DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improved Security Required For U.S. Secret Service 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-05-38 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 United States Secret Service (Secret Service). It is based on interviews with employees and officials of the Secret Service, 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
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
------	--------------------------
IDS	Intrusion Detection System
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

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 United States Secret Service (Secret Service) 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 the Secret Service has implemented adequate controls to protect its networks. The Secret Service shares law enforcement sensitive data through its wide area network (WAN). The Secret Service WAN connects to local area networks (LANs) located throughout the country. To address our objective, we: (1) interviewed personnel at the Secret Service Headquarters, (2) reviewed DHS and Secret Service's policies and procedures, and (3) conducted vulnerability assessments for a select sample of network devices at three Secret Service locations [redacted]

The Secret Service 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. Additionally, the Secret Service 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 the Secret Service 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. Furthermore, our evaluation of router configuration determined that the Secret Service had [redacted] or securely configured its routers to minimize unauthorized access to its networks. These security concerns provide increased potential for unauthorized access to Secret Service resources and data.

We made several recommendations to assist the Secret Service 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, the Secret Service agreed and has already taken steps to implement each of the recommendations. Secret Service'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: 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 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]

[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.

(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.

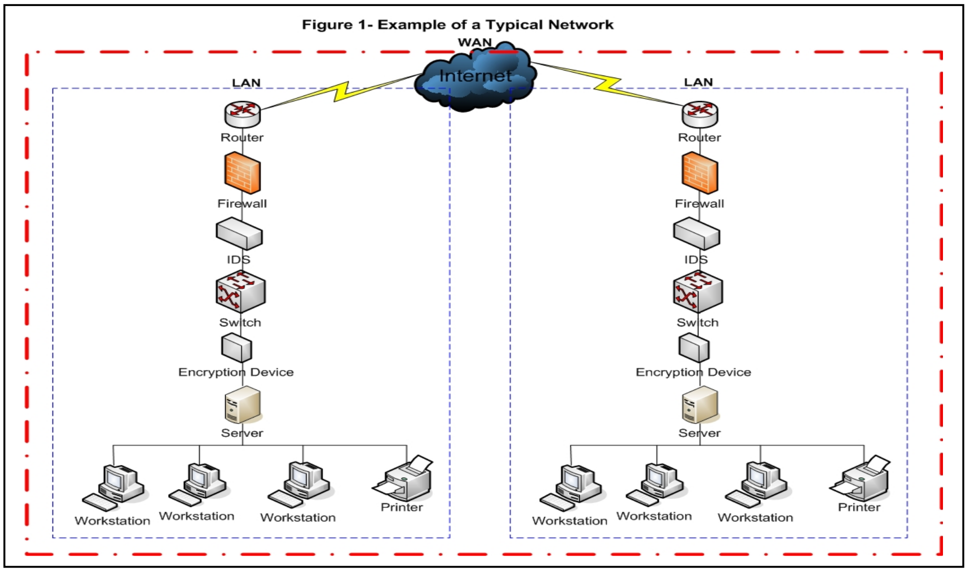


Figure 1- Example of a Typical Network

The Secret Service has over ------------- of its WAN. Since law enforcement sensitive data is stored on and transmitted along its WAN, 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.

[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 from 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.

Results of Audit

The Secret Service Does Not Have a Comprehensive Security Testing Program

The Secret Service does not have a comprehensive security testing program to evaluate the effectiveness of controls implemented on its networks. Although vulnerability scans are performed on new devices before they are connected to the WAN, the Secret Service has not established a comprehensive testing program that would evaluate security controls implemented and identify security patches for known vulnerabilities. While a penetration test was performed in December 2003, the Secret Service does not perform other security testing periodically, such as password analysis; and, it has yet to decide whether to perform a penetration test in 2005. Furthermore, the Secret Service has not developed policy and procedures that require security testing, (such as vulnerability scans, password analysis, and penetration testing) be performed periodically throughout its networks.

The Federal Information Security Management Act of 2002 (FISMA) requires that federal agencies perform periodic testing to evaluate the effectiveness of security controls. Also, 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 may continue to exist if the Secret Service does not implement a comprehensive testing program to identify obsolete software versions and applicable patches on its network devices. Without performing routine security testing, the Secret Service cannot ensure that the security controls implemented 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 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 Director, U.S. Secret Service, direct the Chief Information Officer (CIO) to:

1. Implement a security testing program for its WAN and LANs, 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

The Secret Service agreed with our recommendation. The Secret Service plans to develop policies and procedures to establish a security testing program that includes periodic network scanning, vulnerability scanning, penetration testing, password analysis, and war driving by January 2006.

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

Improved Administration is Required to Strengthen Network Security

The Secret Service has not implemented effective system controls over its networks. To assess the security of the Secret Service's networks, we interviewed information technology personnel at Secret Service Headquarters; performed vulnerability scans at three Secret Service locations [redacted] using ISS Internet Scanner software and Kane Security Analyst; and, evaluated router configurations.

In assessing the effectiveness of system controls, we performed vulnerability scans on [redacted] network devices and identified [redacted] security vulnerabilities that are classified as either high or medium risk.[6] The Secret Service has established LANs at its field offices across the country and in major cities around the world - the scans that we performed only represent a sample of the entire Secret Service WAN. [redacted] of the security vulnerabilities discovered are primarily attributed to inadequate [redacted], often which are not recognized as potential security exposures, can be exploited for

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

[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

The Secret Service needs to improve its configuration management process to ensure that all network devices are appropriately secured.[7] The Secret Service has not established detailed configuration procedures for all of its network devices. Furthermore, the results of our ISS scans indicate that the network devices are not securely configured throughout the organization. Specifically:

- Users could access network [redacted] This vulnerability may allow attackers unauthorized access to Secret Service's networks.
- Outdated versions of the [redacted]. This vulnerability may allow an attacker to gain unauthorized access to Secret Service networks.
- A user could access [redacted]. This vulnerability could allow an attacker access to sensitive information through [redacted]
- [redacted] This condition may allow an attacker to obtain [redacted] that could be used to mount further attacks on a network.

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

[redacted]

- [redacted]
- [redacted]

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 is 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.

Improvement of the Patch Management Process Can Reduce Security Vulnerabilities

While the Secret Service has established a centralized patch management[11] process, our scan results revealed the need for improvement. In addition, the Secret Service has not documented its patch management policy and procedures. Unpatched network devices may expose Secret Service's networks to [redacted] The Secret Service can strengthen its patch management process by developing documented policy and procedures to ensure that security patches are appropriately identified and applied to mitigate

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

[redacted]

vulnerabilities on all network devices.[13] For example, we identified the following vulnerabilities which are due to missing security patches that were issued [redacted] in 2003 and 2004:

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

NIST recommends that agencies have an explicit and documented policy as well as a systematic, accountable, and documented set of processes and procedures for handling and applying 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 an effective documented patch management process, the Secret Service cannot ensure that all security vulnerabilities have been mitigated before malicious users exploit these vulnerabilities. Applying security patches is critical for securing the Secret Service WAN and LANs and protecting sensitive data from unauthorized access, manipulation, and misuse.

<u>Weaknesses Identified in User Account and Password Management</u>

The Secret Service had weak password configuration. Our review of the account policy settings on selected [redacted] determined

[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]

that the Secret Service had configured the [redacted] Secret Service personnel indicated that they had temporarily configured the [redacted] while they were migrating from [redacted]. In addition, we discovered the following weaknesses in account and password administration during our vulnerability scans on selected [redacted]:

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

These weaknesses are an indication that user accounts and passwords on LANs across the Secret Service WAN may not be effective to control access to Secret Service 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

The Secret Service 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. The Secret Service has not developed detailed configuration guidelines for its [redacted] routers.

Based on our evaluation of the router configurations, we determined that the Secret Service had not implemented the following to minimize unauthorized access to its networks:

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

[redacted]

-

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

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

Recommendation

We recommend that the Director, U.S. Secret Service, direct the CIO to:

2. Develop, update, and implement policies and procedures to strengthen the configuration and patch management process 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.

Management Comments and OIG Analysis

The Secret Service agreed with our recommendation. The Secret Service has implemented an automated process to deploy security patches. In addition, the Secret Service is in the process of developing policy and procedures for patch management. The procedures will include the methodology to prioritize, as well as test and install security patches. The Secret Service plans to complete the policy and procedures by October 2005. Furthermore, the Secret Service plans to implement stronger controls and perform periodic scans on its network devices, as part of its testing program. The Secret Service plans to complete this action by January 2006. Finally, the Secret Service plans to review all vulnerabilities reported and determine specific corrective actions to mitigate the vulnerabilities identified.

[redacted]

[redacted]

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

Audit Trails Are Not Regularly Reviewed and Maintained

The Secret Service does not ensure that audit trails on all network devices are regularly reviewed to ensure that only authorized activity is occurring on the networks. 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 did not consistently use audit trails to monitor network activities. For example, [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 Secret Service may not detect unauthorized activity or determine the users who are responsible.

Recommendation

We recommend that the Director, U.S. Secret Service, direct the CIO to:

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

Management Comments and OIG Analysis

The Secret Service agreed with our recommendation and is in the process of revising its audit trail policy to require the capture, review and proper maintenance of audit logs for Secret Service servers. The Secret Service plans to complete this action by December 2005.

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

Contingency Plan Has Not Been Developed

The Secret Service WAN and associated LANs were certified and accredited in 2003; however, they lacked a documented and tested contingency plan. 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.

DHS policy and the Office of Management and Budget require that contingency plans be developed and the plans 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. 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.

Since the Secret Service has not developed contingency plans for its networks, the Secret Service cannot ensure that it will be able to promptly recover essential operations if an unexpected interruption occurs. Untested plans may create a false sense of ability to recover operations in a timely manner.

Recommendation

We recommend that the Director, U.S. Secret Service, direct the CIO to:

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

Management Comments and OIG Analysis

The Secret Service agreed with our recommendation to develop and regularly test contingency plans for all systems. The Secret Service has developed a template that will be used to prepare contingency plans for all systems. The Secret Service indicated that the completion of contingency plans for the WAN and associated LANs is considered a high priority, and the target date to complete the development and approval of contingency plans for the WAN is January 2006 and each of the LANs is March 2006.

We agree that the steps that the Secret Service has taken, and plans to take begin to satisfy this recommendation. However, once the contingency plans have been developed, the Secret Service should test its contingency plans annually, as required by applicable federal guidelines and DHS policy.

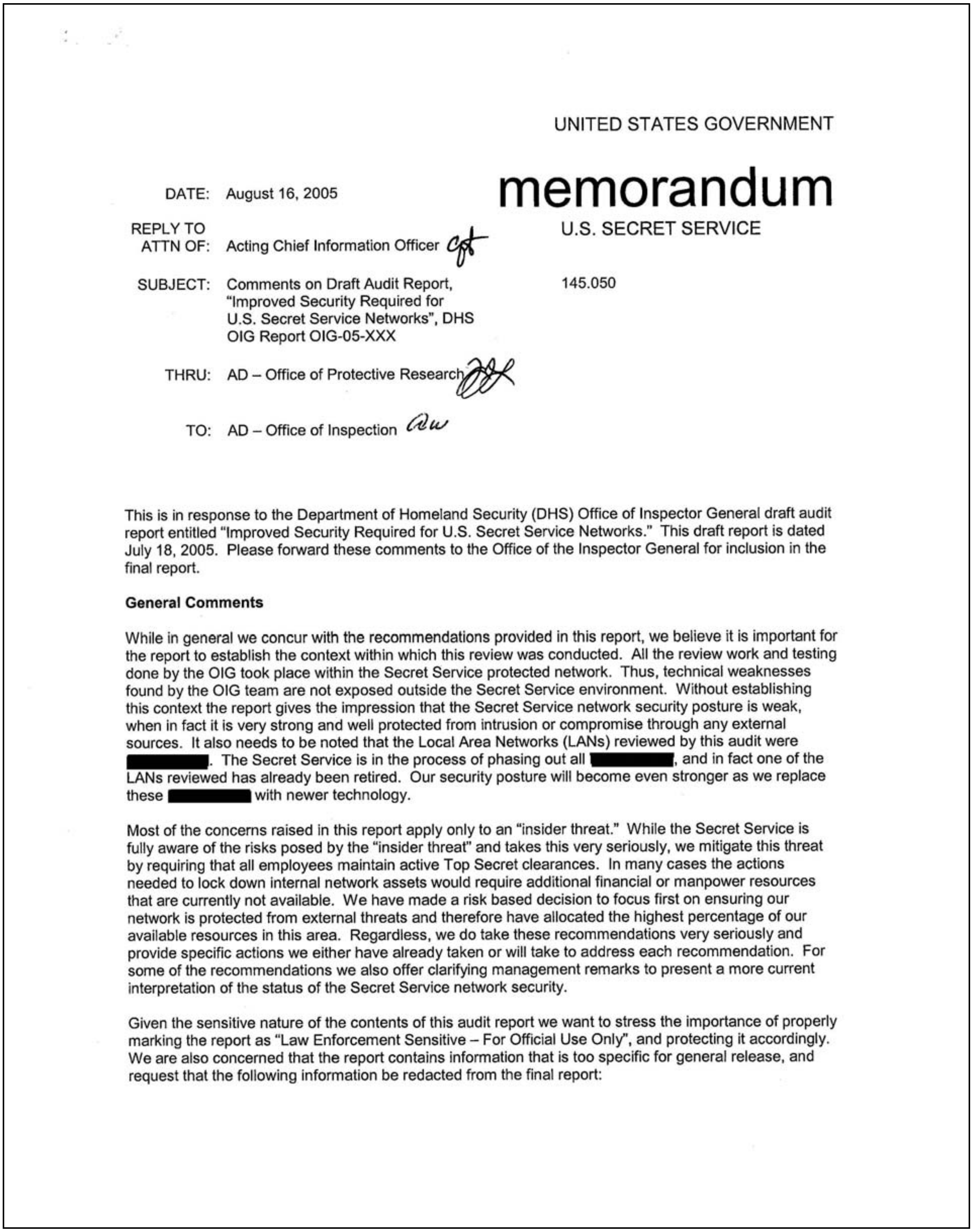
Purpose, Scope, and Methodology

The objective of this audit was to determine whether the Secret Service had implemented adequate controls for protecting its WAN and LANs. Specifically, we determined whether: (1) the Secret Service 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 Secret Service Headquarters. In addition, we reviewed and evaluated DHS and Secret Service 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, switches and network printers. Upon completion of the assessments, we provided the Secret Service the technical reports detailing the specific vulnerabilities detected on their network devices and the actions needed for remediation. We also evaluated configuration settings on routers.

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.



UNITED STATES GOVERNMENT

memorandum

U.S. SECRET SERVICE

DATE: August 16, 2005

REPLY TO
ATTN OF: Acting Chief Information Officer

SUBJECT: Comments on Draft Audit Report, "Improved Security Required for U.S. Secret Service Networks", DHS OIG Report OIG-05-XXX

145.050

THRU: AD – Office of Protective Research

TO: AD – Office of Inspection

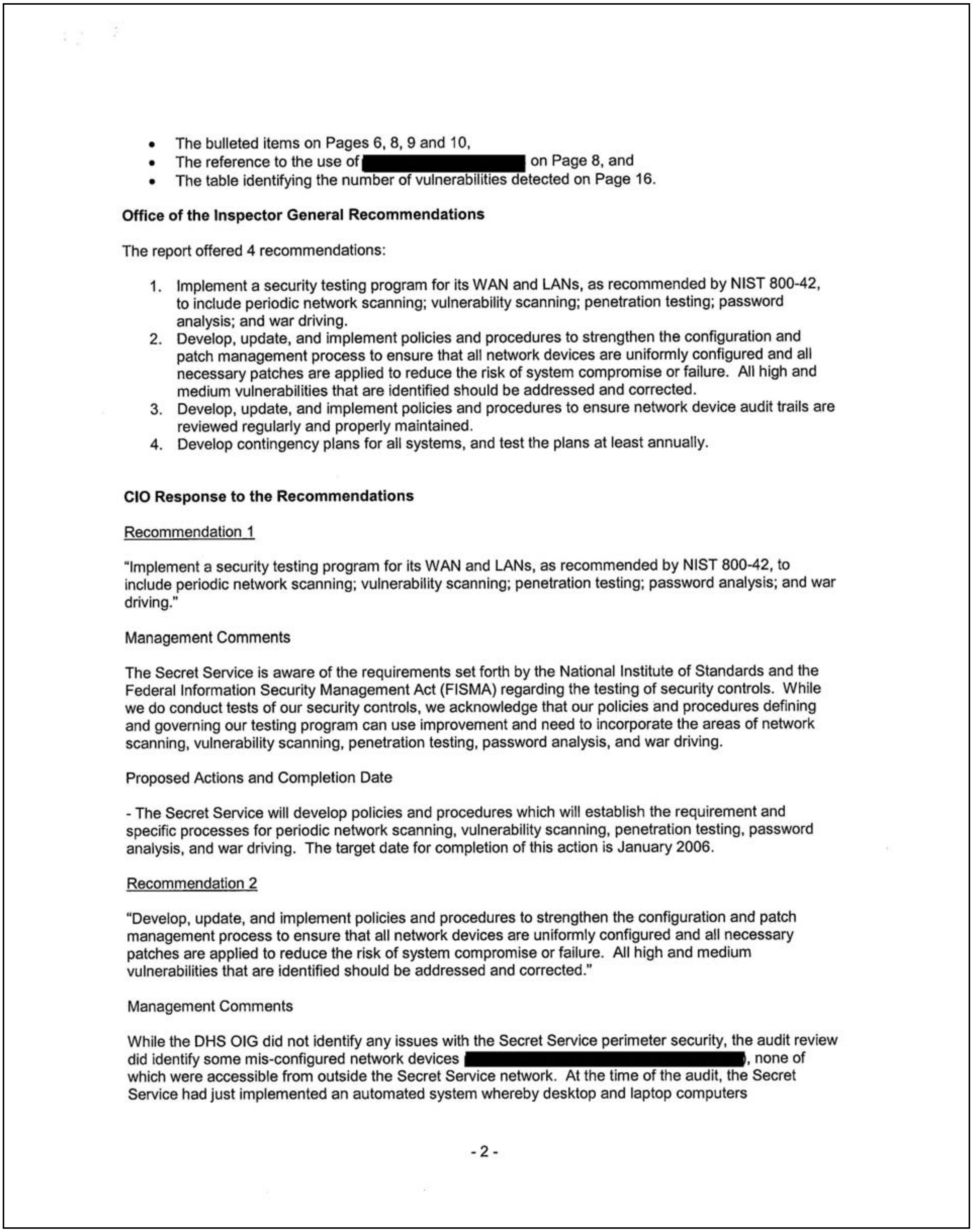
This is in response to the Department of Homeland Security (DHS) Office of Inspector General draft audit report entitled "Improved Security Required for U.S. Secret Service Networks." This draft report is dated July 18, 2005. Please forward these comments to the Office of the Inspector General for inclusion in the final report.

General Comments

While in general we concur with the recommendations provided in this report, we believe it is important for the report to establish the context within which this review was conducted. All the review work and testing done by the OIG took place within the Secret Service protected network. Thus, technical weaknesses found by the OIG team are not exposed outside the Secret Service environment. Without establishing this context the report gives the impression that the Secret Service network security posture is weak, when in fact it is very strong and well protected from intrusion or compromise through any external sources. It also needs to be noted that the Local Area Networks (LANs) reviewed by this audit were [redacted]. The Secret Service is in the process of phasing out all [redacted], and in fact one of the LANs reviewed has already been retired. Our security posture will become even stronger as we replace these [redacted] with newer technology.

Most of the concerns raised in this report apply only to an "insider threat." While the Secret Service is fully aware of the risks posed by the "insider threat" and takes this very seriously, we mitigate this threat by requiring that all employees maintain active Top Secret clearances. In many cases the actions needed to lock down internal network assets would require additional financial or manpower resources that are currently not available. We have made a risk based decision to focus first on ensuring our network is protected from external threats and therefore have allocated the highest percentage of our available resources in this area. Regardless, we do take these recommendations very seriously and provide specific actions we either have already taken or will take to address each recommendation. For some of the recommendations we also offer clarifying management remarks to present a more current interpretation of the status of the Secret Service network security.

Given the sensitive nature of the contents of this audit report we want to stress the importance of properly marking the report as "Law Enforcement Sensitive – For Official Use Only", and protecting it accordingly. We are also concerned that the report contains information that is too specific for general release, and request that the following information be redacted from the final report:



- The bulleted items on Pages 6, 8, 9 and 10,
- The reference to the use of [redacted] on Page 8, and
- The table identifying the number of vulnerabilities detected on Page 16.

Office of the Inspector General Recommendations

The report offered 4 recommendations:

1. Implement a security testing program for its WAN and LANs, as recommended by NIST 800-42, to include periodic network scanning; vulnerability scanning; penetration testing; password analysis; and war driving.
2. Develop, update, and implement policies and procedures to strengthen the configuration and patch management process 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 ensure network device audit trails are reviewed regularly and properly maintained.
4. Develop contingency plans for all systems, and test the plans at least annually.

CIO Response to the Recommendations

Recommendation 1

"Implement a security testing program for its WAN and LANs, as recommended by NIST 800-42, to include periodic network scanning; vulnerability scanning; penetration testing; password analysis; and war driving."

Management Comments

The Secret Service is aware of the requirements set forth by the National Institute of Standards and the Federal Information Security Management Act (FISMA) regarding the testing of security controls. While we do conduct tests of our security controls, we acknowledge that our policies and procedures defining and governing our testing program can use improvement and need to incorporate the areas of network scanning, vulnerability scanning, penetration testing, password analysis, and war driving.

Proposed Actions and Completion Date

- The Secret Service will develop policies and procedures which will establish the requirement and specific processes for periodic network scanning, vulnerability scanning, penetration testing, password analysis, and war driving. The target date for completion of this action is January 2006.

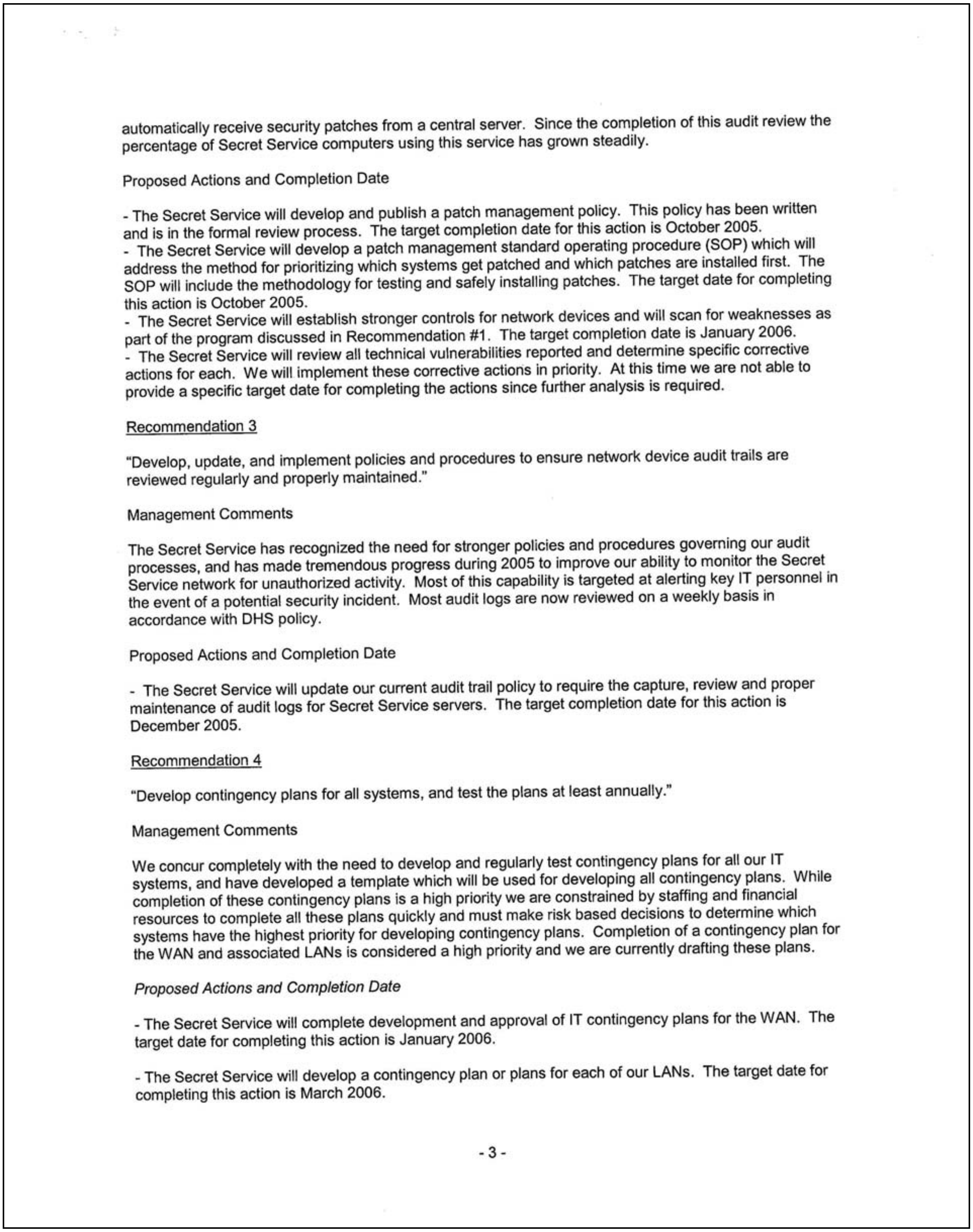
Recommendation 2

"Develop, update, and implement policies and procedures to strengthen the configuration and patch management process 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."

Management Comments

While the DHS OIG did not identify any issues with the Secret Service perimeter security, the audit review did identify some mis-configured network devices [redacted], none of which were accessible from outside the Secret Service network. At the time of the audit, the Secret Service had just implemented an automated system whereby desktop and laptop computers

- 2 -



automatically receive security patches from a central server. Since the completion of this audit review the percentage of Secret Service computers using this service has grown steadily.

Proposed Actions and Completion Date

- The Secret Service will develop and publish a patch management policy. This policy has been written and is in the formal review process. The target completion date for this action is October 2005.
- The Secret Service will develop a patch management standard operating procedure (SOP) which will address the method for prioritizing which systems get patched and which patches are installed first. The SOP will include the methodology for testing and safely installing patches. The target date for completing this action is October 2005.
- The Secret Service will establish stronger controls for network devices and will scan for weaknesses as part of the program discussed in Recommendation #1. The target completion date is January 2006.
- The Secret Service will review all technical vulnerabilities reported and determine specific corrective actions for each. We will implement these corrective actions in priority. At this time we are not able to provide a specific target date for completing the actions since further analysis is required.

Recommendation 3

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

Management Comments

The Secret Service has recognized the need for stronger policies and procedures governing our audit processes, and has made tremendous progress during 2005 to improve our ability to monitor the Secret Service network for unauthorized activity. Most of this capability is targeted at alerting key IT personnel in the event of a potential security incident. Most audit logs are now reviewed on a weekly basis in accordance with DHS policy.

Proposed Actions and Completion Date

- The Secret Service will update our current audit trail policy to require the capture, review and proper maintenance of audit logs for Secret Service servers. The target completion date for this action is December 2005.

Recommendation 4

"Develop contingency plans for all systems, and test the plans at least annually."

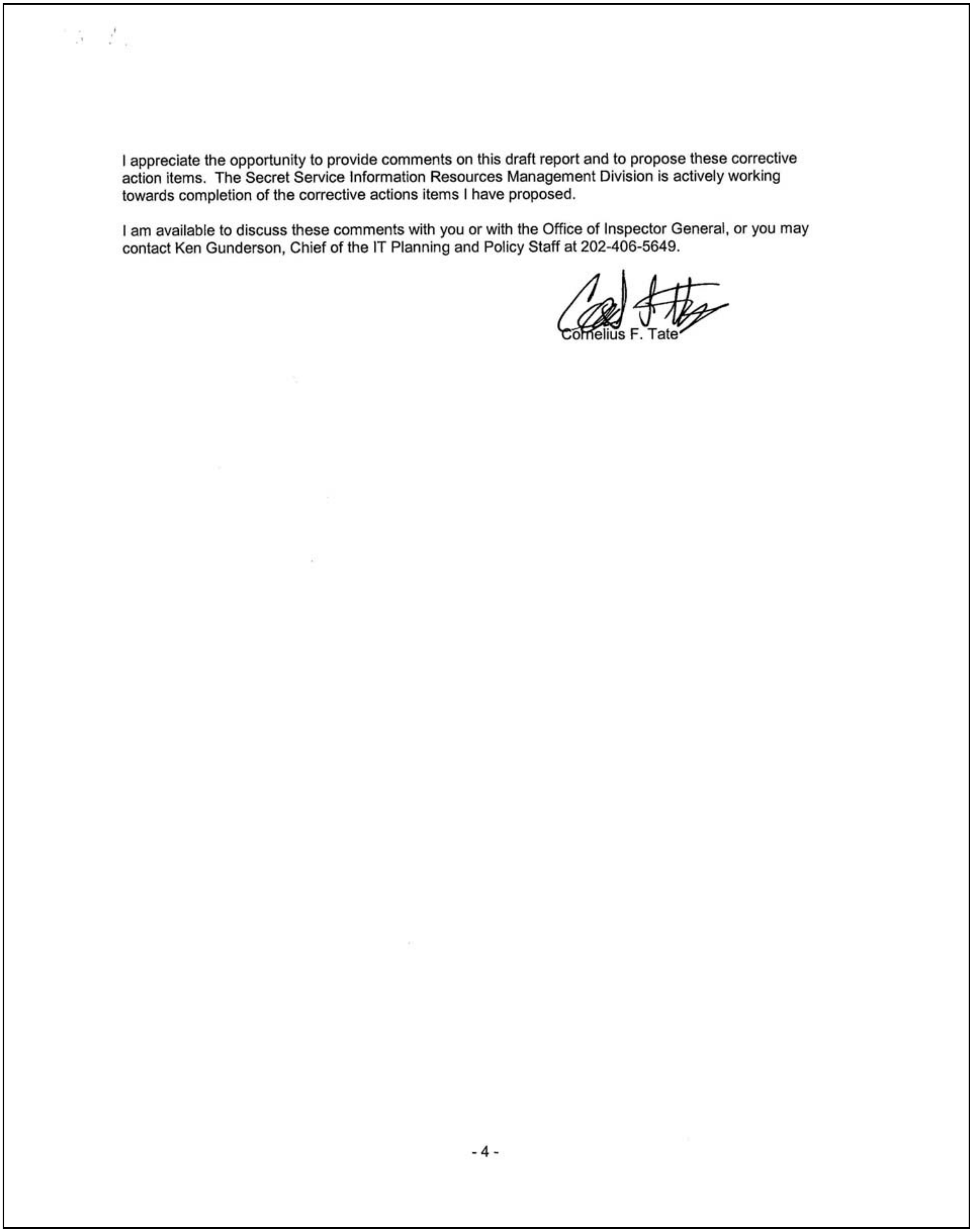
Management Comments

We concur completely with the need to develop and regularly test contingency plans for all our IT systems, and have developed a template which will be used for developing all contingency plans. While completion of these contingency plans is a high priority we are constrained by staffing and financial resources to complete all these plans quickly and must make risk based decisions to determine which systems have the highest priority for developing contingency plans. Completion of a contingency plan for the WAN and associated LANs is considered a high priority and we are currently drafting these plans.

Proposed Actions and Completion Date

- The Secret Service will complete development and approval of IT contingency plans for the WAN. The target date for completing this action is January 2006.

- The Secret Service will develop a contingency plan or plans for each of our LANs. The target date for completing this action is March 2006.



I appreciate the opportunity to provide comments on this draft report and to propose these corrective action items. The Secret Service Information Resources Management Division is actively working towards completion of the corrective actions items I have proposed.

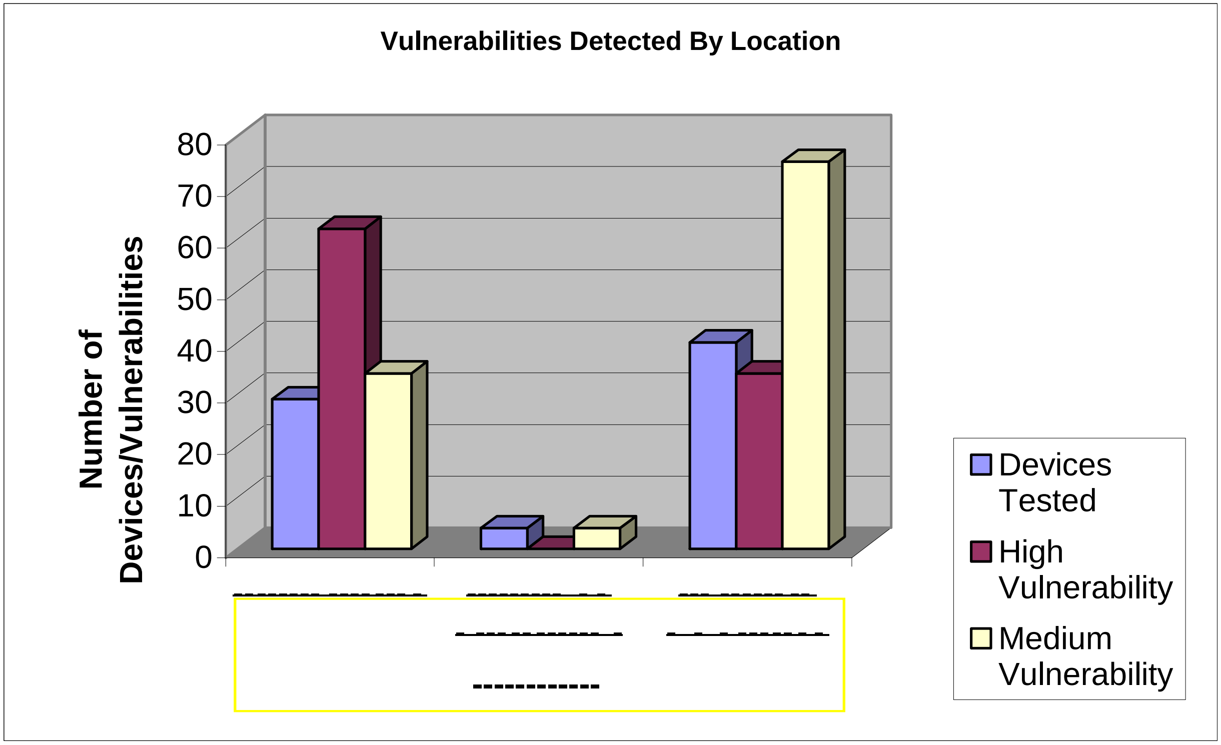
I am available to discuss these comments with you or with the Office of Inspector General, or you may contact Ken Gunderson, Chief of the IT Planning and Policy Staff at 202-406-5649.

Cornelius F. Tate

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

Appendix D
Vulnerabilities Detected By Location



Location	Devices Tested [1]	High Vulnerability	Medium Vulnerability
[redacted]	29	62	34
[redacted]	4	0	4
[redacted]	40	34	74
Total	**73**	**96**	**112**

[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
Louis Ochoa, 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
Chief Security Officer
Chief Information Officer
Chief Information Security Officer
Public Affairs
Legislative Affairs
U.S. Secret Service, Director
U.S. Secret Service, Chief Information Officer
U.S. Secret Service, Audit Liaison
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.