DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improved Security Required For U.S. Customs and Border Protection 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-05-39 September 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 U.S. Customs and Border Protection (CBP). It is based on interviews with employees and officials of CBP, 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

------	------------------------
------	----------------------------------
CIO	Chief Information Officer
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
-----	-------------------------
IDS	Intrusion Detection System
IP	Internet Protocol
ISS	Internet Security Systems
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
--------	---- -------------------------- - -------------
WAN	Wide Area Network

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

The Office of Inspector General (OIG) 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 U.S. Customs and Border Protection (CBP) 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 objective was to determine whether CBP has implemented adequate controls to protect its networks. CBP shares law enforcement and trade sensitive data through its wide area network (WAN) or Private Internet Protocol (IP) WAN. The Private IP WAN connects to local area networks (LANs) located throughout the country. To address our objective, we: (1) interviewed personnel at the CBP [redacted], (2) reviewed DHS and CBP's policies and procedures, and (3) conducted vulnerability assessments for a select sample of network devices at three CBP locations [redacted].

CBP has not developed adequate policies and procedures or fully implemented processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. In addition, CBP has not implemented the necessary controls to ensure that the data residing on and traveling through its network resources is properly protected.

Security controls must be improved in order for CBP to provide adequate and effective security over its networks. Our vulnerability assessments 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 CBP resources and data.

We made several recommendations to assist CBP 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, CBP agreed and has already taken steps to implement each of the recommendations. CBP'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 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. Network security 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 LAN. A network which connects various LANs dispersed over a wide geographical area is called a WAN. 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]

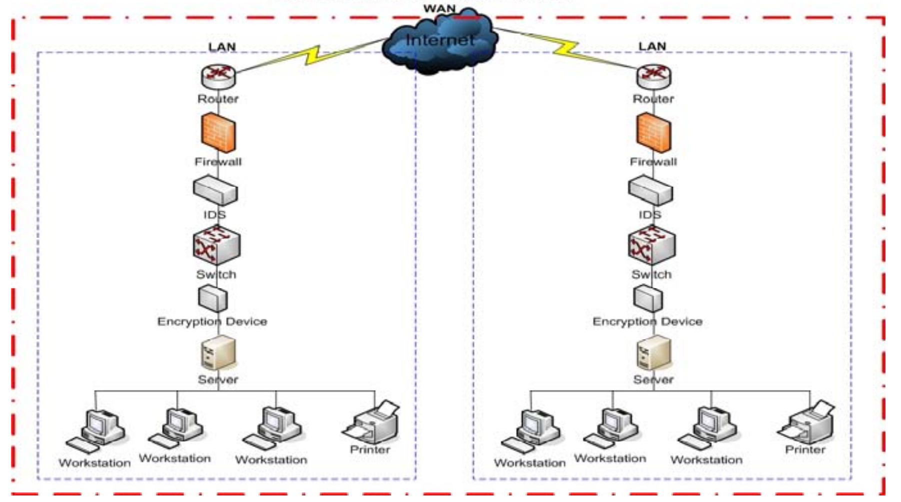
[1] Routers are devices which join multiple networks. Configuration information maintained in the "routing table" allows routers to filter traffic, either incoming or outgoing, based on the Internet Protocol addresses of senders and receivers.

[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.

(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 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.

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

[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.

Results of Audit

CBP Can Improve Network Security with an Enhanced Security Testing Program

CBP can improve the security of its Private IP WAN with an enhanced security testing program. Our review of CBP's testing program confirmed that CBP performed vulnerability assessments (1) on new devices prior to introducing them to the network, (2) on devices that trigger an IDS security alert, and (3) on selected LANs periodically. In addition, CBP performed password analysis to evaluate password length and complexity; and, a penetration test in 2004 to evaluate the effectiveness of controls implemented on its networks. However, CBP personnel indicated that they have yet to decide whether a penetration test would be performed on the Private IP WAN in 2005. Further, CBP's policy for security testing is incomplete because the policy requires vulnerability scanning of new devices connected to the Private IP WAN only but does not require that other forms of testing, such as password analysis and penetration tests, be performed periodically on the entire network.

Our vulnerability assessment revealed that CBP's password analysis was inadequate. We identified accounts ------------------------------------ ------------------------------------ ----------------------------.

The Federal Information Security Management Act of 2002 (FISMA) requires that federal agencies 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 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.

Security vulnerabilities continue to exist because CBP has not implemented a comprehensive testing program to identify obsolete software versions and applicable patches on its network devices. Without an effective security testing program, CBP cannot ensure that the security controls implemented are working as intended or that the sensitive data processed and stored on its network is protected from unauthorized access and potential misuse. Security testing can lead to the discovery of potential vulnerabilities. It reduces 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 Commissioner, U.S. Customs and Border Protection, direct its Chief Information Officer (CIO) to:

1. Improve the security testing program for the Private IP WAN (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

CBP agreed with our recommendation. CBP plans to improve its security testing program as recommended by NIST 800-42 by developing a vulnerability assessment policy, conducting continuous network scanning, and increasing password analysis testing efforts. The program will establish testing schedules and will also ensure that adequate security testing is performed. CBP plans to complete this recommendation by December 31, 2005.

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

CBP Needs Improvements to Secure its Network

CBP has not implemented effective system controls over its network. To assess the security of CBP's network, we interviewed information technology personnel at its ---------------- --------; performed vulnerability scans at three CBP locations ------- ----------------------- ---------------- -------------- ------------------------------------ using ISS Internet Scanner software and Kane Security Analyst; and, reviewed router configuration files using Cisco Security Analyzer. To provide network security and manage its LANs, CBP has established multiple geographical regions. Regional administrators with administrative rights can modify configuration settings on servers, workstations, and network printers.

In assessing the effectiveness of system controls, we performed vulnerability scans on 368 network devices and identified 906 security vulnerabilities that are classified as either high or medium risk[6]. CBP has [redacted] LANs - the scans that we performed represent a sample of its entire Private IP WAN network. One-third (305) of the security vulnerabilities discovered are primarily attributed to inadequate [redacted]. -[redacted], often which are not recognized as potential security exposures, can be exploited for [redacted] 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 Can Improve Security

CBP needs to improve its configuration management process to protect its networks against unauthorized access.[7] While CBP has established a configuration management process, it does not have a centralized process to ensure that all network devices are securely configured throughout its Private IP WAN. For example, regional administrators with administrative rights can modify configuration settings on servers, workstations, and printers that are connected to the LANs. Furthermore, the results of our ISS scans indicate that the configuration procedures developed do not effectively ensure that these devices are securely configured throughout the organization. Specifically:

- Users could access network [redacted] This vulnerability may allow attackers unauthorized access to CBP's networks.
- Outdated versions of the [redacted] This vulnerability may allow an attacker to gain unauthorized access to CBP networks.

[6] See Appendix D for the number of high and medium risk vulnerabilities identified by location.
[7] Configuration management is the control and documentation of changes made to a system's hardware and software.
[redacted]

- A user could access [redacted] This vulnerability could allow an attacker access to sensitive information through default accounts or easily-guessed passwords.
- [redacted], which allows malicious users to change the [redacted]. This vulnerability allows anyone-[redacted] the ability to obtain valuable information about the system, such as information on network devices and current open connections.
- [redacted] This condition may allow an attacker to obtain account names that could be used to mount further attacks on the network.
- [redacted] that is vulnerable to denial of service attacks.

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 also recommends that agencies develop standardized configurations to reduce the labor involved in identifying, testing, and applying security patches. DHS has developed configuration guidelines, which are a set of procedures to ensure a minimum baseline of security when installing or configuring network devices, such as [redacted].

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.

[redacted]

Improvement of the Patch Management Process Can Reduce Security Vulnerabilities

While CBP has established a centralized patch management process, our scan results revealed that the process needs improvement.[11] Unpatched network devices may expose CBP's network to [redacted] CBP can strengthen its patch management process by updating its policy to ensure that security patches[13] are appropriately identified and applied to mitigate vulnerabilities on all network devices. For example, we identified the following vulnerabilities which are due to missing security patches that were issued in 2003 and 2004:

- Patches to eliminate three [redacted] A remote attacker could exploit this vulnerability to [redacted] to gain unauthorized access to [redacted].

- [redacted]

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

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

[redacted]

[13] 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.

[redacted]

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 an effective patch management process, CBP cannot ensure that all security vulnerabilities have been mitigated before malicious users exploit these vulnerabilities. Applying security patches is critical for securing CBP's Private IP WAN and protecting sensitive data from unauthorized access, manipulation, and misuse.

Further Improvements Can Be Made in User Account and Password Management

CBP's password policy does not comply with DHS' requirements for strong passwords. CBP's *"Information Systems Security Policy and Procedures Handbook"*, dated June 22, 2001, requires a minimum password length between six and eight characters; however, DHS requires passwords to be at least eight characters. A revised version of the CBP Handbook - that has not been approved by CBP management - now requires minimum password length of eight characters. DHS has developed a set of guidelines in its DHS Handbook to implement passwords that restrict access to authorized users only. Specifically, CBP's current and revised draft password policy lack the following required provisions:

- 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 (e.g., 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 (e.g., 99xyz123, nothing2).

Our review of account policy settings determined that CBP had weak or inappropriate and inconsistent password configurations on selected [redacted] servers. For example:

- [redacted]

- [redacted]

Finally, we identified the following weaknesses in account and password administration during our vulnerability scans:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

These weaknesses are an indication that user accounts and passwords on LANs across the Private IP WAN may not be effective to control access to CBP 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 the implementation of a strong password policy as the best and most appropriate defense against security vulnerabilities that are related to compromised passwords.

Routers Need To Be Securely Configured

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

Our review of the start-up and running configurations[15] on eight CBP routers identified three high risk and ten medium risk weaknesses that may lead to undetected and unauthorized access to the CBP network. For example:

- There were four occurrences of a [redacted]

[15] 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 settings and parameters that are currently being used for the network device.

[redacted]

- There were 25 occurrences where the [redacted]. Unauthorized users may gain undetected access to the routers and monitor [redacted].
- There were 1,981 occurrences of [redacted] enabled on seven routers. This may allow unauthorized users to intercept sensitive data transmitted over CBP networks.
- There were seven occurrences of [redacted] enabled on seven routers. This may allow malicious users to obtain [redacted] to gain unauthorized access to CBP networks.

There is little assurance that CBP can prevent unauthorized users from connecting to its networks since all routers are not securely configured. In addition, CBP is unable to ensure that only legitimate users can access the network resources.

Recommendations

We recommend that the Commissioner, U.S. Customs and Border Protection, direct its CIO to:

2. Develop, update, and implement policies and procedures to strengthen configuration and patch management processes to ensure that all network devices are uniformly configured and all necessary patches are applied to reduce the risk of system compromise or failure. All high and medium vulnerabilities that are identified should be addressed and corrected.

3. Develop, update, and implement policies and procedures to strengthen user account and password management process, as required by DHS Policy and DHS Handbook.

[redacted]

Management Comments and OIG Analysis

CBP agreed with recommendation 2. CBP plans to refine its patch and vulnerability management processes and implement a comprehensive testing program to identify obsolete software and applicable patches. Furthermore, CBP plans to establish a Security Operation Center to ensure network devices are uniformly configured and provide monitoring and oversight of CBP's patch and management and procedures. CBP plans to complete this recommendation by March 31, 2006.

We agree that the steps that CBP plans to take satisfy this recommendation.

CBP agreed with recommendation 3. CBP indicated that, since the policy enforcement is not allowed on -- ----------------------, they could not enforce DHS password policy until after the migration to -- ---------------- ---------------------------. CBP plans to begin the rollout of -- ---------------- - ------ by the end of calendar year 2005. The full deployment of -- ------- ----------------------------------- is scheduled to be completed by second quarter of fiscal year 2007. Furthermore, CBP is currently evaluating products to enforce DHS password standards on all ---------------. Pending the availability of funding and success in pilot testing, CBP plans to deploy products to enforce DHS password standards on all --------------- by April 1, 2007. In addition, CBP is in the process of migrating to -------- --------------, which allows the enforcement of DHS password policy. Once the migration is completed by March 31, 2007, CBP will implement DHS password policy on all -----------------.

We agree that the response that CBP plans to take begin to satisfy this recommendation. However, CBP did not address whether it will update its policy for password complexity, as required by DHS policy. In addition, the timeline to implement the new platforms should be shortened to minimize unauthorized access to CBP systems.

Audit Trails Are Not Regularly Reviewed or Maintained

CBP does not ensure that audit trails on all network devices are regularly reviewed or maintained to ensure that only authorized activity is occurring 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.

Network administrators at the [redacted] did not consistently use audit trails to monitor network activities. Further, when network activities were monitored, there was no documentation supporting these activities. Specifically, we determined that:

- [redacted]
- [redacted]
- [redacted]

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 the CBP may not detect unauthorized activity or determine the users who are responsible.

Recommendation

We recommend that the Commissioner, U.S. Customs and Border Protection, direct its CIO to:

4. Develop, update, and implement policies and procedures to ensure network device audit trails are reviewed regularly and properly maintained.

Management Comments and OIG Analysis

CBP agreed with our recommendation and is in the process of developing a procedure to ensure audit trails are reviewed regularly. CBP plans to complete this recommendation by September 1, 2005.

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

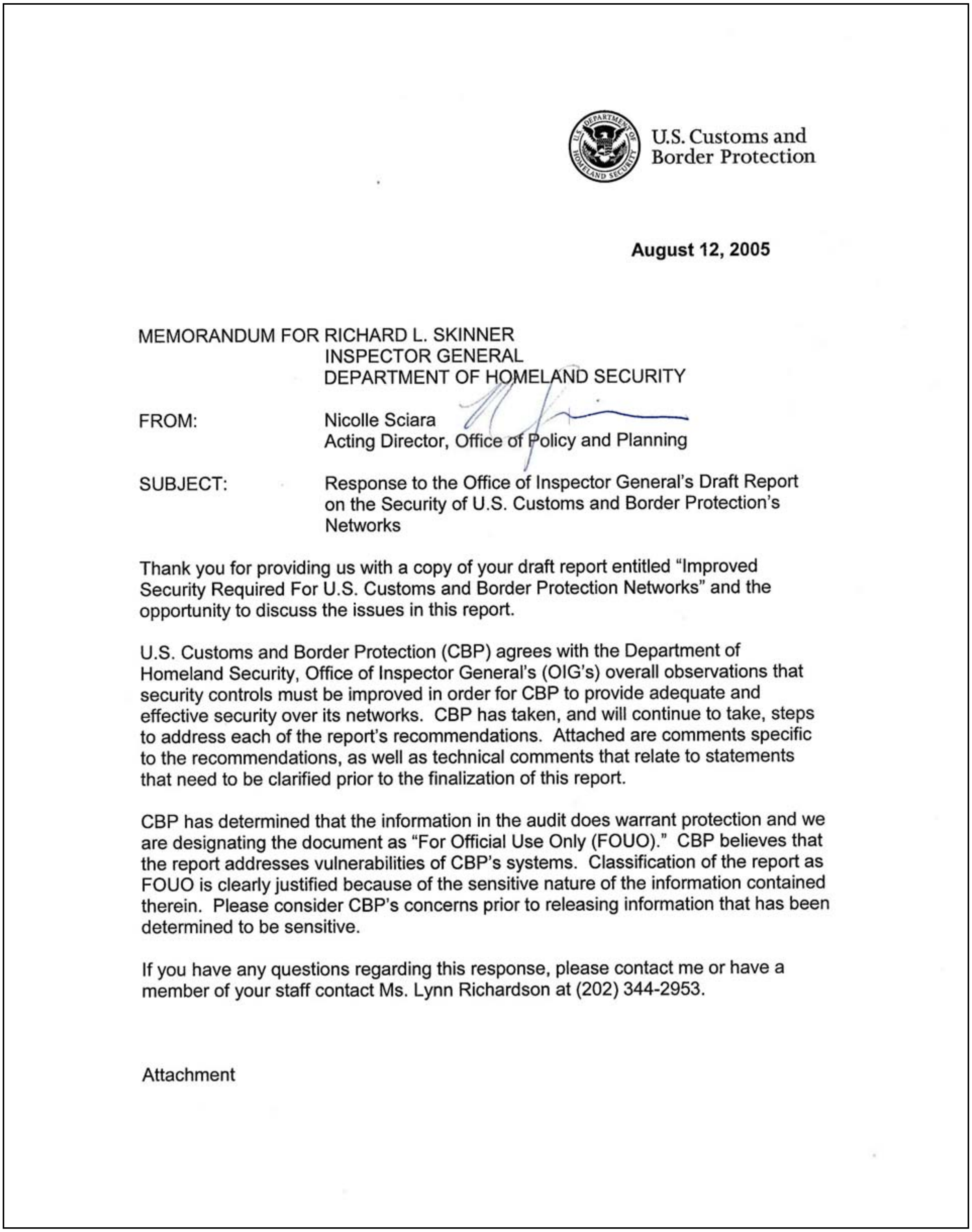
Purpose, Scope, and Methodology

The objective of this audit was to determine whether CBP had implemented adequate controls for protecting its Private IP WAN. Specifically, we determined whether: (1) CBP 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 interviewed personnel at the ----------------------------- . In addition, we reviewed and evaluated DHS and CBP security policies, procedures, and other appropriate documentation. During the audit, we used two software tools (ISS Internet Scanner and Kane Security Analyst) to detect and analyze vulnerabilities on servers, workstations, network printers, and switches as well as another tool (Cisco Security Analyzer) to analyze vulnerabilities on routers in order to evaluate the effectiveness of controls implemented on CBP devices. Upon completion of the assessments, we provided CBP 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.



U.S. Customs and
Border Protection

August 12, 2005

MEMORANDUM FOR RICHARD L. SKINNER
INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

FROM: Nicolle Sciara
Acting Director, Office of Policy and Planning

SUBJECT: Response to the Office of Inspector General's Draft Report on the Security of U.S. Customs and Border Protection's Networks

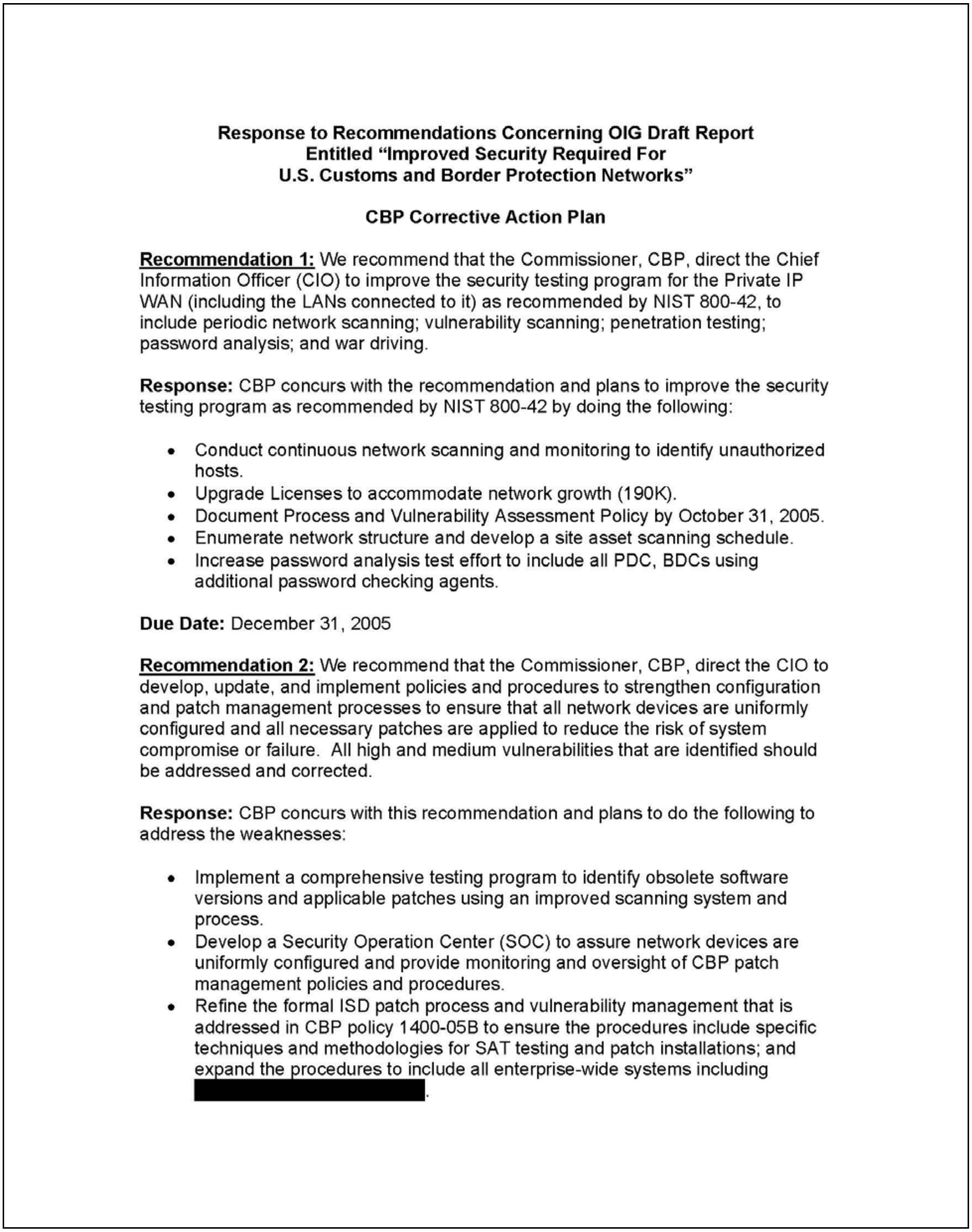
Thank you for providing us with a copy of your draft report entitled "Improved Security Required For U.S. Customs and Border Protection Networks" and the opportunity to discuss the issues in this report.

U.S. Customs and Border Protection (CBP) agrees with the Department of Homeland Security, Office of Inspector General's (OIG's) overall observations that security controls must be improved in order for CBP to provide adequate and effective security over its networks. CBP has taken, and will continue to take, steps to address each of the report's recommendations. Attached are comments specific to the recommendations, as well as technical comments that relate to statements that need to be clarified prior to the finalization of this report.

CBP has determined that the information in the audit does warrant protection and we are designating the document as "For Official Use Only (FOUO)." CBP believes that the report addresses vulnerabilities of CBP's systems. Classification of the report as FOUO is clearly justified because of the sensitive nature of the information contained therein. Please consider CBP's concerns prior to releasing information that has been determined to be sensitive.

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Lynn Richardson at (202) 344-2953.

Attachment



Response to Recommendations Concerning OIG Draft Report Entitled "Improved Security Required For U.S. Customs and Border Protection Networks"

CBP Corrective Action Plan

Recommendation 1: We recommend that the Commissioner, CBP, direct the Chief Information Officer (CIO) to improve the security testing program for the Private IP WAN (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.

Response: CBP concurs with the recommendation and plans to improve the security testing program as recommended by NIST 800-42 by doing the following:

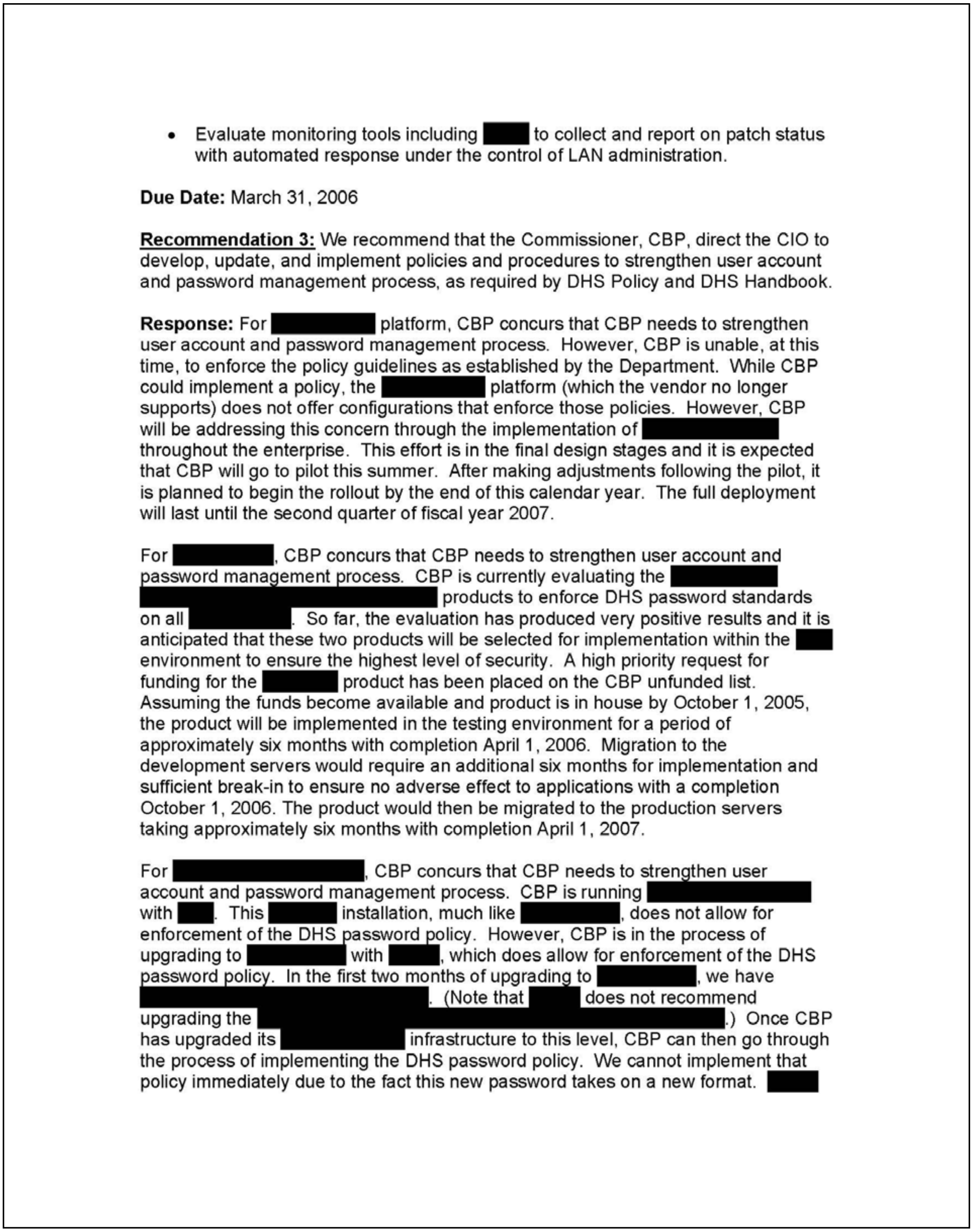
- Conduct continuous network scanning and monitoring to identify unauthorized hosts.
- Upgrade Licenses to accommodate network growth (190K).
- Document Process and Vulnerability Assessment Policy by October 31, 2005.
- Enumerate network structure and develop a site asset scanning schedule.
- Increase password analysis test effort to include all PDC, BDCs using additional password checking agents.

Due Date: December 31, 2005

Recommendation 2: We recommend that the Commissioner, CBP, direct the CIO to develop, update, and implement policies and procedures to strengthen configuration and patch management processes to ensure that all network devices are uniformly configured and all necessary patches are applied to reduce the risk of system compromise or failure. All high and medium vulnerabilities that are identified should be addressed and corrected.

Response: CBP concurs with this recommendation and plans to do the following to address the weaknesses:

- Implement a comprehensive testing program to identify obsolete software versions and applicable patches using an improved scanning system and process.
- Develop a Security Operation Center (SOC) to assure network devices are uniformly configured and provide monitoring and oversight of CBP patch management policies and procedures.
- Refine the formal ISD patch process and vulnerability management that is addressed in CBP policy 1400-05B to ensure the procedures include specific techniques and methodologies for SAT testing and patch installations; and expand the procedures to include all enterprise-wide systems including [redacted].



- Evaluate monitoring tools including [redacted] to collect and report on patch status with automated response under the control of LAN administration.

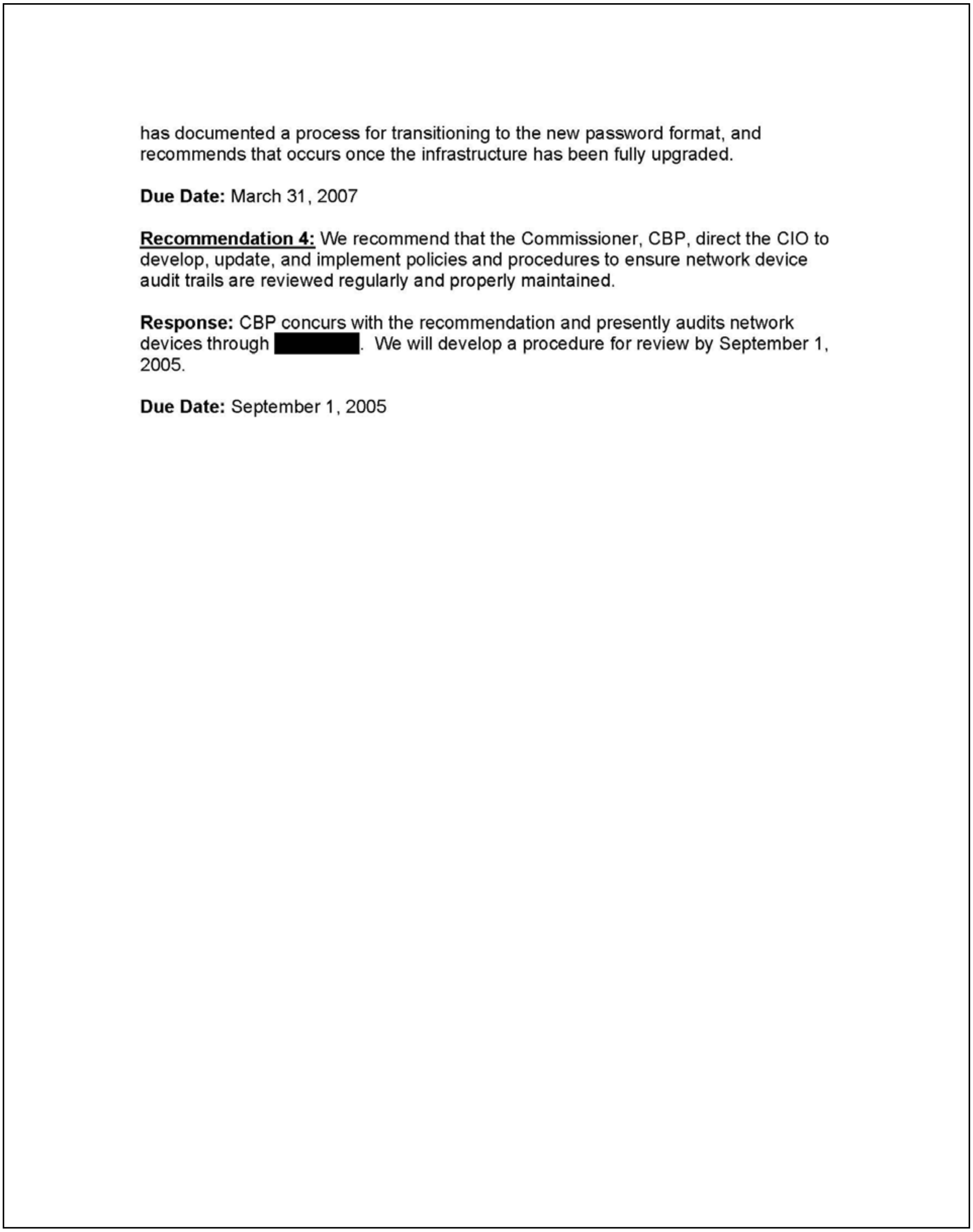
Due Date: March 31, 2006

<u>Recommendation 3:</u> We recommend that the Commissioner, CBP, direct the CIO to develop, update, and implement policies and procedures to strengthen user account and password management process, as required by DHS Policy and DHS Handbook.

Response: For [redacted] platform, CBP concurs that CBP needs to strengthen user account and password management process. However, CBP is unable, at this time, to enforce the policy guidelines as established by the Department. While CBP could implement a policy, the [redacted] platform (which the vendor no longer supports) does not offer configurations that enforce those policies. However, CBP will be addressing this concern through the implementation of [redacted] throughout the enterprise. This effort is in the final design stages and it is expected that CBP will go to pilot this summer. After making adjustments following the pilot, it is planned to begin the rollout by the end of this calendar year. The full deployment will last until the second quarter of fiscal year 2007.

For [redacted], CBP concurs that CBP needs to strengthen user account and password management process. CBP is currently evaluating the [redacted] products to enforce DHS password standards on all [redacted]. So far, the evaluation has produced very positive results and it is anticipated that these two products will be selected for implementation within the [redacted] environment to ensure the highest level of security. A high priority request for funding for the [redacted] product has been placed on the CBP unfunded list. Assuming the funds become available and product is in house by October 1, 2005, the product will be implemented in the testing environment for a period of approximately six months with completion April 1, 2006. Migration to the development servers would require an additional six months for implementation and sufficient break-in to ensure no adverse effect to applications with a completion October 1, 2006. The product would then be migrated to the production servers taking approximately six months with completion April 1, 2007.

For [redacted], CBP concurs that CBP needs to strengthen user account and password management process. CBP is running [redacted] with [redacted]. This [redacted] installation, much like [redacted], does not allow for enforcement of the DHS password policy. However, CBP is in the process of upgrading to [redacted] with [redacted], which does allow for enforcement of the DHS password policy. In the first two months of upgrading to [redacted], we have [redacted]. (Note that [redacted] does not recommend upgrading the [redacted].) Once CBP has upgraded its [redacted] infrastructure to this level, CBP can then go through the process of implementing the DHS password policy. We cannot implement that policy immediately due to the fact this new password takes on a new format. [redacted]



has documented a process for transitioning to the new password format, and recommends that occurs once the infrastructure has been fully upgraded.

Due Date: March 31, 2007

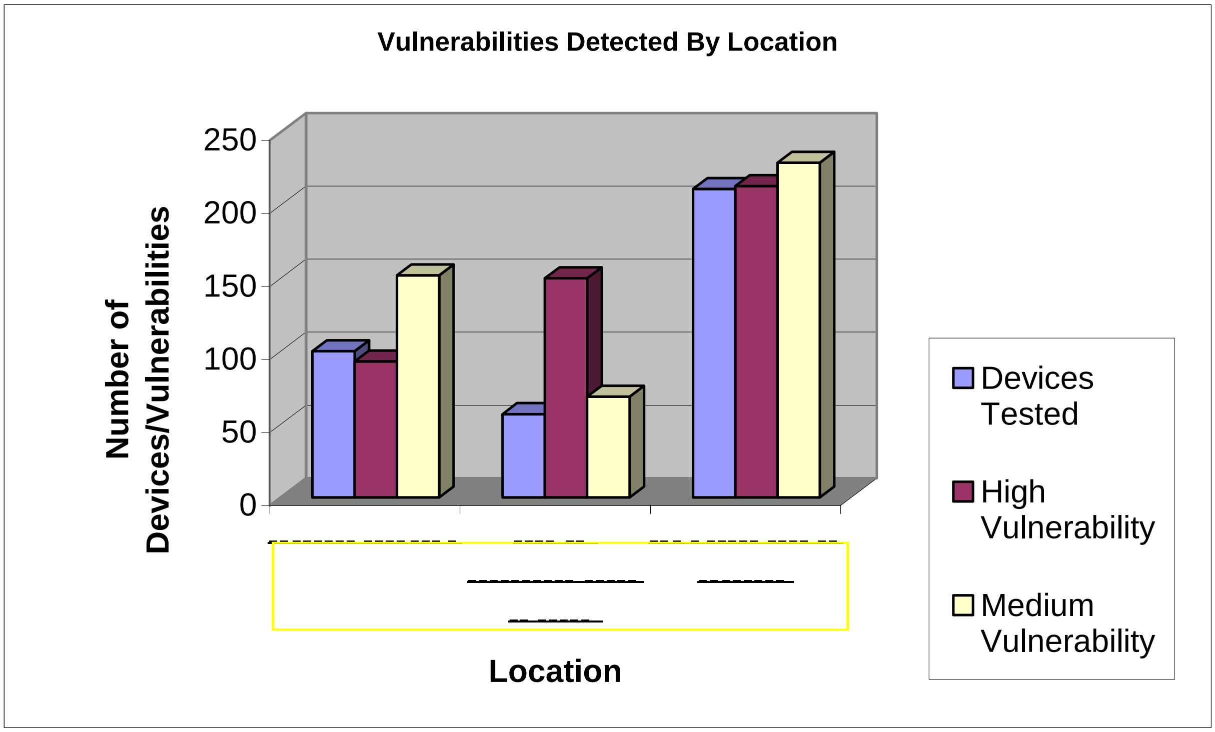
Recommendation 4: We recommend that the Commissioner, CBP, direct the CIO to develop, update, and implement policies and procedures to ensure network device audit trails are reviewed regularly and properly maintained.

Response: CBP concurs with the recommendation and presently audits network devices through [redacted]. We will develop a procedure for review by September 1, 2005.

Due Date: September 1, 2005

Appendix C
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



Location	Devices Tested [1]	High Vulnerability	Medium Vulnerability
[redacted]	100	93	152
[redacted]	57	150	69
[redacted]	211	213	229
Total	**368**	**456**	**450**

[1] Devices tested include servers, workstations, switches, and network 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
Theresa Spinola, 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
Border and Transportation Security, Under Secretary
Chief Information Officer
Chief Information Security Officer
Chief Security Officer
Public Affairs
Legislative Affairs
CBP, Commissioner
CBP, Chief Information Officer
CBP, 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.

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.