004 (OIG-05-03).

---

To evaluate the effectiveness of the controls implemented, we conducted vulnerability assessments of network devices at three TSA locations. These assessments identified security concerns resulting from missing critical patches, vulnerable network devices, and weaknesses in configuration management. These security concerns provide increased potential for unauthorized access to TSA resources and data.

We made several recommendations to assist TSA in remedying these issues in order to more effectively secure its networks. Effective network management and security controls are needed in order to protect the confidentiality, integrity, and availability of sensitive information.

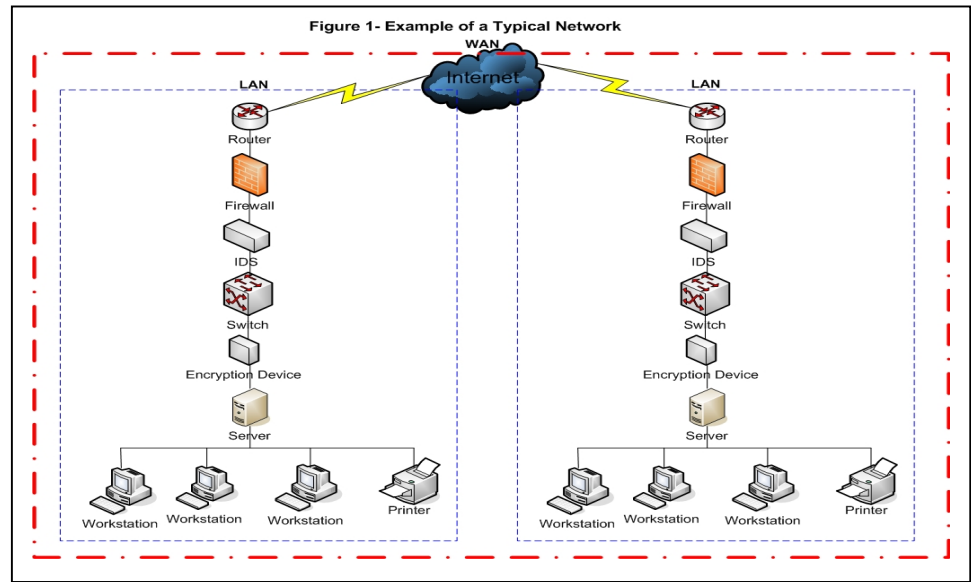
In response to our draft report, TSA agreed and has already taken steps to implement each of the recommendations. TSA's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

## **Background**

There are many advantages associated with utilizing computer networks to share information, not the least of which is to dramatically boost productivity, efficiency, and competitiveness for government agencies. However, the open nature of networks makes it important that government agencies secure their networks and protect them from vulnerabilities. As a result, network security is no longer something that resides primarily at the perimeter of a network. Network security must be evaluated from all points of entry into the network: desktop and laptop computers, remote access, connections to third-party networks, and wireless access points. Effective network security is needed to protect the confidentiality, integrity, and availability of sensitive information. The primary reason to develop controls and test the security of an operational network is to identify and remedy potential vulnerabilities.

Networks are a series of interconnected devices which allow individual users and organizations to share information. A network that comprises a relatively small geographical area is known as a local area network (LAN). A network which connects various LANs dispersed over a wide geographical area is called a wide area network (WAN). Network devices include servers, workstations, and printers (used to create, process,

maintain, and view information); routers<sup>2</sup> and switches<sup>3</sup> (used to communicate information); firewalls<sup>4</sup> and encryption devices<sup>5</sup> (used to protect information being transported; and intrusion detection systems (IDS)<sup>6</sup> (used to monitor and analyze network events). Figure 1 is an illustration of a typical network.



Since sensitive data is stored on and transmitted along networks, effectively securing networks is essential for protecting sensitive data from unauthorized access, manipulation, and misuse. Improperly configured network services expose a network to internal or external threats such as hackers, cyber-terrorist groups, and Denial of Service (DoS) attacks. Further, as networks provide the entry point for access to

<sup>2</sup> Routers are devices which join multiple networks. Configuration information maintained in the “routing table” allows routers to filter traffic - either incoming or outgoing - based on the Internet Protocol addresses of senders and receivers.

<sup>3</sup> Switches are devices which join multiple networks at a low-level network protocol layer. Switches inspect data packets as they are received, determine the source and destination device of that packet, and forward that packet appropriately.

<sup>4</sup> Firewalls protect a network from unauthorized access. Firewalls may be hardware devices, software programs, or a combination of the two. A firewall typically guards an internal network against unauthorized access from the outside; however, firewalls may also be configured to limit access to outside from internal users.

<sup>5</sup> Encryption devices perform the task of converting plain text into an unreadable form and vice versa, in order to create secure communications.

<sup>6</sup> IDS is a security countermeasure that monitors the network for signs of intruders.

---

electronic information assets, failure to secure them increases the risk of unauthorized use of sensitive data.

TSA shares information through its WAN or TSANet. The TSANet connects to LANs located throughout the country, including airports, and offices of FSDs. We used two software products: Internet Security Systems' (ISS) Internet Scanner 7.0, and Cisco Security Analyzer 3.3, to perform the vulnerability assessments on selected network routers, switches, servers, and workstations. At the time of our review, TSA was in the process of migrating its workstations to a new operating system. As a result, we performed our vulnerability scans of workstations functioning with the new operating system, which is Microsoft Windows XP Professional based. Upon completion of the assessments, we provided TSA with the technical reports detailing the specific vulnerabilities detected on each network device and the actions required for remediation.

The audit was conducted from December 2004 through March 2005. See Appendix A for our purpose, scope, and methodology.

## Results of Audit

### **TSA Does Not Have a Comprehensive Network Security Testing Program**

TSA does not have a comprehensive security testing program in place to ensure the integrity of its TSANet. Our review of TSA's vulnerability assessment results confirmed that TSA's contractor performs vulnerability scanning of [REDACTED] network devices monthly. However, TSA does not conduct other forms of testing, such as penetration testing and password analysis. In addition, TSA's draft policy for security testing is incomplete, as the policy only requires vulnerability scanning of all devices connected to the TSANet and does not require that other forms of testing be performed periodically. Security vulnerabilities continue to exist because TSA has not implemented a comprehensive testing program to identify obsolete software versions or applicable patches on its network devices.

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to perform periodic testing to evaluate the effectiveness of security controls. In addition, National Institute of Standards and Technology (NIST) Special Publication 800-42 (*Guideline on Network Security Testing*) recommends that organizations establish a testing program and conduct routine security testing to verify that systems

---

have been configured correctly with the appropriate security resources and in agreement with established policies.

Without performing routine security testing, TSA cannot ensure that the security controls developed and implemented are working as intended or that the sensitive data processed and stored on its network is protected from unauthorized accesses and potential misuse. Security testing can lead to the discovery of potential vulnerabilities and reduce the likelihood of systems being compromised by identifying counter measures and applicable patches for the vulnerabilities discovered. See Appendix C for NIST's recommended routine testing schedule.

### **Recommendation**

We recommend that the Assistant Secretary of Homeland Security for TSA direct the TSA Chief Information Officer (CIO) to:

1. Implement a security testing program for TSANet (including the LANs connected to it) as recommended by NIST 800-42 to include periodic network scanning, vulnerability scanning, penetration testing, password analysis, and war driving.

### **Management Comments and OIG Analysis**

TSA agreed with our recommendation. TSA has begun to implement a security testing and evaluation program. The program will establish testing schedules and will also ensure that adequate security testing is performed.

We agree that the steps that TSA has taken, and plans to take, satisfy this recommendation.

## **TSA Needs Further Improvements To Secure Its Network**

While TSA has made progress in securing its network by strengthening the security configurations of its network devices, TSA can make additional improvements by establishing detailed configuration procedures, develop a patch management policy, implementing a strong password policy, and securely configure its routers. Since TSA has strengthened the security configurations on its servers and workstations, we detected significantly fewer security vulnerabilities compared to the



---

vulnerability assessment results reported in a prior OIG audit report.<sup>7</sup> To assess the security of TSA's network, we interviewed information technology personnel at TSA Headquarters, [REDACTED]; performed vulnerability scans at three TSA locations (TSA Headquarters, St. Louis Hosting Center, and St. Louis' Office of FSD) using ISS Internet Scanner software; and reviewed router configuration files using Cisco Security Analyzer.

In assessing the effectiveness of system controls, we identified several high and medium risk vulnerabilities that could be exploited to gain inappropriate access to TSA sensitive information systems and resources.<sup>8</sup> TSA has several hundred LANs - the scans that we performed represent only a sample of the entire TSANet network. Without processes in place to ensure that all material vulnerabilities are identified and reviewed, management cannot ensure that its network - and the data that resides on it - is secure.

### **Strengthening Configuration Management Process Can Improve Security**

TSA does not have a management approved or documented configuration management process and has not established detailed configuration procedures to ensure that network devices are appropriately secured.<sup>9</sup> Configuration procedures can be used to establish management-approved standard configuration and security settings for each type of device, which leads to improved network security.

The results of our ISS scans indicate that TSA has strengthened the security configuration because we identified fewer security vulnerabilities on its servers and workstations. We identified security vulnerabilities on two network printers that could be exploited to gain unauthorized access to TSANet. Our review of the December 2004 vulnerability assessment results performed by the TSA contractor identified these security vulnerabilities but they had not been remediated at the time of our vulnerability assessment in February 2005. The vulnerabilities discovered are attributed primarily to inadequate [REDACTED] configurations. Network printers, which are often not recognized as potential security exposures, can be exploited for DoS attacks. Administrative access to

---

<sup>7</sup> *DHS Needs to Strengthen Controls For Remote Access to Its Systems and Data*, November 2004 (OIG-05-03).

<sup>8</sup> See Appendix D for the number of high and medium risk vulnerabilities identified by location.

<sup>9</sup> Configuration management is the control and documentation of changes made to a system's hardware and software.

---

most networked printers is not password protected by default. Therefore, network printers must be configured as other networked devices prior to installing them on a network. Specifically:

- [REDACTED] This vulnerability may allow attackers unauthorized access to TSA's networks.
- [REDACTED], which are vulnerable to a wide range of attacks, [REDACTED] These vulnerabilities may allow an attacker to gain unauthorized access to TSA networks.
- A user could access the [REDACTED] An attacker could access sensitive information through default accounts or easily-guessed passwords.
- The network printers [REDACTED] This vulnerability allows anyone [REDACTED] the ability to obtain [REDACTED] information about the system, [REDACTED]

In addition, TSA had a list of accounts on two workstations that could be accessed without requiring identification and authentication. This condition may allow an attacker to obtain account names that could be used to mount further attacks on the network.

FISMA requires federal agencies to develop, document, and implement policies and procedures which ensure compliance with the minimally acceptable system configuration requirements determined by the agency. NIST recommends that agencies develop standardized configurations to reduce the labor involved in identifying, testing, and applying security patches too. DHS has developed configuration guidelines, which is a set of procedures to ensure a minimum baseline of security when installing or configuring network devices, such as Microsoft Windows XP, Windows 2000, and Cisco routers.

[REDACTED]

---

Configured devices that are not secure could make a network vulnerable to internal or external threats, such as DoS attacks. Since networks provide the entry point for access to data, failure to secure them increases the risk of unauthorized access and use of sensitive data. Networks operating without a standard configuration increase the risk that security controls protecting networks could be circumvented. Furthermore, standardized configurations encourage a higher level of consistency by providing administrators with specific instructions on how to implement controls and configure network devices in accordance with agency policies.

### **Improvement of the Patch Management Process Can Reduce Security Vulnerabilities**

While TSA has established a centralized patch management process, our scan results revealed that this process needs improvement.<sup>13</sup> In addition, TSA has not developed its own patch management policy. Instead, TSA relies on the patch management procedures developed by the contractor responsible for its network management. Unpatched network devices may expose TSA's network to [REDACTED]. TSA can strengthen its patch management process by developing a documented policy to ensure that security patches are appropriately identified and applied to mitigate vulnerabilities on all network devices.<sup>15</sup> For example, we identified the following vulnerabilities that are related to missing security patches which were issued in 2003 and 2004:

- [REDACTED]
- [REDACTED] A remote attacker could exploit this vulnerability to [REDACTED]

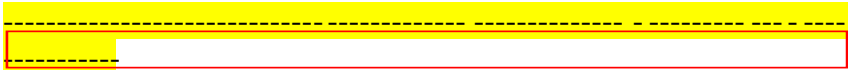
---

<sup>13</sup> Patch management, which is a component of configuration management, is a critical process used to mitigate security vulnerabilities that have been identified.

[REDACTED]

<sup>15</sup> A patch (sometimes called a "fix") is a repair job for a piece of programming. System patches are usually released to: (a) fix faults, correct performance or functionality problems in an application or operating system; (b) alter functionality or to address a new security threat; and, (c) change or modify the software configuration to make it less susceptible to attacks and more secure.

---



NIST recommends that agencies have an explicit and documented patching and vulnerability policy as well as a systematic, accountable, and documented set of processes and procedures for handling patches. The policy should specify what techniques an agency will use to monitor for new patches and vulnerabilities and which personnel will be responsible for such monitoring. An agency's patching process should define a method for deciding which systems get patched and which patches get installed first. It should also include a methodology for testing and safely installing patches.

Without a documented policy and an effective patch management process, TSA cannot ensure that all security vulnerabilities have been mitigated before malicious users exploit these vulnerabilities. Applying security patches is critical for securing TSANet and protects sensitive data from unauthorized access, manipulation, and misuse.

### **Further Improvements Can Be Made in User Account and Password Management**

TSA's draft password policy does not comply with DHS' requirements for strong passwords. Furthermore, TSA's password policy has been in draft since 2004 and has yet to be approved by TSA management. DHS has developed a set of guidelines in its DHS Handbook to implement passwords that restrict access to authorized users only. Specifically, TSA's password policy lacks the following required provisions:

- Passwords shall not contain any two identical consecutive characters (example: 22apples, 14588904).
- Passwords shall contain no more than three identical consecutive characters in any position from the previous password.
- Passwords shall not contain any simple pattern of letters or numbers (example: xyz12345, qwertyui).
- Passwords shall not be any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string (example: 99xyz123, nothing2).

In addition, multiple users shared the passwords of a firewall administrator as well as an IDS administrator account. The DHS Handbook prohibits the sharing of user accounts and passwords.

---

In November 2004, we reported that [REDACTED].<sup>16</sup> The current assessment results reveal that TSA has made significant improvements in user account and password management. We did not identify any user account or password related security vulnerabilities as a result of our scans of selected network devices.

Without a fully developed password policy, user accounts and passwords on the TSANet may not be effective to control access to TSA sensitive data. Passwords are important - they are often the first lines of defense against hackers or insiders who may be trying to obtain unauthorized access to a computer system. SANS Institute recommends that the implementation of a strong password policy is the best and most appropriate defense against security vulnerabilities that are related to compromised passwords.

### **Routers Need To Be Securely Configured**

TSA does not securely configure all of its routers to prevent unauthorized access to its networks. Properly configured routers only permit authorized network service requests and deny unauthorized ones.

Our review of the start-up and running configurations on six TSA routers identified five high risk and seven medium risk weaknesses that may lead to undetected or unauthorized access to the TSA network.<sup>17</sup> For example:

- Five occurrences of a [REDACTED] on five routers.<sup>18</sup> [REDACTED]
- Four occurrences of an [REDACTED] on four routers. The risks that unauthorized users may gain access to the routers or the networks increases when routers [REDACTED].

---

<sup>16</sup> *DHS Needs to Strengthen Controls For Remote Access to Its Systems and Data*, dated November 2004 (OIG-05-03).

<sup>17</sup> The startup configuration is the initial settings and parameters that were used when the network device was started. Since settings and parameters can be changed once a device is operating, the running configuration is the

[REDACTED]

- 
- One occurrence of the [REDACTED] on one router. Unauthorized users may gain undetected access to the routers and monitor TSA networks [REDACTED].

There is no assurance that TSA can prevent unauthorized users from connecting to its networks since all routers are not securely configured. In addition, the TSA cannot ensure that only legitimate users can access the network resources.

### **Recommendation**

We recommend that the Assistant Secretary of Homeland Security for TSA direct the CIO to:

2. Develop, update, and implement management approved policies and procedures for configuration management, standard configuration of network devices, patch management, and passwords, as required by DHS Policy and DHS Handbook. All draft policies and procedures should be promptly approved by TSA management, communicated to all employees, and updated as necessary. All high and medium vulnerabilities that are identified should be addressed and corrected.

### **Management Comments and OIG Analysis**

TSA agreed with our recommendation. TSA has recently formalized and approved IT policies related to configuration management, configuration of network devices and patch management. TSA has also adopted the DHS password policy. TSA will ensure that all vulnerabilities identified in the report are addressed. TSA is also exploring the purchase of an automated tool to assist in vulnerability analysis and patch and risk management. Pilot testing of the tool is expected to begin in August 2005.

We agree that the steps that TSA has taken, and plans to take, satisfy this recommendation.

## **Audit Trails Are Not Regularly Reviewed and Maintained**

TSA does not ensure that audit trails on all network devices are regularly reviewed and maintained to ensure that only authorized activity occurs on the network. Audit trails can track the identity of each user attempting to access the network device, the time and date of access, and time of log off. In addition, audit trails can capture all activities performed during a

---

session and can specifically identify those activities that have the potential to modify, bypass, or negate the system's security safeguards.

TSA's draft policy requires that audit trail data be recorded for each user on all network devices. In addition, the draft policy requires that audit trails be regularly reviewed. However, the policy has not been approved by TSA management. We determined that, due to management decision,

[REDACTED]

[REDACTED] by the contractor responsible for network management.

DHS policy requires that audit trails be reviewed at least once a week. Without prompt and appropriate review and responses to security events or incidents, violations could occur continuously and cause damage to an entity's resources without detection. As a result, increased risks exist that TSA may not detect unauthorized activity or determine the users who are responsible.

### **Recommendation**

We recommend that the Assistant Secretary of Homeland Security for TSA direct the CIO to:

3. Develop, update, and implement management approved policies and procedures to ensure audit trails are recorded and reviewed regularly.

### **Management Comments and OIG Analysis**

TSA agreed with our recommendation. TSA recently formalized and approved the audit trail policy. TSA has requested that the contractor responsible for network management follow TSA's audit trail policy, which requires weekly reviews of audit trails. TSA will also review audit trails using the vulnerability tool that TSA is pilot testing in August 2005.

We agree that the steps that TSA has taken, and plans to take, satisfy this recommendation.

## **Contingency Plan Has Not Been Completed**

The TSANet contingency plan has not been completed. TSA has taken actions, as part of its current ongoing certification and accreditation process of TSANet, to develop various security supporting documents,

---

including the contingency plan, and expects to have the plan completed by July 2005. Contingency planning is designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of an emergency, system failure, or disaster.

Office of Management and Budget Circular A-130 Appendix III requires that contingency plans be developed and tested periodically. FISMA requires that agencies' information security programs include plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency. DHS also requires the contingency plans be developed and tested annually. Testing of contingency plans is performed to validate specific aspects of the plan, policies, procedures, systems, and facilities that will be used in the event of an emergency. Testing the plan is also a training exercise to prepare recovery personnel for plan activation, which can improve plan effectiveness and overall agency preparedness.

When the contingency plan is not documented, even relatively minor interruptions can result in the lost of sensitive or mission-critical data. Since TSA's contingency plan is only in draft, TSA cannot ensure that it will be able to promptly recover essential operations if an unexpected interruption occurs.

### **Recommendation**

We recommend that the Assistant Secretary of Homeland Security for TSA direct the CIO to:

4. Develop and test, at least annually, the contingency plan for all systems.

### **Management Comments and OIG Analysis**

TSA agreed with our recommendation. TSA is in the process of developing and testing contingency plans as part of the certification and accreditation of all of its systems.

We agree that the steps that TSA has taken, and plans to take, satisfy this recommendation.



## Purpose, Scope, and Methodology

The objective of this audit was to determine whether TSA had implemented adequate controls for protecting its TSANet. Specifically, we determined whether: (1) TSA had developed adequate policies and procedures for standard configurations, patch and vulnerability management processes, reviewing audit trails, performing periodic network testing, identification and authentication mechanisms, and deploying anti-virus software; (2) the network administration processes were adequate; (3) adequate security controls were implemented on firewalls, IDS, encryption devices, routers, switches, servers, and workstations; and (4) adequate physical security controls had been established to restrict access to network resources.

To accomplish our audit, we interviewed personnel at TSA Headquarters, [REDACTED]. In addition, we reviewed and evaluated DHS and TSA security policies, procedures, and other appropriate documentation. During the audit, we used a software tool (ISS Internet Scanner) to detect and analyze vulnerabilities on servers, workstations, and switches and another tool (Cisco Security Analyzer) to analyze vulnerabilities on routers in order to evaluate the effectiveness of controls implemented on TSA devices. Upon completion of the assessments, we provided TSA the technical reports detailing the specific vulnerabilities detected on their network devices and the actions needed for remediation.

We conducted our audit between December 2004 and March 2005 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix F.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General, Office of Information Technology at (202) 254-4100 and Edward G. Coleman, Director, Information Security Audits Division at (202) 254-5444.

Appendix B  
Management Response To Draft Report

Office of the Assistant Secretary

U.S. Department of Homeland Security  
601 South 12th Street  
Arlington, VA 22202-4220

JUL 19 2005



Transportation  
Security  
Administration

INFORMATION

MEMORANDUM FOR: Richard L. Skinner  
Acting Inspector General  
Department of Homeland Security

THROUGH: *UWh, FOR*  
Randy Beardsworth  
Acting Under Secretary  
Border and Transportation Security

FROM: Kenneth S. Kasprisin *Kasprisin*  
Acting Assistant Secretary  
Transportation Security Administration

SUBJECT: TSA response to the Department of Homeland Security  
Office of Inspector General draft report titled "*Improved  
Security Required for Transportation Security  
Administration Networks*" (A-IT-05-002)

This memorandum constitutes the Transportation Security Administration's (TSA) response to the findings and recommendations made in the Department of Homeland Security Office of Inspector General draft report titled "*Improved Security Required for Transportation Security Administration Networks*" (A-IT-05-002).

TSA has implemented several changes since the DHS OIG opened this audit and continues to make significant improvements within its Information Technology Security Offices. The accompanying attachment is TSA's official agency comment on the recommendations raised in the Draft Report, and any other relevant comments on the entire report.

TSA appreciates the OIG's efforts to provide a clear and thorough account of TSA's activities related to this report. TSA looks forward to an ongoing relationship with your office as we work towards identifying and correcting vulnerabilities in our transportation security infrastructure.

Attachment

**TSA Response to DHS OIG Report:**  
**“Improved Security Required for Transportation Security Administration Networks”**

**OIG Recommendation 1:** Implement a security testing program for TSANet (including the LANs connected to it) as recommended by NIST 800-42 to include periodic network scanning, vulnerability scanning, penetration testing, password analysis, and war driving.

**TSA concurs.** TSA has implemented stage one of the Security Testing and Evaluation program (ST&E). This program will establish testing schedules and will also ensure adequate security testing is performed. DHS mandated the use of the Risk Management Systems (RMS) tool which generates test plans based on DHS baseline security requirements. TSA will use this tool and any necessary supplements based on the NIST (National Institute of Standards and Technology) standards, which are mandated by the Office of Management and Budget.

TSA also developed an Audit and Assessments program office led by an Assistant Director. The office will ensure that reviews are performed on a scheduled and ad hoc basis to ensure compliance to existing DHS and TSA policies. Additionally, TSA has performed three ad hoc audits of processes, policies and procedures providing summary reports with recommendations to the TSA Chief Information Officer (CIO) for remediation. In order to measure progress, TSA has generated plan of action and milestones (POA&M) on the findings and they have been uploaded in to the Trusted Agent FISMA (Federal Information Systems Management Act) Tool (TAFT).

In addition to the recent changes TSA has made, the Agency also continues to perform monthly scans of the enterprise through the ITMS (Information Technology Managed Services) contractor Unisys. There have also been several ad hoc scans providing results that have generated POA&M's [REDACTED]

**OIG Recommendation 2:** Develop, update, and implement management approved policies and procedures for configuration management, standard configuration of network devices, patch management, and passwords, as required by DHS policy and DHS Handbook. All draft policies and procedures should be promptly approved by TSA management, communicated to all employees, and updated as necessary. All high and medium vulnerabilities that are identified should be addressed and corrected.

**TSA concurs.** TSA has recently formalized and approved IT policies related to configuration management, configuration of network devices, and patch management. For further reference, these policies are a part of TSA's 1400A policy series, and DHS' 4300A policy series. Additionally, the Agency has also adopted the DHS password policy. There are known vulnerabilities with legacy

applications that do not implement strong password requirements. These risks have been adequately assumed by the Designated Accrediting Authority (DAA) and are a portion of the residual risk assumption. These are documented in the risk assumption letters and will be further documented as TSA performs full certification and accreditation (C&A) on each system.

TSA has addressed vulnerabilities by taking steps to work with several vendors to strengthen security on all levels of the enterprise. Recent tests with the Cisco Auditor tool provided results that will generate POA&M's for remediation of vulnerabilities. Some of the remedial activities will require significant funding and will be addressed in TSA's follow on contract with Unisys referred to as the "Bridge" contract. Also contained within the Bridge contract will be requirements to secure vulnerabilities presented in this audit. TSA is also looking to purchase a vulnerability tool for visibility into patch management, vulnerabilities and the risk management areas. Pilot testing will likely begin in the summer of 2005 with potential implementation to follow. The tool will provide full visibility into configurations and other weaknesses.

**OIG Recommendation 3: Develop, update, and implement management approved policies and procedures to ensure audit trails are recorded and reviewed regularly.**

**TSA concurs.** TSA has requested that Unisys correct the audit trail process in the follow on Bridge contract between TSA and Unisys. However, there are significant costs associated with this requirement due to storage requirements. TSA will also review audit trails as part of the vulnerability tool that the Agency is implementing through the pilot testing described in TSA's response under the DHS OIG's recommendation one above.

**OIG Recommendation 4: Develop and test, at least annually, the contingency plan for all systems.**

**TSA concurs.** TSA is undergoing the massive effort to certify and accredit all 107 systems listed in the system inventory throughout FY06, if appropriately funded. A portion of this C&A effort is the collection of all FIPS 199's (Data Categorization Standards) and Contingency Plans as mandated by Federal Information Security Management Act (FISMA).

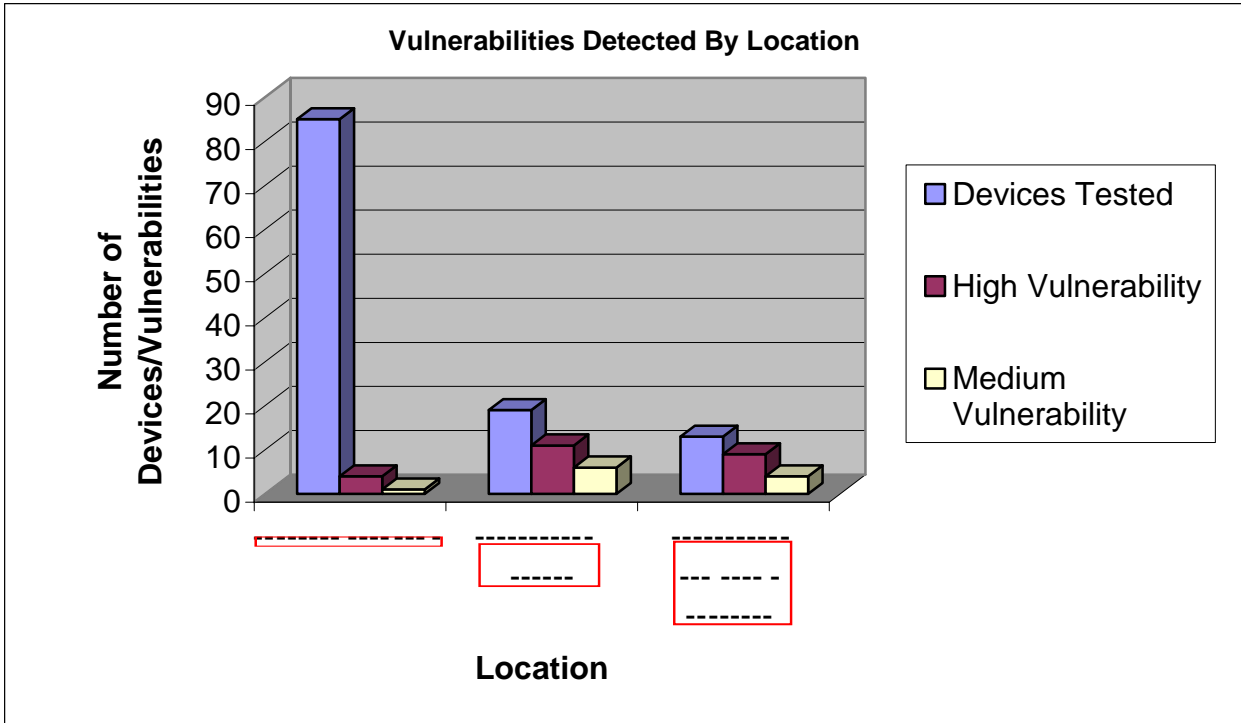
Based on the "Vulnerabilities Detected by Location" that the OIG notes in the report, TSA will work to evaluate and respond to the vulnerabilities identified. Once reviewed, TSA will follow-up with OIG to determine if any additional measures are needed.

TSA is also working through DHS Critical Infrastructure Program, Project Matrix Step 1 and will likely be completed by fall of 2005. This program will help TSA develop critical system planning, which will include annual testing, and will be bolstered by the contingency plans for each system.

Appendix C  
 NIST's Recommended Testing Schedule

Test Type	Frequency For Critical Systems	Frequency For Non-Critical Systems	Benefit
<b>Network Scanning</b>	Continuously to Quarterly	Semi-Annually	<ul style="list-style-type: none"> <li>▪ Enumerates the network structure and determines the set of active hosts, and associated software</li> <li>▪ Identifies unauthorized hosts connected to a network</li> <li>▪ Identifies open ports</li> <li>▪ Identifies unauthorized services</li> </ul>
<b>Vulnerability Scanning</b>	Quarterly or bi-monthly (more often for certain high risk systems), when the vulnerability database is updated	Semi-Annually	<ul style="list-style-type: none"> <li>▪ Enumerates the network structure and determines the set of active hosts, and associated software</li> <li>▪ Identifies a target set of computers to focus vulnerability analysis</li> <li>▪ Identifies potential vulnerabilities on the target set</li> <li>▪ Validates that operating systems and major applications are up to date with security patches and software versions</li> </ul>
<b>Penetration Testing</b>	Annually	Annually	<ul style="list-style-type: none"> <li>▪ Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred</li> <li>▪ Tests IT staff's response to perceived security incidents and their knowledge of and implementation of the organization's security policy and system's security requirements</li> </ul>
<b>Password Analysis</b>	Continuously to same frequency as password expiration policy	Same frequency as password expiration policy	<ul style="list-style-type: none"> <li>▪ Verifies that the policy is effective in producing passwords that are more or less difficult to break</li> <li>▪ Verifies that users select passwords that are compliant with the organization's security policy</li> </ul>
<b>Log Review</b>	Daily for critical systems (e.g., firewalls)	Weekly	<ul style="list-style-type: none"> <li>▪ Validates that the system is operating according to policies</li> </ul>
<b>Virus Detection</b>	Weekly or as required	Weekly or as required	<ul style="list-style-type: none"> <li>▪ Detects and deletes viruses before successful installation on the system</li> </ul>

Appendix D  
Vulnerabilities Detected By Location



Location	Devices Tested <sup>1</sup>	High Vulnerability	Medium Vulnerability
[Redacted]	85	4	1
[Redacted]	19	11	6
[Redacted]	13	9	4
<b>Total</b>	<b>117</b>	<b>24</b>	<b>11</b>

<sup>1</sup> Devices tested include servers, workstations, routers, switches, and printers.

**Information Security Audits Division**

Edward G. Coleman, Director

Jeff Arman, Audit Manager

Chiu-Tong Tsang, Audit Team Leader

Benita Holliman, Auditor

Evan Portelos, Associate

William Matthews, Referencer

**Advanced Technology Division**

Jim Lantzy, Director

Chris Hablas, Senior Security Engineer

**Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Executive Secretariat  
General Counsel  
Border and Transportation Security, Under Secretary  
Chief Information Officer  
Chief Information Security Officer  
Public Affairs  
Legislative Affairs  
Office of Security  
TSA, Assistant Secretary  
TSA, Chief Information Officer  
TSA, Audit Liaison  
Director, Departmental GAO/OIG Liaison Office  
Director, Compliance and Oversight Program, Office of CIO  
Chief Information Officer Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees, as appropriate





### **Additional Information and Copies**

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at [www.dhs.gov/oig](http://www.dhs.gov/oig).

### **OIG Hotline**

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov). The OIG seeks to protect the identity of each writer and caller.