DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improved Security Required for U.S. Coast Guard 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-05-30 **August 2005**

Office of Inspector General

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

Homeland Security

Preface

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

This report assesses the strengths and weaknesses of controls over network security at the United States Coast Guard (Coast Guard). It is based on interviews with employees and officials of the Coast Guard, 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
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CGDN+	Coast Guard Data Network Plus
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

OMB	Office of Management and Budget
TISCOM	Telecommunication and Information Systems Command
WAN	Wide Area Network

Executive Summary

The Office of Inspector General (OIG) audited the security program of the Department of Homeland Security (DHS) and its organizational components to evaluate the effectiveness of controls implemented on selected wired-based sensitive but unclassified networks. This audit included a review of applicable DHS and United States Coast Guard (Coast Guard) 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 Coast Guard has implemented adequate controls for protecting its networks. To address our objective we: (1) interviewed personnel at the Telecommunication and Information Systems Command (TISCOM), Coast Guard Headquarters, [redacted]; (2) reviewed DHS and Coast Guard's policies and procedures; and, (3) conducted vulnerability assessments for a select sample of network devices at seven locations ([redacted]

The Coast Guard relies on TISCOM for the overall management and security of its Coast Guard Data Network Plus (CGDN+) network. However, different groups throughout the organization manage the [redacted] local area networks (LAN)s that connect to the CGDN+ network. For example, each major command, including Coast Guard Headquarters, is responsible for managing its own LANs, configuring its own network devices, and deploying security patches.

The Coast Guard has not developed or implemented controls necessary to ensure that the data residing on and traveling through its network resources is properly protected. The Coast Guard has developed various policies, procedures, and processes to help monitor and secure its CGDN+ network and its LANs. However, the Coast Guard has not developed policies or procedures and fully implemented processes that address security testing, monitoring network activities with audit trails, and configuration and patch management. In addition, the CGDN+ network contingency plan has not been tested, yet.

Security controls must be improved in order for the Coast Guard 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 inconsistent configuration and patch management. These security concerns indicate increased potential for unauthorized access to Coast Guard resources and data.

We are making several recommendations to assist the Coast Guard 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 Coast Guard agreed and has already taken steps to implement each of the recommendations. The Coast Guard's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

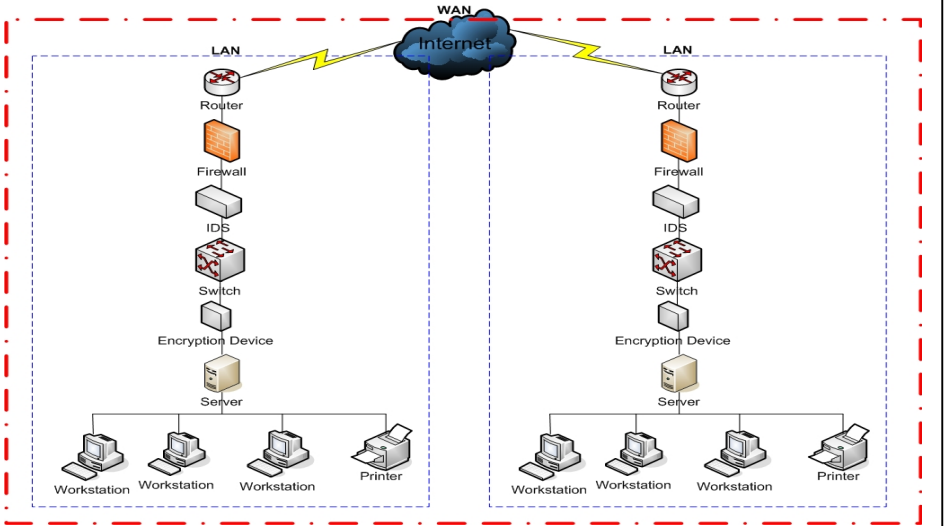
Background

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 wide area network (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] (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.

[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 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.

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 critical that government agencies secure their networks and protect them from vulnerabilities. As a result, network security is no longer something which 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.

Figure 1- Example of a Typical Network



The Coast Guard shares information through its WAN or CGDN+, which is connected to [redacted] LANs located throughout the country. Since sensitive data is stored on and transmitted along networks, effectively securing networks is essential to protect sensitive data from unauthorized access, manipulation, and misuse. Improperly configured network services expose a network to internal or external threats such as hackers, cyber-terrorist groups, and denial of service 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.

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

Results of Audit

The Coast Guard Does Not Have a Comprehensive Network Security Testing Program

The Coast Guard does not have a comprehensive security testing program in place to ensure the integrity of the CGDN+ network. TISCOM performs vulnerability scanning, such as scans of the entire CGDN+ WAN and a limited number of LANs for a specific vulnerability, and scans individual devices for all vulnerabilities. However, TISCOM does not conduct other forms of testing, such as penetration testing, integrity checking, or password analysis. In addition, the testing program is not centrally managed by TISCOM, as other groups (including the Coast Guard Headquarters) are responsible for performing security testing on the LANs that they manage. Furthermore, the Coast Guard's policy for vulnerability scanning is incomplete and only in draft. The draft policy requires that vulnerability scanning of all devices connected to the CGDN+ WAN be conducted annually, or when changes to networks occur. However, annual vulnerability scanning is not performed.

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to perform periodic testing to evaluate the effectiveness of security controls. In addition, National Institute of Standards and Technology (NIST) Special Publication 800-42 (*Guideline on Network Security Testing*) recommends 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 the Coast Guard has not implemented a comprehensive testing program to identify obsolete software versions and applicable patches on its network devices.

Without a centrally managed group responsible for performing security testing, the Coast Guard cannot ensure that all network devices connected to the CGDN+ WAN are properly secured or that the sensitive data processed and stored on its network is protected from unauthorized accesses and potential misuse. Security testing can identify potential vulnerabilities and subsequently repair them to reduce the likelihood of systems being compromised, too. See Appendix C for NIST's recommended routine testing schedule.

Recommendation

We recommend that the Coast Guard Commandant direct the Chief Information Officer (CIO) to:

1. Implement a security testing program for CGDN+ (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. One centralized group should be responsible for ensuring that security testing is performed periodically on the CGDN+ (including the LANs connected to it).

Management Comments and OIG Analysis

The Coast Guard agreed with our recommendation. The Coast Guard has put into operation a team to design, test, implement, and maintain a Coast Guard wide vulnerability and penetration program. The team has been tasked to regularly perform security scanning, penetration testing, integrity checking, and password analysis on the CGDN+ network.

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

The Coast Guard Network Is Vulnerable

The Coast Guard has not implemented effective system controls over its network. To assess the security of the Coast Guard's network, we interviewed information technology personnel at TISCOM, Coast Guard Headquarters, [redacted] performed vulnerability scans at seven Cost Guard locations [redacted] using ISS Internet Scanner software; and reviewed router configuration files using Cisco Security Analyzer.

In assessing the effectiveness of system controls, we identified several high and medium risk vulnerabilities which could be exploited to gain inappropriate access to Coast Guard sensitive information systems and resources.[6] The Coast Guard has [redacted] LANs - the scans that we performed only represent a sample of the entire CGDN+ network.

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

Without processes in place to ensure that all material vulnerabilities are identified and reviewed, management cannot ensure that its network and the data that resides on it is secure.

Strengthening Configuration Management Process Can Improve Security

The Coast Guard needs to strengthen its configuration management process.[7] There is no centralized process to ensure that all network devices are securely configured throughout the organization. The policies and procedures for the standard configurations of all network devices have not been developed.[8] In addition, the procedures for configuring switches, servers, workstations, and anti-virus software are not effective to protect the networks against unauthorized access.

The Coast Guard has established configuration procedures for servers, workstations, and switches. However, configuration procedures for other network devices, such as firewalls, routers, IDS, and encryption devices have not been developed. Configuration procedures can be used to establish management approved standard configuration and security settings for each type of device, which leads to improved security.

Many of the network devices that we tested were not configured properly to protect against unauthorized access.[9] Specifically:

- Users could gain access to sensitive system information on [redacted]
- A list of accounts on 320 network devices [redacted] could be accessed [redacted] This condition may allow an attacker to obtain account names that could be used to mount further attacks on the network.
- [redacted] Information (e.g., security settings, account names) could be obtained which could compromise the security of the system.
- A user could utilize [redacted] without using an account name.[10] An attacker could access

[7] Configuration management is the control and documentation of changes made to a system's hardware and software.
[8] Standard configuration is a set organizational standard install and configuration instructions that is created for each network device to ensure it works properly and protects it from unauthorized access.
[9] See Appendix E for the number of configuration weaknesses identified by location.

sensitive information through default accounts or easily-guessed passwords.

- [redacted] was running on one server. [redacted] is a service that allows [redacted] access to a computer, [redacted]
- Twenty-one network devices, i.e., [redacted], were running a service [redacted] that is vulnerable to denial of service attacks.
- Twenty-three network devices, [redacted] This allows anyone who can guess the name the ability to obtain valuable information about the system, such as information on network devices and current open connections.

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.

Configured devices which are not secure 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 sensitive data, failure to secure them increases the risk of unauthorized access and use of sensitive data. Networks operating without a standard configuration increase the risk that security controls protecting networks could be circumvented. Furthermore, standardized configurations encourage a higher level of consistency.

[redacted]

Effective Patch Management Process Can Reduce Security Vulnerabilities

The Coast Guard needs to improve its patch management process.[12] There is no centralized process to ensure that software security vulnerabilities are mitigated to minimize unauthorized access. A centralized process can ensure a uniform and consistent implementation of all patches and updates on a timely basis, and help to foster good communication between agency components and ensure the implementation of necessary patches. While the Coast Guard has established patch management groups to identify, test, and deploy security patches, it does not have a uniform process to verify whether security patches have been deployed to all network devices at all locations.[13]

Our scan results revealed that unpatched network devices may expose the Coast Guard's network to [redacted] For example, we identified the following vulnerabilities that are due to missing security patches which were issued in 2003 and 2004:

- [redacted] which could compromise services. Attackers could also take control of a session to gain access to unauthorized information.
- [redacted]
- [redacted] did not have recommended patches installed for [redacted]
- Seven workstations had missing patches to [redacted]

NIST recommends that agencies create a systematic, comprehensive, documented, and accountable patching process to identify and apply patches. To ensure consistency across an organization, agencies should

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

[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]

create a centralized group in charge of patches and vulnerabilities which supports the patching efforts of local administrators.

Without an effective patch verification process and periodic scanning of network devices for vulnerabilities, the Coast Guard cannot ensure that all security vulnerabilities have been mitigated before malicious users exploit these vulnerabilities. Applying security patches is critical to the operational availability, confidentiality, and integrity of information technology systems.

Improvements Needed in User Account and Password Management

User account and password management processes and controls need to be improved. Ineffective controls could lead to unauthorized access to sensitive information.

The Coast Guard's password policy does not comply with DHS' password requirements. DHS has developed a set of password guidelines in its DHS Handbook. However, the Coast Guard's password policy lacks the following required provisions:

- Passwords shall not contain any two identical consecutive characters (e.g., 22apples, 14588904).
- Passwords shall contain no more that 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).

In addition, while the DHS Handbook prohibits the use of concurrent logins or the sharing of user accounts and passwords, the Coast Guard allows concurrent logins (Coast Guard policy does not prohibit concurrent logins), and an account with administrative privileges on multiple routers was shared by two users.

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

- ------ ----------
- ----------
- -------- ----------
- ---------- - ---------- - ----------

- [redacted]

These weaknesses are an indication that user accounts and passwords on LANs across CGDN+ may not be effective to control access to Coast Guard sensitive data. Passwords are important, as they are often the first lines of defense against hackers or insiders who may be trying to obtain unauthorized access to a computer system. SANS Institute recommends that the implementation of a strong password policy is the best and most appropriate defense against security vulnerabilities that are related to weak passwords.

Routers Need To Be Securely Configured

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

Our review of the startup and running configurations on seven Coast Guard routers identified seven high risk and 12 medium risk weaknesses that may lead to undetected and unauthorized access to the Coast Guard network.[15] For example, we identified:

- One hundred eighty occurrences of a [redacted] enabled on six routers.[16] [redacted]
- Ten occurrences of [redacted] on five routers. When routers are misconfigured with this statement, it increases the risk that unauthorized users may gain access to the routers or the networks.
- Four occurrences of the [redacted] on two routers. [redacted] unauthorized users may gain undetected access to the routers and to monitor USCG networks.

[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]

- Six occurrences of [redacted] enabled on six routers.[17] This may allow malicious users to [redacted] addresses to gain unauthorized access to USCG networks.

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

Recommendations

We recommend that the Coast Guard Commandant direct the CIO to:

2. Develop, update, and implement policies as well as procedures for standard configuration of network devices, and passwords, as required by DHS Policy and DHS Handbook.

3. Centralize the configuration and patch management process to ensure that all network devices are properly configured and all necessary patches are applied in a timely manner 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 Coast Guard agreed with recommendation 2. The Coast Guard will review and revise its policy and procedures concerning standardized configuration of network devices and passwords by April 2006.

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

The Coast Guard agreed with recommendation 3. The Coast Guard has implemented a centralized automatic patch management process. Standard practices are now in place to ensure that new vulnerabilities are patched in a set time period. The Coast Guard is developing a testing and implementation plan for a service that will track installation of patches. This service will be implemented in FY 2006. TISCOM provides guidance and tools to all local security officers to ensure compliance with the standardization of security policy and configuration of network

[redacted]

devices. All Coast Guard servers and workstations are now up-to-date regarding [redacted].

> We agree that the steps that the Coast Guard has taken, and plans to take for patch management, satisfy this recommendation. However, TISCOM should put a process in place to ensure that all new network devices set up by local security officers are properly configured.

Audit Trails Are Not Regularly Reviewed and Maintained

The Coast Guard does not ensure that audit trails on all network devices are regularly reviewed and maintained to ensure 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 TISCOM did not consistently use audit trails to monitor network activities. In addition, when network activities were monitored, there was no documentation supporting these activities. Finally, there was no policy for the retention of audit trails.

Specifically, our review determined the following:

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

To be effective, audit trails must be periodically reviewed and analyzed. In many cases, it is only through the review process that incidents of unauthorized access, modification, or destruction are uncovered. 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 Coast Guard may not detect unauthorized activity or determine the users who are responsible.

Recommendation

We recommend that the Coast Guard Commandant direct the CIO to:

4. Develop, update, and implement policies as well as procedures to ensure audit trails are reviewed and maintained.

Management Comments and OIG Analysis

The Coast Guard agreed with our recommendation. The Coast Guard will establish policy and procedures for auditing and monitoring system logs for the servers that will be centrally managed by the second quarter of FY 2008 and by January 2006 for servers that will not be centrally managed.

We agree that the steps that the Coast Guard plans to take begin to satisfy this recommendation. However, the timeline to implement the procedures needs to be shortened to ensure that unauthorized access, modification, or destruction is discovered. Also, the Coast Guard should ensure that the policy and procedures are in line with DHS policy on the frequency of the reviews and address the type of documentation required when performing the reviews.

Contingency Plan Has Not Been Tested

The CGDN+ network was certified and accredited in 2002 without a contingency plan. A contingency plan was later developed in 2004, but it has not been tested. Contingency planning is designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. A well-tested contingency plan can ensure the recovery of critical network operations should interruptions occur.

Office of Management and Budget (OMB) Circular A-130 Appendix III requires that contingency plans be developed and tested periodically. DHS also requires the testing of contingency plans at a minimum annually. Testing of contingency plans is performed to validate specific aspects of the plan, policies, procedures, systems, and facilities that will be used in the event of an emergency. Testing the plan identifies planning

gaps and is also a training exercise to prepare recovery personnel for plan activation, which can improve plan effectiveness and overall agency preparedness.

Untested plans may create a false sense of ability to recover operations in a timely manner. Since the CGDN+ contingency plan has not been tested, the Coast Guard cannot ensure that the procedures documented within the plan will work as intended, or that it will be able to recover all of its critical functions in the event of an emergency or service disruption.

Recommendation

We recommend that the Coast Guard Commandant direct the CIO to:

5. Test the contingency plan for all systems at least annually.

Management Comments and OIG Analysis

The Coast Guard agreed with our recommendation. The Coast Guard indicated that a monthly test of the backup facility housing the CGDN+ WAN is performed. The Coast Guard also indicated that contingency plans for all other sites housing network devices are required to be tested yearly.

We do not agree that the response that the Coast Guard provided adequately satisfies this recommendation. The Coast Guard must test the contingency plan for the CGDN+. In addition, the Coast Guard does not have a process in place to ensure that all contingency plans are tested.

Rogue Wireless Access Point May Allow Unauthorized Access

Although Coast Guard policy prohibits the use of wireless access devices, we detected a wireless access point at one of its facilities. The rogue device detected may allow malicious users unauthorized access to the Coast Guard network. The rogue device may also reveal a systemic problem, as this was the second time wireless access points were detected at Coast Guard facilities. We identified two wireless access points at a different Coast Guard facility in a prior OIG audit report, *Inadequate Security Controls Increased Risks to DHS Wireless Networks*, dated June 2004 (OIG-04-27).

OMB Circular A-130 Appendix III requires federal agencies to provide adequate security to its systems and restrict access to authorized users only. NIST 800-42 recommends that organizations, with high risks and threats, test for unauthorized wireless devices (called war driving) periodically. Running vulnerable network services and insecurely configured network devices increases the risk of system compromise, such as unauthorized access to and manipulation of sensitive system data, disruption of services, and denial of service.

Recommendation

We recommend that the Coast Guard Commandant direct the CIO to:

6. Develop, update, and implement policies as well as procedures to define the acceptable use of wireless technologies, and the consequences of non-compliance. Perform scans for rogue wireless devices regularly.

Management Comments and OIG Analysis

The Coast Guard agreed with our recommendation. The Coast Guard in finalizing enterprise practices regarding acceptable use of wireless technologies. The practices are expected to be approved by September 30, 2005.

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

Purpose, Scope, and Methodology

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

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

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

The principal OIG points of contact for this 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.

J.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol CG-823
Phone: (202) 267-2294
Fax: (202) 267-4850
Email: mark.kulwicki@uscg.dhs.gov

7501

MEMORANDUM

13 JUL 2005

From: T.W. Allen, VADM
Chief of Staff, U.S. Coast Guard

Reply to Attn of: CG-823
Mark Kulwicki
202-267-2294

To: Assistant Inspector General for Audits

Subj: IMPROVED SECURITY REQUIRED FOR U.S. COAST GUARD NETWORKS

Ref: (a) Draft Report dated June 28, 2005

1. This memo transmits our comments to the Department of Homeland Security Inspector General (DHSIG) draft report findings and recommendations contained in reference (a).

2. We have reviewed the draft report and generally concur with the findings and recommendations. We have provided some technical comments and corrections for your consideration.

3. The Coast Guard appreciates the opportunity to comment on this report and will continue our efforts to reduce our network vulnerabilities. We continually strive to improve the security of the network as we realize the critical importance it plays in the conduct of daily operations of the Coast Guard and welcome external evaluations of our systems. Because this report highlights Coast Guard vulnerabilities, please do not publish the full context of your findings on your web site and redact information as appropriate. If you have any questions, please contact Mark Kulwicki at (202)-267-2294.

#

Enclosure: U.S. Coast Guard Comments

UNITED STATES COAST GUARD
STATEMENT ON INSPECTOR GENERAL REPORT

TITLE: "Improved Security Required for U. S. Coast Guard Networks" (Draft Report dated June 9, 2005)

The overall finding of the report indicates that the Coast Guard has not implemented adequate controls for protecting its networks. In that regard, the Coast Guard has the following comments:

Recommendation #1. Implement a security testing program for CGDN+ (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. One centralized group should be responsible for ensuring that security testing is performed periodically on the CGDN+ (including the LANs connected to it).

Concur. As noted in the report, the Coast Guard performs vulnerability scans of the networks and its components, but not on regimented basis or in accordance with an established policy. Since the time of the audit, the CG CIRT has implemented the Vulnerability Assessment and Penetration team to design, test, implement, and maintain Coast Guard wide vulnerability scanning and penetration program. The team has the responsibility for ensuring security scanning and testing is performed regularly on the CGDN+ network.

Recommendation #2. Develop, update, and implement policies as well as procedures for standard configuration of network devices, and passwords, as required by DHS Policy and DHS Handbook.

Concur. The audit accurately documented the differences between the Coast Guard and DHS policies regarding password management. We will review and revise the Coast Guard policy to comply with the DHS policy. As part of this effort, we will examine the policy requirements of our DOD relationship and .MIL status and revise as applicable. Where there are differences between DHS and DoD policy, the Coast Guard will apply the more restrictive policy whenever possible. This policy and procedure evaluation and revision and subsequent standardization of the configuration of network devices will be accomplished within 9 months.

Recommendation #3. Centralize the configuration and patch management process to ensure that all network devices are properly configured and all necessary patches are applied in a timely manner to reduce the risk of system compromise or failure. All high and medium vulnerabilities that are identified should be addressed and corrected.

Concur. At the time this DHS IG review was conducted, the Coast Guard's implementation of [redacted] was not yet mature or fully fielded within the Coast Guard. We now have [redacted] in place for automatic patch management for all workstations and servers. All Coast Guard servers and workstations are now up-to-date regarding [redacted] security vulnerability patches. The CGCIRT has established the

Vulnerability Assessment and Penetration Team for the Coast Guard. The CGCIRT at TISCOM is the central source of CG-wide management of [redacted] alerts and patch management. The CGCIRT also provides guidance and toolset of local ISSOs (Information System Security Officers) for specific security tasks to ensure compliance with standardization of security policy and configuration of network devices. This team is tasked to perform scanning, penetration testing, integrity checking and password analysis for the entire Coast Guard. Scan results will be used to report standard workstation vulnerabilities and [redacted] compliance for the Coast Guard. This Team has worked with TISCOM's standard workstation engineers over the past two months to ensure all vulnerabilities have been patched on the standard workstation. Standard practices are now in place to ensure new vulnerabilities are patched in a set time period, as applicable.

While [redacted] enables automated patch deployment, it does not provide a good tool to track actual installations of a patch. Once [redacted] replacement patch installation tracking will improve. [redacted] is now commercially available. The Coast Guard Telecommunications & Information Systems Command (TISCOM) is developing a testing and implementation plan with deployment scheduled to begin by the end of FY05 and continuing through calendar 2006. The Coast Guard is also exploring the use of [redacted]. This product will enable a central location to not only scan a computer to determine its patch status, but to remotely apply any patches that were found to be missing [redacted] is a solution we will look to in the future to do this from a central location (such as the Coast Guard's Enterprise Management Facility). However, acquiring the funding for the acquisition of SMS and the engineering of this complex product are issues that preclude setting a date for projected deployment. Funding and engineering resources would be necessary to completely centralize the patch management at the CGCRT.

In regards to the WAN router configuration referenced in the report, these are centrally managed and maintained in a standard configuration. The configuration is controlled by Coast Guard network engineers and maintained by the contractor hired to operate and monitor the network.

Recommendation #4. Develop, update, and implement policies as well as procedures to ensure audit trails are reviewed and maintained.

Concur. As noted in the report, [redacted]. This is due to the current decentralized management of the servers. The Coast Guard is currently in the process of implementing the Windows Server 2003 operating system across the Coast Guard. As part of this implementation an Enterprise Management Facility has been established to provide the centralized server management necessary to allow for a periodic, systematic review of server audit logs for the enterprise servers. The Windows 2003 Active Directory solution provides the capability to perform specific logging for workstations and servers based on established policy. The Coast Guard will establish the policy and procedures for auditing and how system logs will be monitored and by whom within 6 months after IOC (Initial Operating Capability) for the Windows Server 2003 implementation.

The Windows Server 2003 implementation has begun and is scheduled to be complete in Q4FY07. The policy will be implemented by Q2FY08. For those servers that remain under decentralized field management, policy requiring the review of server logs on a regular basis will be developed within 6 months.

Recommendation #5. Test the contingency plan for all systems at least annually.

Concur. As noted in the report the CGDN+ contingency plan was developed in 2004. The plan essentially addresses the loss of service at the contractors network control center (NCC) due to various types of emergencies. The continuous operation of the NCC is vital to monitoring the health of the network and for immediate discovery of network outages. Due to the critical nature of the NCC, the contractor maintains a geographically diverse, hot back up site that is always on line. It is a fully equipped and operational control center. A **monthly test** is performed by the contractor to verify the capability of the Backup NCC to assume the required functions. The plan is reviewed and analyzed by the contractor on a periodic basis to ensure its accuracy. The contingency plans for all other Government Owned/Government Operated Network devices are addressed in each site's contingency and disaster recovery plans documented in the SSP (System Security Plan) or SSA (System Security Authorization Agreements) and required to be tested yearly.

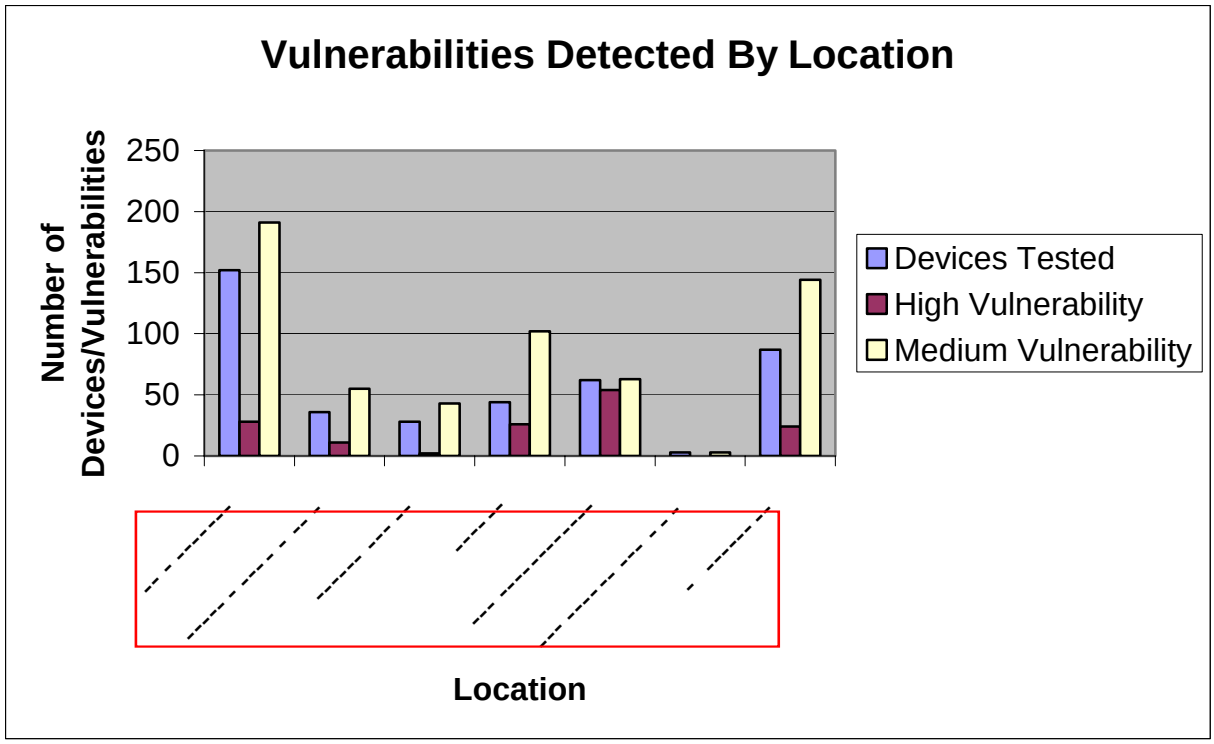
Recommendation #6. Develop, update, and implement policies as well as procedures to define the acceptable use of wireless technologies, and the consequences of non-compliance. Perform scans for rogue wireless devices regularly.

Concur. The Coast Guard is finalizing enterprise practices regarding the acceptable use of wireless technologies. The practice will provide a comprehensive policy to govern the implementation and use of wireless networks within the Coast Guard. It contains standard configuration requirements, as well as requirements for the implementing program managers to provide monitoring. This practice is expected to be approved before the end of this fiscal year.

The CGCIRT has established the Vulnerability Assessment and Penetration Team for the Coast Guard. This team is tasked to perform scanning, penetration testing, integrity checking and password analysis for the entire Coast Guard. The team also provides guidance for local ISSOs in tools and techniques for testing for rogue wireless devices in the area of responsibility on a regular basis.

Other Technical Comments and Corrections:
As a network that operates as part of the .mil domain and connects to the DoD NIPRNET, the Coast Guard Data Network security has been, and continues to be routinely reviewed by the DISA and NSA. The DISN Security Accreditation Working Group (DSAWG) annually reviews our security configurations and has repeatedly recommended to the DOD Global Information Grid (GIG) Waiver Panel to approve our connection to NIPRNET. The NSA has scanned our network with both Red and Blue Team scans. The latest scan was in June 2003 by the NSA Blue Team. The results of that scan were favorable to the network.

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 and their knowledge of 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]	152	28	191
[redacted]	36	11	55
[redacted]	28	2	43
[redacted]	44	26	102
[redacted]	62	54	63
[redacted]	3	0	3
[redacted]	87	24	144
Total	**412**	**145**	**601**

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

Appendix E
Configuration Weaknesses Identified By Location

Location	# Devices tested	Configuration Weaknesses Identified						
[redacted]	62	0	37	0	1	0	3	13
[redacted]	152	2	131	0	0	0	5	6
[redacted]	36	4	4	1	0	1	4	1
[redacted]	28	0	20	0	0	0	5	1
[redacted]	44	6	31	0	1	0	0	0
[redacted]	3	0	2	0	0	0	0	0
[redacted]	87	7	95	1	0	0	4	2
Total	**412**	**19**	**320**	**2**	**2**	**1**	**21**	**23**

Information Security Audits Division

Edward G. Coleman, Director
Jeff Arman, Audit Manager
Chiu-Tong Tsang, Audit Team Leader
Benita Holliman, Auditor
Evan Portelos, Associate
Chris Udoji, 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
Office of Security
Chief Information Officer
Chief Information Security Officer
Public Affairs
Legislative Affairs
U.S. Coast Guard, Commandant
U.S. Coast Guard, Chief Information Officer
U.S. Coast Guard, 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.