DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improved Security Required for DHS 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-06-05 **November 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 DHS. It is based on interviews with DHS officials, direct observations, technical scans, and a review of applicable documents.

The recommendation herein has been developed to the best knowledge available to our office, and has 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
DHS	Department of Homeland Security
IDS	Intrusion Detection System
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
SOC	Security Operations Center
TSA	Transportation Security Administration
VAT	Vulnerability Assessment Team

Executive Summary

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

Our objective was to determine whether DHS and its organizational components have implemented adequate controls to protect its networks. We interviewed DHS personnel, reviewed policies and procedures, and conducted vulnerability assessments for select network devices at four DHS organizational components: U.S. Customs and Border Protection (CBP), United States Coast Guard (Coast Guard), Transportation Security Administration (TSA), and, United States Secret Service (Secret Service). Our results were summarized in separate audit reports with findings and recommendations issued to each component.

The four components reviewed are taking actions to secure their networks. Some vulnerability assessments are being performed on all or parts of the components' network devices (for example servers and workstations). CBP and the Secret Service have each performed a penetration test on their networks in previous years. TSA and the Secret Service are migrating to a more secure operating environment which has less vulnerabilities. Three of the components - CBP, TSA, and Secret Service - have implemented a centralized patch management process, which helps to ensure that all devices across the network are properly patched.

While progress has been made and efforts by the organizational components continue to improve security, specific areas need attention. The DHS Chief Information Officer (CIO) has not developed a department-wide testing program to ensure that the necessary controls over all of its networks are adequate and effective. In addition, the components have not completely implemented DHS policies and procedures or processes that address security testing, monitoring network

activities with audit trails, configuration and patch management, and contingency planning.

Security controls must be improved in order for DHS to provide adequate and effective security over its networks. Our vulnerability assessments at the components identified security concerns resulting from inadequate password controls, missing critical patches, vulnerable network devices, and weaknesses in configuration management. These security concerns provide increased potential for unauthorized access to DHS resources and data.

We made a recommendation to assist DHS more effectively secure its networks. Both effective network management and security controls are needed in order to protect the confidentiality, integrity, and availability of sensitive information stored and processed on DHS information systems.

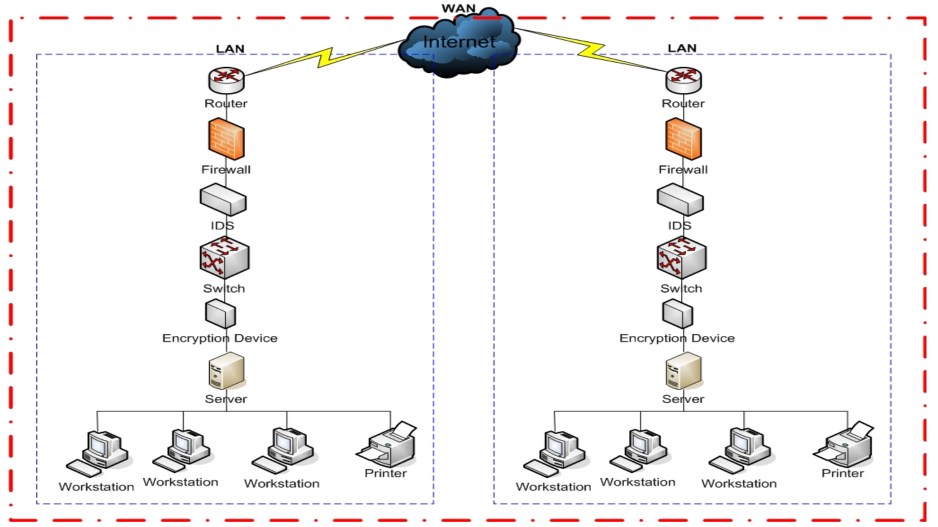
In response to our draft report, DHS agreed and has already taken steps to implement the recommendation. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

There are many advantages associated with using computer networks to share information, not the least of which for government agencies is to dramatically boost productivity, efficiency, and competitiveness. 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: it must be evaluated from all points of entry into the network such as 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 which 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. Network devices include servers, workstations, and printers (used to create, process, maintain, and view information); routers[1] and switches[2] (used to communicate information); firewalls[3] and encryption devices[4] (used to protect information being transported); and intrusion detection systems (IDS)[5] (used to monitor and analyze network events). Figure 1 is an illustration of a typical network.

Figure 1- Example of a Typical Network



Since sensitive data is stored on and transmitted along wide area networks, effectively securing networks is essential to protect sensitive data from unauthorized access, manipulation, or misuse. Improperly configured network services expose a network to internal or external threats, such as hackers, cyber-terrorist groups, as well as denial of service attacks. Further, as networks provide the entry point for access to electronic information assets, failure to secure them increases the risk of unauthorized use of sensitive data.

[1] 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.

[2] 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.

[3] 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 by internal users.

[4] Encryption devices perform the task of converting plain text into an unreadable form and vice versa, in order to create secure communications.

[5] IDS is a security countermeasure that monitors the network for signs of intruders.

DHS Sensitive Systems Policy Publication 4300A (DHS Policy) provides direction to DHS' components regarding the management and protection of sensitive systems. In addition, the policy outlines management, operational, and technical controls necessary to ensure confidentiality, integrity, availability, and authenticity within the DHS information technology infrastructure and operations. Additionally, the department developed the DHS Sensitive Systems Handbook (DHS Handbook) to provide components with specific procedures and techniques for implementing the requirements of the policy.

This audit was conducted from December 2004 through March 2005 at four DHS components: CBP, TSA, the Coast Guard, and the Secret Service. See Appendix A for our purpose, scope, and methodology.

Results of Audit

DHS Needs to Implement A Network Security Testing Program

DHS requires a comprehensive department-wide testing program to evaluate and ensure the effectiveness of security measures and controls implemented on its networks. A testing program should be established to ensure that vulnerability assessments are an on-going, effective process that provides assessment coverage for the entire DHS network.

DHS issued policy and procedures to implement a department-wide vulnerability assessment program as part of the DHS Handbook in July 2004 (*Attachment O – Vulnerability Assessment Program*). Further, DHS would establish a Vulnerability Assessment Team (VAT) to provide vulnerability assessment services to the department's organizational components. As described in the DHS Handbook, the program's goal was to provide 100% vulnerability assessment coverage for all DHS systems (including networks) annually. Vulnerability assessments would be a four-phase process: reconnaissance, scanning, penetration testing, and reporting. The program would rely on DHS components to conduct their own assessments and report results to the DHS VAT. Where the capability to perform vulnerability assessments did not exist, the DHS VAT would perform these assessments for the components. The DHS VAT would conduct an ongoing, external assessment program for all peripheral connections to DHS networks. Annually, the DHS VAT would provide at least one independent vulnerability assessment at each DHS component. In addition, as part of the assessment program, periodic penetration testing would be required. The DHS Computer Security

Incident Response Center (CSIRC) would conduct operational oversight for the DHS VAT under the guidance of the DHS CISO.

However, as of August 2005, the department's Vulnerability Assessment Program, as established in the Attachment, has not been implemented. Furthermore, the DHS VAT has only performed a limited number of vulnerability assessments.

To determine whether DHS and its organizational components have implemented adequate controls to protect its networks, we performed testing at four of the department's organizational components (CBP, Coast Guard, Secret Service, and TSA). The four components covered in this review had not implemented all of the controls needed to ensure that their networks are secure. For example, the components have not implemented the necessary policies and procedures to ensure the security of their networks. In addition, we identified vulnerabilities on network devices at all components tested. The vulnerabilities identified support the fact that DHS should implement a department-wide program to either ensure compliance with established policies and procedures or to independently identify security exposures that jeopardize the security of its networks. While each of the component networks reviewed had varying degrees of network security appropriately established, the following were areas common to each which presented security issues requiring attention.

Comprehensive Network Security Assessments Are Required

The components have not developed policies or procedures to establish and implement their own comprehensive network-testing program. Each of the four components has implemented procedures to perform some measure of vulnerability assessments on all or parts of their networks. However, the component's programs are deficient in the following areas:

- Coast Guard and TSA have not performed other forms of security testing, such as penetration testing, and password analysis.
- Penetration testing was performed at CBP in 2004 and at the Secret Service in 2003; however, both components have yet to decide whether to perform penetration testing in 2005.
- CBP is the only component reviewed that performed periodic password analysis.

The *Federal Information Security Management Act of 2002* requires that federal agencies perform periodic testing to evaluate the effectiveness of security controls. Also, the National Institute of Standards and

Technology (NIST) Special Publication 800-42 (*Guideline for Network Security Testing*) recommends 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. See Appendix D for NIST's recommended routine testing schedule.

Established Security Policies and Procedures Require Implementation

DHS security policies and procedures, as described in the DHS Policy and Handbook, have yet to be implemented by the organizational components. The major elements not yet addressed are audit trail review and maintenance, minimum password length and complexity, and contingency planning.

None of the components reviewed have implemented an adequate procedure for recording, reviewing, and maintaining audit trail information for their networks and network devices. 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.

DHS has developed a set of guidelines in its DHS Handbook to implement passwords that restrict access to authorized users only. However, the password policies at three of four components (CBP, Coast Guard, and TSA) did not comply with DHS' requirements for strong passwords. There were also instances of components allowing the use of shared user accounts and passwords.

Contingency plans for the networks at three of the four components (Coast Guard, Secret Service, and TSA) have either not been developed or tested. DHS policy and the Office of Management and Budget require that contingency plans be developed and the plans tested periodically. In addition, the DHS Handbook specifically requires the testing of contingency plans at a minimum annually.

Network Devices Require Strengthened Security Configurations

We performed vulnerability assessments on a sample of network devices and identified vulnerabilities at all four components reviewed.[6] We noted

[6] See Appendix C for the number of high and medium risk vulnerabilities identified by component.

that the Secret Service and TSA are in the process of migrating to a more secure operating environment [redacted] and found fewer vulnerabilities on devices at these components.

Those areas where security improvements are most needed include configuration management[7], router configurations, patch management[8], and user account and password management. Without procedures in place to ensure that all material vulnerabilities are identified and reviewed, management cannot ensure that its networks - and the data that resides on them - are secure.

In addition, at all four components, many of the [redacted]

We identified vulnerabilities related to configuration management at all four components reviewed. Improperly configured devices could make a network vulnerable to internal or external threats, such as denial of service 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.

We noted vulnerabilities due to missing security patches at all four components even though three of the four components (CBP, TSA, and Secret Service) had established a centralized patch management process. Without an effective documented patch management process, DHS cannot ensure that all security vulnerabilities have been mitigated before malicious users exploit these vulnerabilities.

Our vulnerability scans disclosed weak user account and password administration, [redacted], at three of the four components (CBP, Coast Guard, and Secret Service). These weaknesses are an indication that user accounts and passwords may not be effective to control access to DHS sensitive data.

[7] Configuration management is the control and documentation of the initial settings and changes made to a system's hardware and software.

[8] Patch management, which is a component of configuration management, is a critical process used to mitigate security vulnerabilities that have been identified.

Vulnerabilities in router configurations exist at all four components reviewed. Properly configured routers permit only authorized network service requests and deny unauthorized ones. There is little assurance that components can prevent unauthorized users from connecting to its networks since all routers are not securely configured. In addition, components are unable to ensure that only legitimate users access their network resources.

Conclusion

Security vulnerabilities may continue to exist if DHS does not implement a comprehensive testing program to identify those exposures that place information systems at risk. The organizational components and the DHS CIO share the responsibility for securing all DHS networks. While the DHS CIO is responsible for the oversight and management of the DHS security program, the components, using DHS IT security policies and procedures, are required to develop their own IT security program. The components' security program should include those policies and procedures, including network testing, necessary to effectively secure their information systems. Since DHS' policy and procedures for establishing a network security testing program have not been implemented; without specific DHS policy, the components lack sufficient guidance to implement a comprehensive security testing program.

Without performing routine security testing, DHS cannot ensure that the security controls implemented by the components are working as intended or that the sensitive data processed and stored on its networks is protected from unauthorized access and potential misuse. Security testing also reduces the likelihood of systems being compromised by identifying counter measures for the vulnerabilities discovered.

Recommendation

We recommend that the DHS CIO:

- Implement fully its Vulnerability Assessment Program, or another process, to ensure that all DHS networks are periodically assessed for vulnerabilities, which would include vulnerability assessments and penetration testing.

Management Comments and OIG Analysis

DHS agreed with our recommendation. DHS has established an infrastructure enterprise security program, within the Office of Infrastructure Operations, that is responsible for implementing operational security management for all DHS' computer and network resources. In addition, DHS plans to consolidate all legacy networks into a single DHS core network. This consolidation includes the creation of a DHS Network Operations Center/Security Operations Center (NOC/SOC) to conduct periodic vulnerability assessments and penetration testing. Furthermore, beginning in FY 2006, components will be required to establish component level NOC/SOCs that comply with DHS policy. All component NOC/SOCs will have complementary vulnerability management and assessment capabilities and will be required to report to the DHS NOC/SOC for department-wide analysis and assessments.

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

Purpose, Scope, and Methodology

The objective of this audit was to determine whether DHS and its components had implemented adequate controls for protecting its networks. Specifically, we determined whether: (1) DHS and its components 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, network printers, and workstations; and, (4) adequate physical security controls had been established to restrict access to network resources.

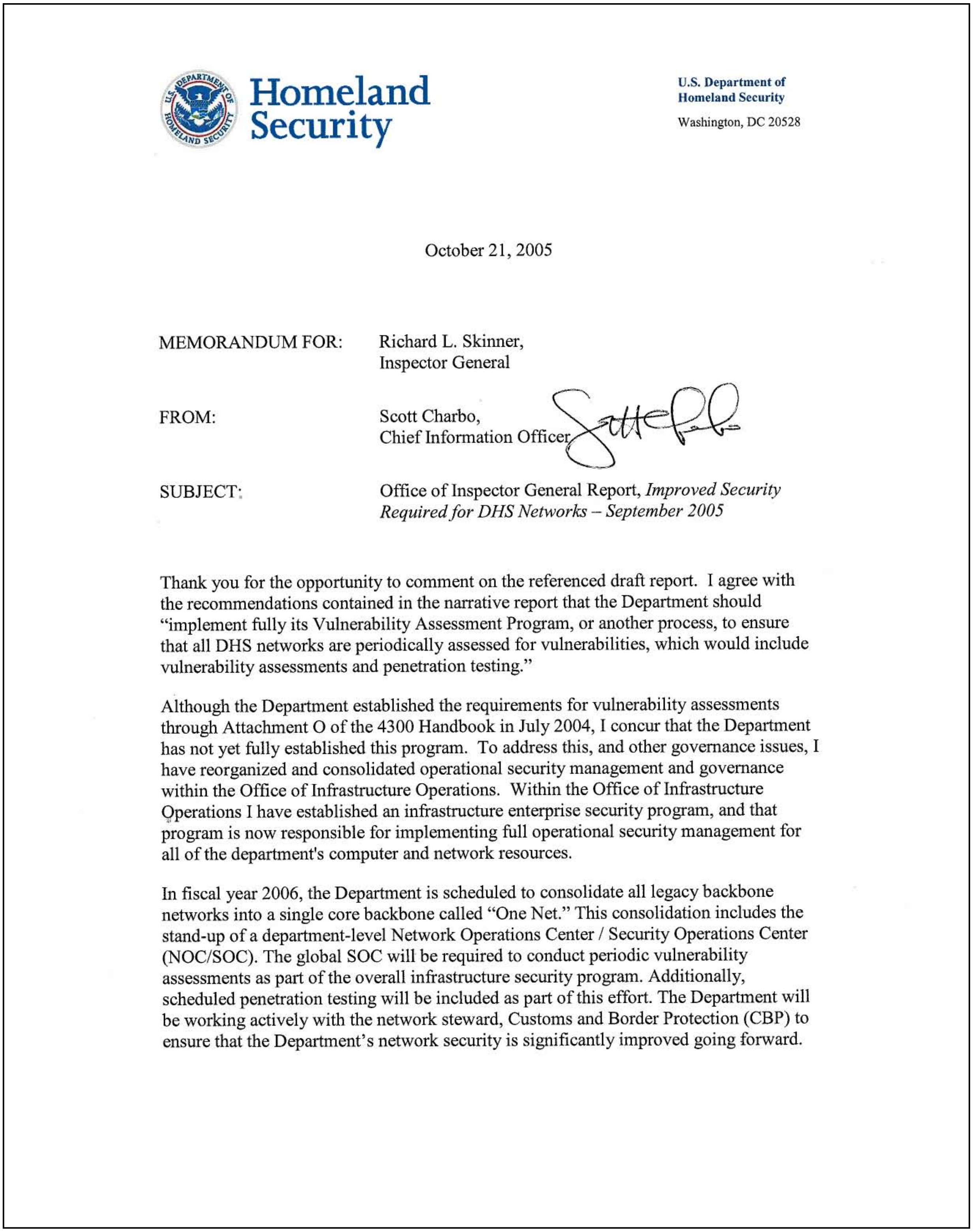
To accomplish our audit, we conducted fieldwork at the following components:

- Transportation Security Administration
- U.S. Customs and Border Protection
- United States Coast Guard
- United States Secret Service

We interviewed personnel at the Office of the Chief Information Officer and the components. In addition, we reviewed and evaluated DHS and component security policies, procedures, and other appropriate documentation. During the audit, we used two software tools (Internet Security Systems' Internet Scanner and Kane Security Analyst) to detect and analyze vulnerabilities on servers, workstations, switches, and network printers and another tool (Cisco Security Analyzer) to analyze vulnerabilities on routers. Upon completion of the assessments, we provided the components 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 E.

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.



Homeland Security

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

October 21, 2005

MEMORANDUM FOR: Richard L. Skinner,
Inspector General

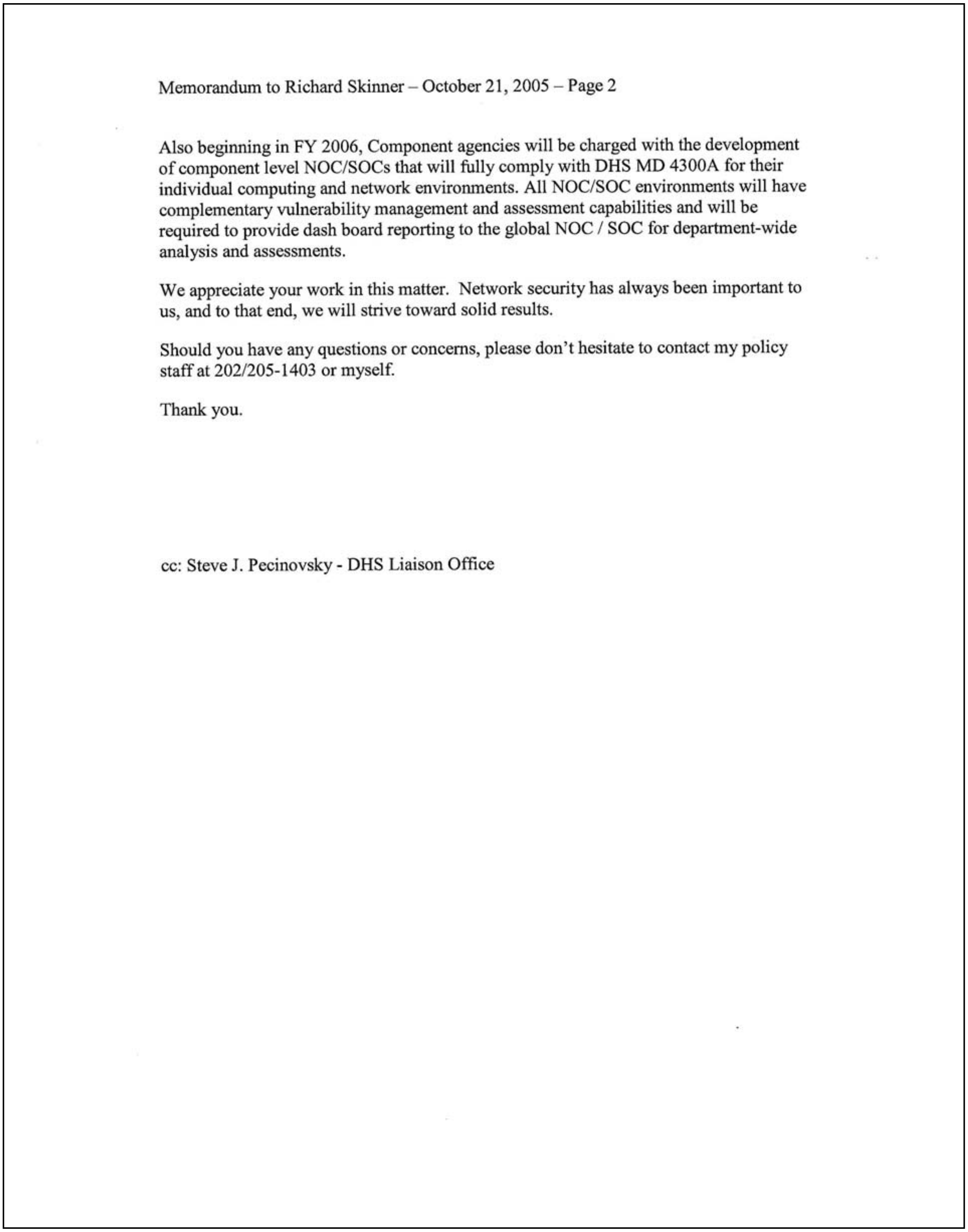
FROM: Scott Charbo,
Chief Information Officer

SUBJECT: Office of Inspector General Report, *Improved Security Required for DHS Networks – September 2005*

Thank you for the opportunity to comment on the referenced draft report. I agree with the recommendations contained in the narrative report that the Department should "implement fully its Vulnerability Assessment Program, or another process, to ensure that all DHS networks are periodically assessed for vulnerabilities, which would include vulnerability assessments and penetration testing."

Although the Department established the requirements for vulnerability assessments through Attachment O of the 4300 Handbook in July 2004, I concur that the Department has not yet fully established this program. To address this, and other governance issues, I have reorganized and consolidated operational security management and governance within the Office of Infrastructure Operations. Within the Office of Infrastructure Operations I have established an infrastructure enterprise security program, and that program is now responsible for implementing full operational security management for all of the department's computer and network resources.

In fiscal year 2006, the Department is scheduled to consolidate all legacy backbone networks into a single core backbone called "One Net." This consolidation includes the stand-up of a department-level Network Operations Center / Security Operations Center (NOC/SOC). The global SOC will be required to conduct periodic vulnerability assessments as part of the overall infrastructure security program. Additionally, scheduled penetration testing will be included as part of this effort. The Department will be working actively with the network steward, Customs and Border Protection (CBP) to ensure that the Department's network security is significantly improved going forward.



Memorandum to Richard Skinner – October 21, 2005 – Page 2

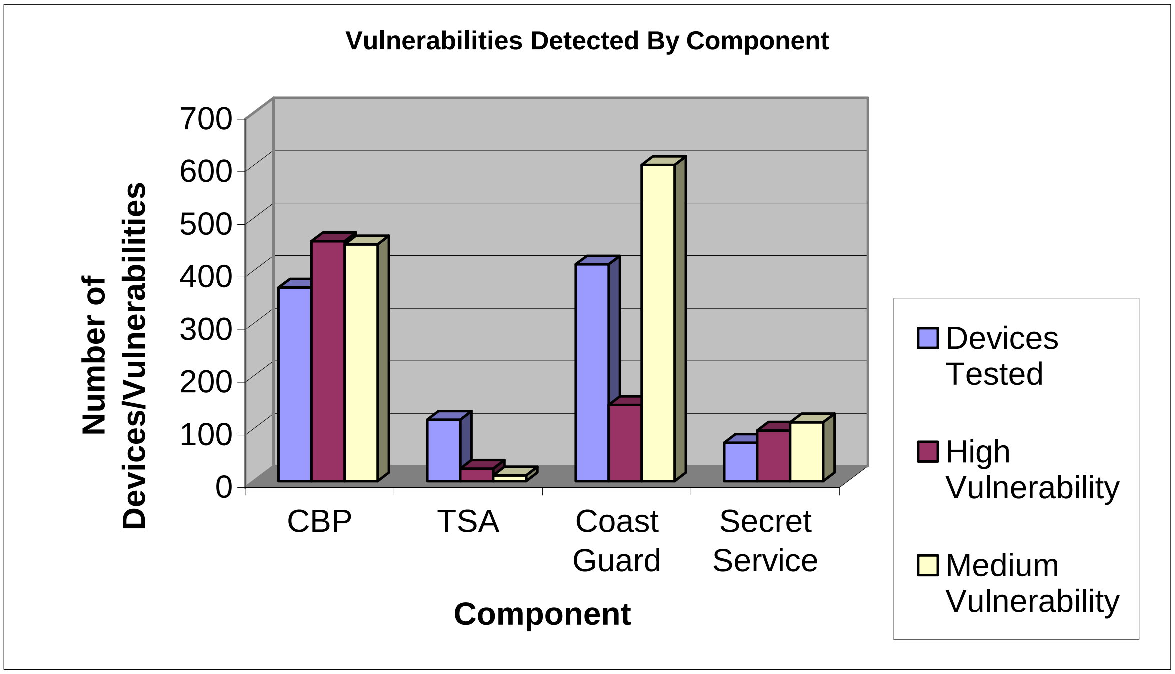
Also beginning in FY 2006, Component agencies will be charged with the development of component level NOC/SOCs that will fully comply with DHS MD 4300A for their individual computing and network environments. All NOC/SOC environments will have complementary vulnerability management and assessment capabilities and will be required to provide dash board reporting to the global NOC / SOC for department-wide analysis and assessments.

We appreciate your work in this matter. Network security has always been important to us, and to that end, we will strive toward solid results.

Should you have any questions or concerns, please don't hesitate to contact my policy staff at 202/205-1403 or myself.

Thank you.

cc: Steve J. Pecinovsky - DHS Liaison Office



Component	Devices Tested [1]	High Vulnerability	Medium Vulnerability
CBP	368	456	450
TSA	117	24	11
Secret Service	73	96	112
Coast Guard	412	145	601
Total	**970**	**721**	**1174**

[1] Devices tested include servers, workstations, switches, and network printers.

Appendix D
NIST's Recommended Testing Schedule

Test Type	Frequency For Critical Systems	Frequency For Non-Critical Systems	Benefit
Network Scanning	Continuously to Quarterly	Semi-Annually	▪ Enumerates the network structure and determines the set of active hosts and associated software ▪ Identifies unauthorized hosts connected to a network ▪ Identifies open ports ▪ Identifies unauthorized services
Vulnerability Scanning	Quarterly or bi-monthly (more often for certain high risk systems), when the vulnerability database is updated	Semi-Annually	▪ Enumerates the network structure and determines the set of active hosts and associated software ▪ Identifies a target set of computers to focus vulnerability analysis ▪ Identifies potential vulnerabilities on the target set ▪ Validates that operating systems and major applications are up-to-date with security patches and software versions
Penetration Testing	Annually	Annually	▪ Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred ▪ Tests IT staff's response to perceived security incidents as well as their knowledge and implementation of the organization's security policy and system's security requirements
Password Analysis	Continuously to same frequency as password expiration policy	Same frequency as password expiration policy	▪ Verifies that the policy is effective in producing passwords that are more or less difficult to break ▪ Verifies that users select passwords that are compliant with the organization's security policy
Log Review	Daily for critical systems (e.g., firewalls)	Weekly	▪ Validates that the system is operating according to policies
Virus Detection	Weekly or as required	Weekly or as required	▪ Detects and deletes viruses before successful installation on the system
War Driving	Continuously to weekly	Semi-annually	▪ Detects unauthorized wireless access points and prevents unauthorized access to a protected network

Information Security Audits Division

Edward G. Coleman, Director
Jeff Arman, Audit Manager
Chiu-Tong Tsang, Audit Team Leader
Benita Holliman, Auditor
Evan Portelos, Associate
Anthony Nicholson, Referencer

Advanced Technology Division

Jim Lantzy, Director
Chris Hablas, Senior Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Executive Secretary
General Counsel
Management, Under Secretary
Chief Security Officer
Chief Information Officer
Chief Information Security Officer
Public Affairs
Legislative Affairs
Director, Departmental GAO/OIG Liaison Office
Director, Compliance and Oversight Program
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.

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. The OIG seeks to protect the identity of each writer and caller.