DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Enhanced Configuration Controls and Management Policies Can Improve USCG Network Security (Redacted)

Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. A review under the Freedom of Information Act will be conducted upon request.

OIG-08-82

August 2008

Office of Inspector General

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

Homeland Security

AUG 15 2008

MEMORANDUM FOR: Admiral Thad W. Allan
Commandant
U.S. Coast Guard

Richard L. Skinner

FROM: Richard L. Skinner
Inspector General

SUBJECT: *Letter Report: Enhanced Configuration Controls and Management Policies Can Improve U.S. Coast Guard Network Security*

We initiated an audit to determine whether the U.S. Coast Guard (USCG) has implemented adequate security controls and policies for protecting its network infrastructure. Network connectivity increases a computer system's vulnerability to threats, such as data theft, tampering, and service disruptions. The proper management of network connections, both internal and external, is vital in reducing the risks associated with the loss, misuse, unauthorized access, or modification to data processed and stored on a network.

The USCG has implemented effective controls for protecting its network infrastructure; however, USCG management needs to take additional steps to ensure that the [redacted] security of its network is not compromised by existing vulnerabilities. We recommend that the USCG enhance its [redacted] configuration controls in compliance with Department of Homeland Security (DHS) information technology security policies and practices. Additionally, the USCG should develop guidelines and procedures to address the configuration management of and [redacted] to its network infrastructure and [redacted] security [redacted].

We hope our recommendations will be of assistance as you move forward to implement actions to further protect your network infrastructure. Should you have any questions, please call me, or your staff may contact Frank Deffer, Assistant Inspector General, Information Technology, at (202) 254-4100.

Background

A system's network connections are the primary targets of most information technology (IT) security attacks. Network connectivity has become an intrinsic part of conducting business; thus, making security planning and controls very important. Network security encompasses remote access, network tuning and monitoring, external connections, boundary protection, internet usage, electronic mail security, and vulnerability management. Sound network security practice dictates that all network connections be identified and that threats and vulnerabilities associated with these connections be analyzed. The network infrastructure is the first line of defense between the Internet and networked information systems. Network security monitoring, detection, and analysis are key functions and are critical to maintaining the security of networked information systems. Vulnerability management, which is a combination of detection, assessment, and mitigation of weaknesses, is critical to reducing the risks associated with unauthorized access to network devices, systems, and data.

Information systems and networks are necessary for USCG business. Communications capabilities are needed by USCG personnel stationed on land, as well as those individuals that are at sea on its cutters. The Coast Guard Data Network Plus (CGDN+) supports USCG's sensitive, operational, and administrative information systems, as well as unclassified e-mail transmission and delivery. The CGDN+ Backbone is a modern common-user Transmission Control Protocol/Internet Protocol routed wide area network (WAN). The Backbone allows the transfer of sensitive information across the WAN. The Backbone design supports all Coast Guard districts and major commands. The network infrastructure extends across the continental U.S., and includes Alaska and Hawaii.

The CGDN+ backbone consists of [redacted]. The CGDN+ system infrastructure includes [redacted] systems. Four point of presence (POP) sites control access to CGDN+. Each POP supports external routers that provide for the transfer of sensitive but unclassified operational and administrative information. The firewall provides filtering of network traffic to protect against security intrusions, as well as controlling and authenticating access to each POP. The POP sites are:

- USCG Commandant (COMDT), located in [redacted].
- USCG Financial Center (FINCEN), located in [redacted].
- USCG Operations Systems Command (OSC), located in [redacted].
- USCG Electronics Systems Support Unit (ESU), located in [redacted].

Coast Guard cutters in port are provided pier side connectivity to CGDN+ by their respective supporting stations, via a T1 capable link. When at sea, minimal connectivity to CGDN+ is provided through a commercial satellite link, which must employ [redacted] for transmission security. The shipboard network connections generally consist of a router, switch, virtual private network, servers, and workstations. Network and system security patches and updates are deployed when the cutters [redacted].

The USCG's Telecommunications and Information Systems Command (TISCOM) centrally manages CGDN+ and the POPs. Additionally, cutter connectivity to CGDN+ is entirely under the purview of TISCOM. TISCOM is responsible for all issues relating to the [redacted] security of CGDN+, including the configuration management of the [redacted], providing guidance to the POP sites when policy changes require modification of the [redacted], maintaining and replacing cutter network devices, managing backups, alert notifications, and incident response. The POP site teams are responsible for providing and maintaining remote access service engineering support for access to CGDN+ 24 hours a day/7 days a week.

In addition to assessing the security of the [redacted] for CGDN+ at the POPs and aboard four selected USCG cutters, we conducted wireless scans for possible rogue network access points at the POP sites and aboard the cutters. We also interviewed TISCOM personnel regarding network administration and evaluated access control and other security policies implemented to protect its network devices, systems, and data. The diagram below depicts an overview of CGDN+, and the devices and locations where we performed testing.

Source: [redacted]

Results of Audit

The overall security posture of the CGDN+ infrastructure is good. Network [redacted] security [redacted] are effectively protecting USCG's network and data. Redundant firewalls are protecting each of the POP sites. [redacted] firewalls are configured to block connection attempts to scan the network. Auditing and logging is performed by a syslog server, and firewall logs are monitored daily for intrusion attacks. TISCOM employs two intrusion detection applications, which run simultaneously and are used to actively monitor and analyze incoming and outgoing network traffic 24 hours a day/7 days a week. No rogue network access points were discovered. We verified that USCG cutter network devices and system connections are patched when they [redacted]; and physical access to network devices aboard the cutters is restricted. Overall, the USCG's management of its network security is consistent with a majority of the policies, practices, and controls required by the *Department of Homeland Security's (DHS) 4300A Sensitive Systems Handbook*, DHS' *CISCO Router Secure Baseline Configuration Guide*, and the National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.

While USCG has been vigilant in its efforts to secure its network infrastructure, we identified system vulnerabilities and areas of noncompliance with DHS' configuration [redacted] on its network [redacted]. If these issues are not addressed, they may compromise USCG's [redacted] security. In addition, important policies and procedures related to network access controls have not been developed. The additional measures we are recommending can be easily implemented without affecting USCG operations and will decrease the risks associated with the issues we identified.

[redacted] Should Be Addressed

A number of management, operational, and technical controls impact network security, including identification and authentication controls, audit logging, integrity controls, and periodic reviews of programs/systems to determine whether changes that could adversely affect security have occurred. While USCG has implemented the majority of these controls, we identified several [redacted] configuration [redacted] on its network [redacted] security [redacted] that could adversely impact the security of its network infrastructure. Specifically, we identified:

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

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

Per DHS guidance, firewalls, when used in concert with a variety of additional security controls, such as IDSs and authentication procedures, provide a level of assurance that unauthorized personnel will be unable to access departmental systems and have proven to be an effective means for securing a network. DHS requires that:

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

The use of [redacted] are inherently critical high-risk vulnerabilities. While the risk to USCG's network infrastructure for the majority of the vulnerabilities identified above could be considered low, together they present a medium to high risk because they can potentially provide an attacker with the means to gain unauthorized access to USCG's network. For example, an attacker can use [redacted] and gain unauthorized access to the USCG network. The unauthorized or the non-intended use of [redacted] poses a potential avenue for unfettered or even covert access to other devices or systems within the infrastructure. The use of [redacted] is associated with numerous vulnerabilities from attackers gaining access to [redacted] with network [redacted]. USCG needs to address these [redacted] involving the configuration [redacted] allowed on CGDN+ to better protect the confidentiality, integrity, and availability of its systems and data, and comply with DHS requirements.

Additional Policies and Procedures Should Be Developed

USCG has implemented guidelines and procedures pertaining to wireless access, standard configurations for workstations, patch management, and incident detection and response. However, USCG has not developed an access control policy or remote access policy to govern employees' access to the USCG network via modem or accessing the USCG network via the Internet. Additionally, USCG management acknowledged that its employees are [redacted].

Per DHS policy, components are required to implement access control measures that provide protection from unauthorized alteration, loss, unavailability, destruction, or disclosure of information. Access control policies are designed to reduce the risk of an individual acting alone from engaging in fraudulent or malicious behavior. Data communication connections via modem are to be limited and tightly controlled because these connections can be used to circumvent security controls intended to protect DHS networks. Data communication connections are not allowed unless the component's Information Systems Security Manager has authorized them. Furthermore, DHS policy does not allow the [redacted] DHS information and systems.

There are significant security risks associated with remote access and dial-in capabilities. Proper procedures and management of network connections are vital in mitigating these risks. If untrusted or uncleared persons obtain unauthorized access, they can violate the integrity, confidentiality, and availability standards of the department. Furthermore, though USCG uses [redacted] to ensure that its [redacted]. For example, USCG does not verify that [redacted] to reduce the risks of compromising CGDN+. Therefore, USCG has no reasonable assurance that the employees' personal [redacted] to the level that is acceptable in accordance with DHS security policy and practices.

Recommendations

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

Recommendation #1: [redacted] or otherwise address the [redacted] configuration [redacted] in accordance with DHS policy, including the use of [redacted].

Recommendation #2: [redacted].

Recommendation #3: Ensure that [redacted] [redacted], are [redacted].

Recommendation #4: Develop and implement security procedures for quarterly firewall testing, perimeter security testing, access control, and remote access.

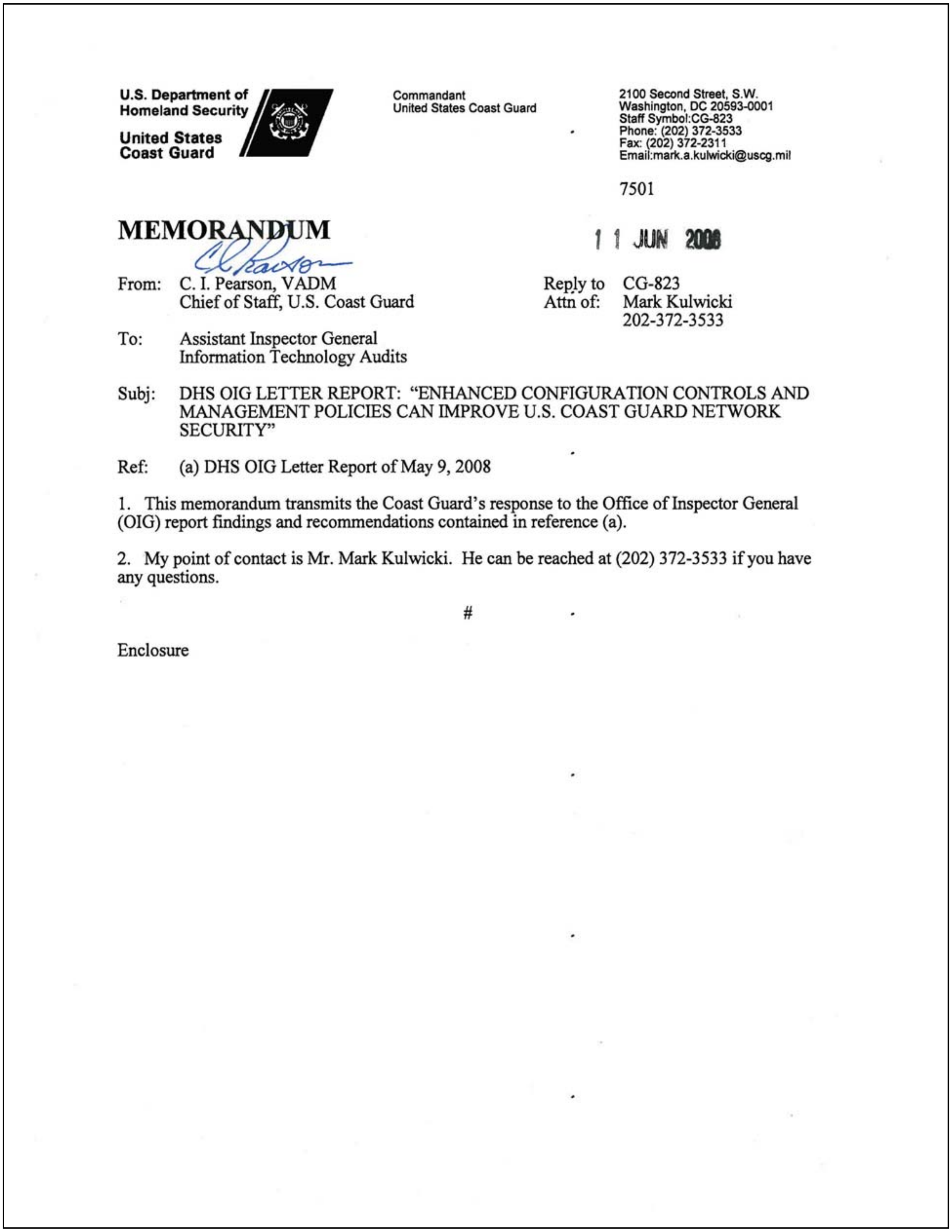
Recommendation #5: Prohibit the use [redacted] [redacted] DHS information and systems.

Management Comments and OIG Analysis

We obtained written comments on a draft of the report from Chief of Staff for USCG. We have included a copy of the comments in Appendix A. The Chief of Staff concurred with four of the five recommendations. The Chief of Staff for the USCG partially concurred with recommendation #5 because USCG will request a waiver from the DHS requirements. We reviewed the USCG management's response and agree that the steps USCG plans to take satisfy the recommendations.

****

We conducted our audit from October 2007 to May 2008 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards.



U.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) 372-3533
Fax: (202) 372-2311
Email:mark.a.kulwicki@uscg.mil

7501

MEMORANDUM

11 JUN 2008

From: C. I. Pearson, VADM
Chief of Staff, U.S. Coast Guard

Reply to Attn of: CG-823
Mark Kulwicki
202-372-3533

To: Assistant Inspector General
Information Technology Audits

Subj: DHS OIG LETTER REPORT: "ENHANCED CONFIGURATION CONTROLS AND MANAGEMENT POLICIES CAN IMPROVE U.S. COAST GUARD NETWORK SECURITY"

Ref: (a) DHS OIG Letter Report of May 9, 2008

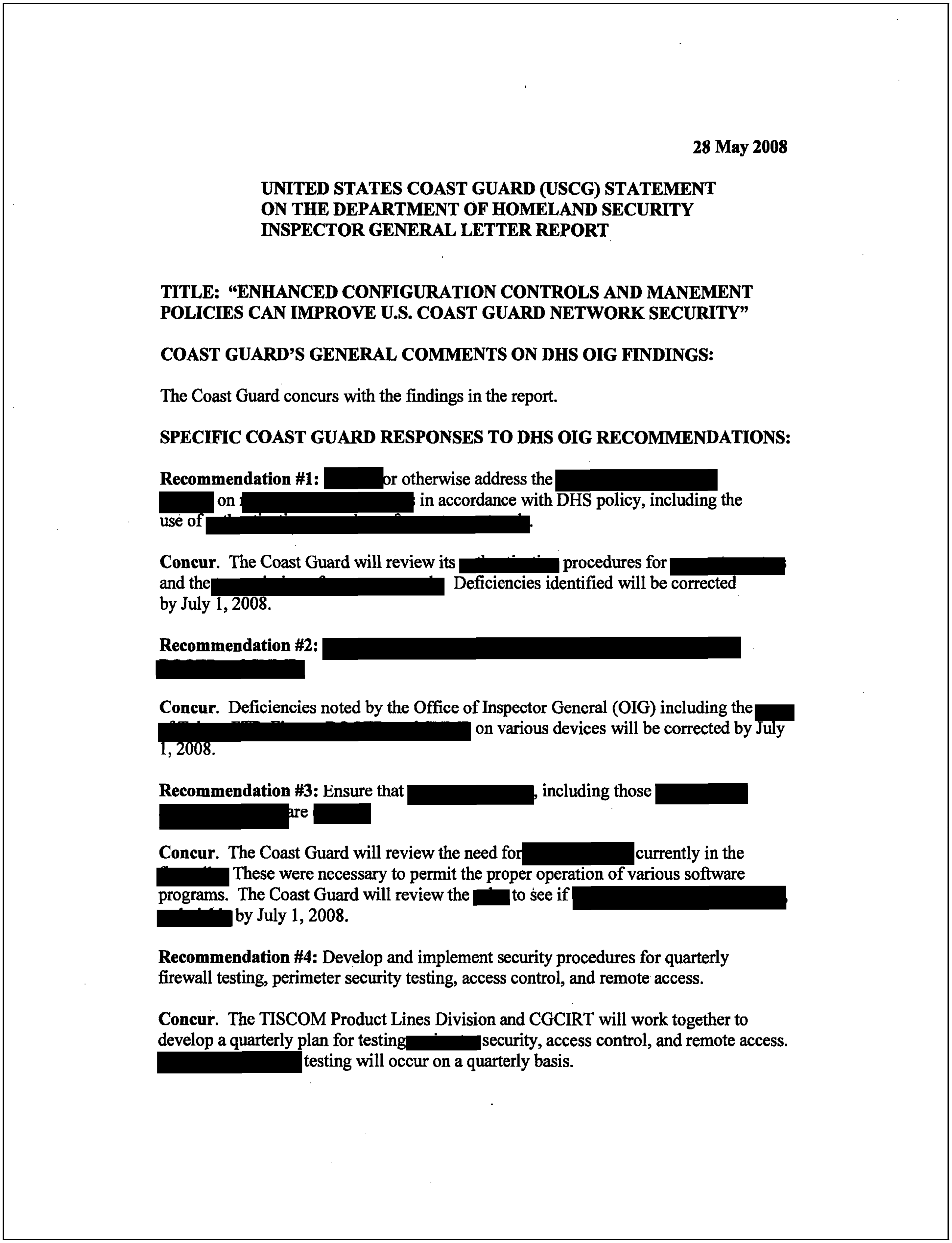
1. This memorandum transmits the Coast Guard's response to the Office of Inspector General (OIG) report findings and recommendations contained in reference (a).

2. My point of contact is Mr. Mark Kulwicki. He can be reached at (202) 372-3533 if you have any questions.

#

Enclosure

Appendix A
Management Response



28 May 2008

UNITED STATES COAST GUARD (USCG) STATEMENT ON THE DEPARTMENT OF HOMELAND SECURITY INSPECTOR GENERAL LETTER REPORT

TITLE: "ENHANCED CONFIGURATION CONTROLS AND MANEMENT POLICIES CAN IMPROVE U.S. COAST GUARD NETWORK SECURITY"

COAST GUARD'S GENERAL COMMENTS ON DHS OIG FINDINGS:

The Coast Guard concurs with the findings in the report.

SPECIFIC COAST GUARD RESPONSES TO DHS OIG RECOMMENDATIONS:

Recommendation #1: [redacted]r otherwise address the [redacted] on [redacted] in accordance with DHS policy, including the use of [redacted].

Concur. The Coast Guard will review its [redacted] procedures for [redacted] and the [redacted] Deficiencies identified will be corrected by July 1, 2008.

Recommendation #2: [redacted]

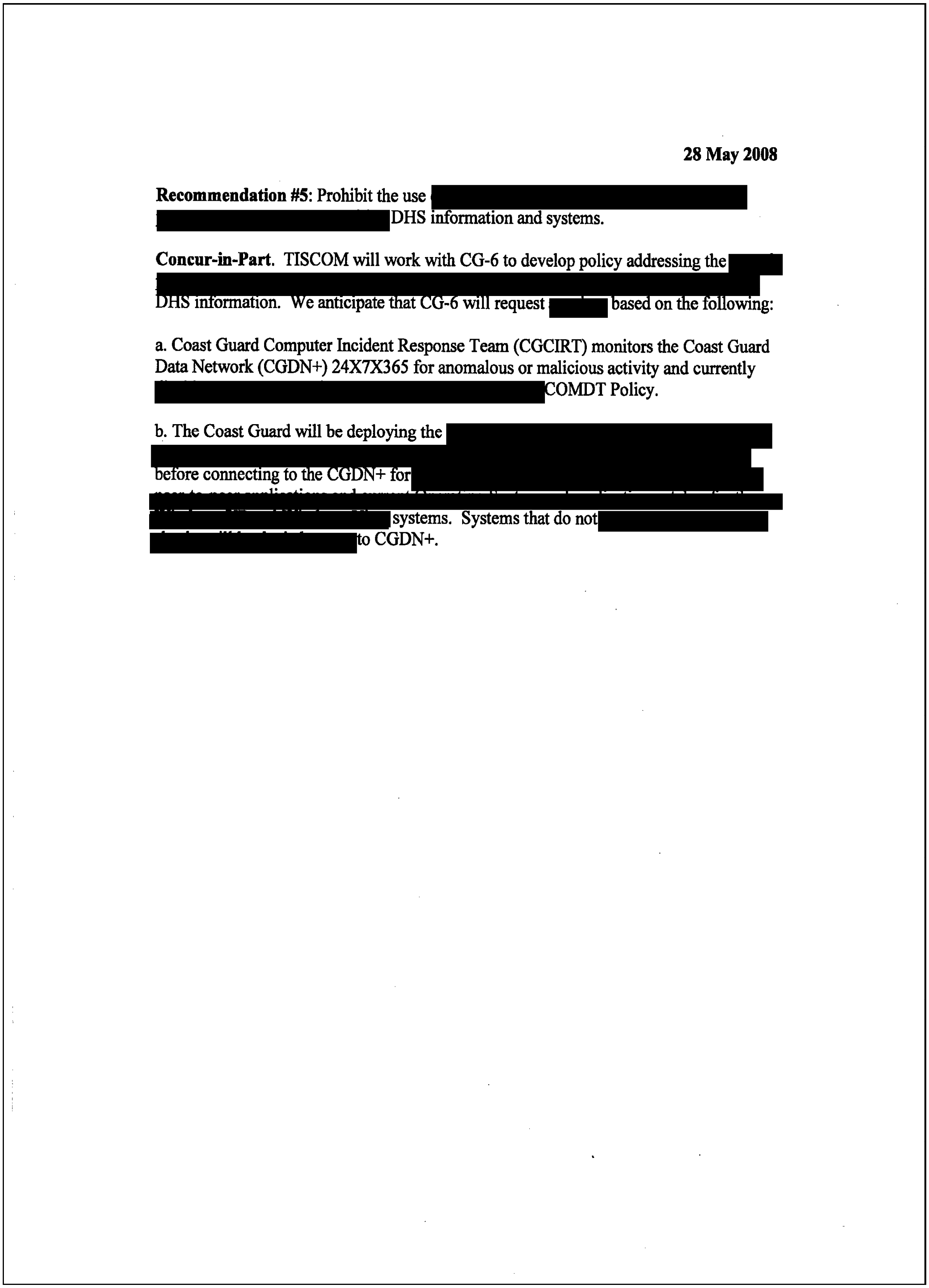
Concur. Deficiencies noted by the Office of Inspector General (OIG) including the [redacted] on various devices will be corrected by July 1, 2008.

Recommendation #3: Ensure that [redacted], including those [redacted]are [redacted]

Concur. The Coast Guard will review the need for [redacted] currently in the [redacted] These were necessary to permit the proper operation of various software programs. The Coast Guard will review the [redacted] to see if [redacted] by July 1, 2008.

Recommendation #4: Develop and implement security procedures for quarterly firewall testing, perimeter security testing, access control, and remote access.

Concur. The TISCOM Product Lines Division and CGCIRT will work together to develop a quarterly plan for testing [redacted] security, access control, and remote access. [redacted] testing will occur on a quarterly basis.



28 May 2008

Recommendation #5: Prohibit the use [redacted] DHS information and systems.

Concur-in-Part. TISCOM will work with CG-6 to develop policy addressing the [redacted] DHS information. We anticipate that CG-6 will request [redacted] based on the following:

a. Coast Guard Computer Incident Response Team (CGCIRT) monitors the Coast Guard Data Network (CGDN+) 24X7X365 for anomalous or malicious activity and currently [redacted] COMDT Policy.

b. The Coast Guard will be deploying the [redacted] before connecting to the CGDN+ for [redacted] systems. Systems that do not [redacted] to CGDN+.

Appendix B
Major Contributors to This Report

Information Security Audits Division

Edward G. Coleman, Director
Barbara Bartuska, Audit Manager
Tarsha Cary, Senior Auditor
Michael Horton, IT Officer
Thomas Rohrback, IT Specialist
Erin Dunham, Referencer

Advanced Technology Division

Richard Saunders, Director
Steve Matthews, Manager
Vincent Feaster, Electrical Engineer, SPAWAR
David Phelps, Computer Scientist, SPAWAR
Chad Cravens, Computer Scientist, SPAWAR
Birdie Rueangvivatanakij, Senior Security Analyst, Devine Consulting

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Under Secretary, Management
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Chief Information Officer
Chief Information Security Officer
DHS Audit Liaison
Chief Information Officer, USCG
Deputy Chief Information Officer, USCG
Chief, Office of Communications Systems, USCG
Information Systems Security Manager, USCG
Audit Liaison, USCG

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) 254-4199, fax your request to (202) 254-4305, 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 our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**
  DHS Office of Inspector General/MAIL STOP 2600, Attention:
  Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

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