

Department of Homeland Security **Office of Inspector General**

USCG Must Improve the Security and Strengthen
the Management of Its Laptops



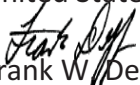


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

May 29, 2013

MEMORANDUM FOR: Rear Admiral Robert Day
Chief Information Officer
United States Coast Guard

FROM: 
Frank W. Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *USCG Must Improve the Security and Strengthen the Management of Its Laptops*

Attached for your action is our final report, *USCG Must Improve the Security and Strengthen the Management of Its Laptops*. We incorporated the United States Coast Guard's formal comments in the final report.

The report contains seven recommendations aimed at improving the laptop program's overall effectiveness. Your office concurred with all recommendations. As prescribed by the Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Attachment



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Executive Summary..... 1

Background 2

Results of Audit..... 4

 Actions Taken To Enhance Laptop and Wireless Security 4

 Laptop Acquisition and Inventory Management Controls Need Strengthening 6

 Weak Laptop Security Controls Put USCG Data at Risk 12

 Recommendations 17

 Management Comments and OIG Analysis 18

Appendixes

Appendix A: Objectives, Scope, and Methodology 20

Appendix B: Management Comments to the Draft Report 22

Appendix C: Major Contributors to This Report 25

Appendix D: Report Distribution 26

Abbreviations

CGOne	Coast Guard One Network
DHS	Department of Homeland Security
FY	fiscal year
IT	information technology
NPFC	National Pollution Funds Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
PII	personally identifiable information
SFLC	Surface Force Logistics Center
SOC	Security Operations Center
TISCOM	Telecommunication and Information Systems Command
USCG	United States Coast Guard
USGCB	United States Government Configuration Baseline



Executive Summary

The use of laptop computers with built-in wireless Internet features has increased the mobility and productivity of the Federal workforce. However, the popularity of laptops has also increased the risk of theft and unauthorized disclosure of sensitive data at Federal agencies. As of November 2012, the United States Coast Guard (USCG) reported more than 15,000 laptop computers in its inventory. These laptops are used by USCG's military personnel and civilian employees to perform their job functions both in the United States and abroad.

Our overall objective was to determine the effectiveness of USCG's efforts to protect its laptop computers and controls implemented to safeguard its laptops and wireless networks and devices from potential exploits. We reviewed USCG's policies and procedures for managing its laptop inventory. In addition, we reviewed the effectiveness of configuration management and technical controls implemented to protect the sensitive information processed by and stored on selected laptops.

USCG has taken actions to govern, track, and secure its laptops. For example, USCG has deployed a component-wide inventory database to account for its property, including laptops. Additionally, USCG has centralized the configuration and patch management of its standard laptops. USCG has also established policies and procedures for securing standard laptops and defining the authorized use of wireless devices, services, and technologies at the component.

USCG needs to improve its laptop acquisition and inventory management practices, and strengthen laptop security controls. Specifically, it needs to improve its laptop recapitalization program to eliminate excess quantities of unused laptops. In addition, it should reduce the acquisition of non-standard laptops, which represent a significant portion of the inventory. Non-standard laptops are acquired outside of the recapitalization program, and generally do not meet USCG security standards. Having large numbers of non-standard laptops that lack adequate security may compromise the integrity and confidentiality of USCG data and systems. Finally, USCG must improve the accountability of its laptop inventory and address deficiencies in implementing the required DHS configuration settings, deploying of security patches to its laptops timely, and developing and implementing procedures to erase and render sensitive data stored on laptop hard drives unrecoverable.

We are making seven recommendations to USCG. The component concurred with all recommendations and has begun to take actions to implement them. USCG's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.



Background

USCG, one of the five armed forces in the United States and the only military branch within the Department of Homeland Security (DHS), has a mission to protect the public, the environment, and our nation's maritime economic interests. As of March 2013, USCG comprises more than 92,000 active-duty service members, civilian employees, reservists, and auxiliary personnel who work as a responsive military force of maritime professionals both at home and abroad.

The mobility provided by laptop computers with built-in wireless Internet features has increased the productivity of the Federal workforce. However, the popularity of laptops across the Federal Government has also increased the risk of theft and unauthorized disclosure of sensitive data. To assist the component in accomplishing its mission, USCG personnel use both desktop and laptop computers to perform their assigned duties. As of November 2012, more than 15,000 laptops were reported in USCG's inventory. These laptops are used by USCG personnel while they are on temporary duty at a different location, teleworking, on travel, or on vessels.

The use of Institute of Electrical and Electronics Engineers 802.11x wireless technology is also becoming increasingly popular throughout the Federal Government.¹ Wireless networks extend the range of traditional wired networks and can offer Federal agencies many benefits in improving employee productivity and flexibility. However, wireless networks and devices also present security challenges, such as physical protection over wireless devices, eavesdropping, and unauthorized deployment of wireless networks.

In August 2005, we reported deficiencies in USCG's efforts to implement effective controls to protect its networks.² Specifically, we identified a rogue, or unauthorized, wireless access point operating at a USCG facility. In August 2008, we identified system vulnerabilities and areas of USCG's noncompliance with DHS configuration settings on network perimeter security.³ In December 2012, we reported that USCG could not ensure that personal property was efficiently reutilized or properly disposed of to prevent unauthorized use or theft. In addition, we determined that USCG did not have adequate policies, procedures, and processes to identify, screen, reutilize, and properly dispose of excess personal property.⁴

¹ The 802.11x (e.g., 802.11 a, b, g, and n) standards developed by the Institute of Electrical and Electronics Engineers are commonly used for transmission specifications on wireless local area networks.

² *Improved Security Required for U.S. Coast Guard Networks*, August 2005 (OIG-05-30).

³ *Enhanced Configuration Controls and Management Policies Can Improve U.S. Coast Guard Network Security*, August 2008 (OIG-08-82).

⁴ *Identification, Reutilization, and Disposal of Excess Personal Property by the United States Coast Guard*, December 2012 (OIG-13-19).

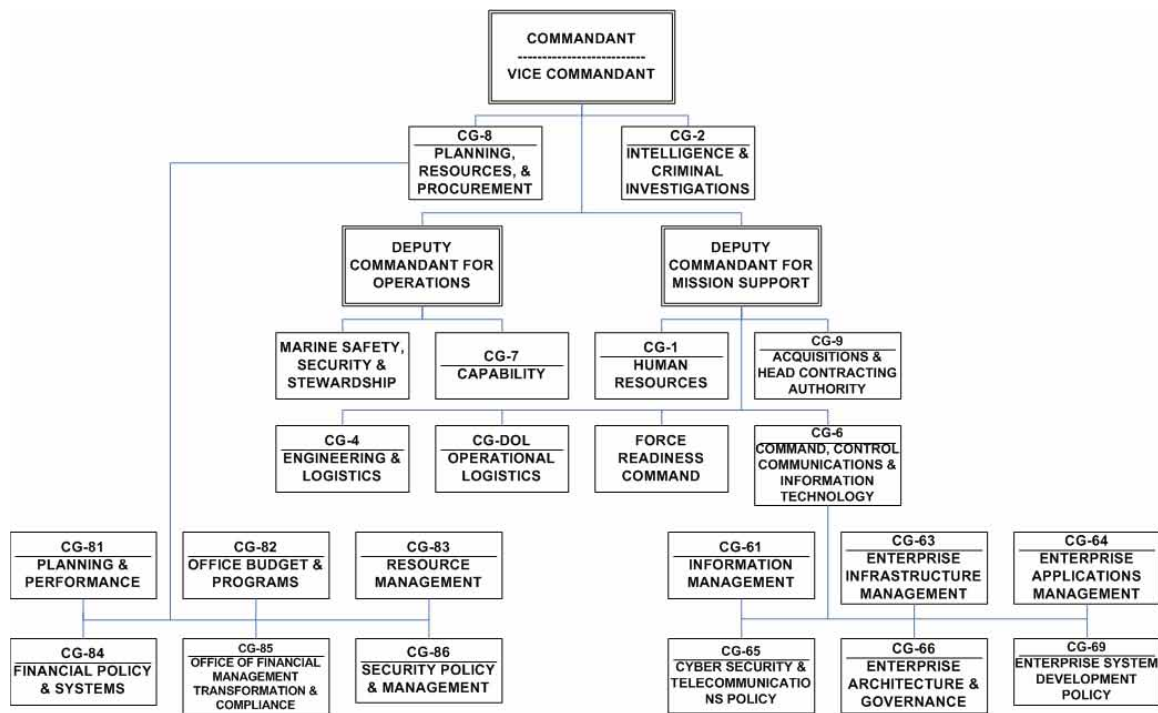


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The Office of Financial Policy and Systems (CG-84), which is part of USCG Headquarters' Planning, Resources, and Procurement Command (CG-8), is responsible for the overall management of the component's personal property. CG-84 develops and implements policies, procedures, as well as deploying systems for effective property management. In addition, commanding officers, officers-in-charge, and unit-level supervisors may designate Accountable Property Officers who are responsible for maintaining accountability, management, use, and control of property within the specified units they support. (Figure 1 presents an organizational chart.)

Figure 1. USCG Headquarters Organizational Chart



The Command, Control, Communications, Computers, and Information Technology Command (CG-6), which is part of USCG Headquarters, leads the Security and Information Assurance program to safeguard the component's information systems. The Telecommunications and Information Systems Command (TISCOM), which is part of CG-6, is responsible for centralizing the procurement, configuring, issuing, and providing information technology (IT) support of USCG's standard laptops.⁵ However, local units

⁵ Standard laptops are Microsoft Vista-based machines that are centrally managed by TISCOM and configured with certain security settings to provide the majority of USCG users with access to CGOne and IT resources.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

can obtain waivers to procure and manage non-standard laptops for uses that fall outside of the scope of standardized laptops. Non-standard laptops are used primarily by participants of the Common Access Control Remote Access System program while at home, offsite, or connecting from a location where ethernet cable Internet connections are not available.⁶ Non-standard laptops have also been deployed to facilitate the use of special-purpose software, such as disability assistance tools and access to social network websites to aid in maritime recovery operations.

Currently, USCG has not authorized wireless network connections to CGOne. However, local commands have deployed wireless networks that are provided by commercial Internet service providers for morale, education, and other public information purposes. While USCG is pilot testing the wireless local area network feature on its standard laptops, users with non-standard laptops can connect to CGOne remotely through a virtual private network connection over a wireless network.⁷

Results of Audit

Actions Taken To Enhance Laptop and Wireless Security

USCG has implemented an inventory management process to account for and safeguard its laptops. Specifically, USCG has implemented the following inventory management controls:

- Developed *Commandant Instruction M4500.5C, Personal Property Management Manual*, for the proper use, safekeeping, and disposal of the component's personal property.⁸
- Implemented an USCG-wide integrated property accountability system to keep track of the component's personal property.

⁶ As of January 2013, more than 10,000 USCG military and full-time employees were enrolled in the Common Access Card Remote Access Service program which grants authorized users remote access to Coast Guard One Network (CGOne), USCG's wide area network that connects various information systems and local area networks across the component enterprise.

⁷ Wireless adapters attached to laptops enable connectivity to a wireless local area network, which provides multiple users access to IT resources within a geographical area.

⁸ USCG defines "personal property" as any Federal property, except buildings, land, and structures, with an estimated useful life of more than two years, such as aircraft, vessels, boats, vehicles, trailers, major electronics systems, general purpose equipment, small arms, and computers.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Adopted unit-level policies and procedures for managing inventory records, performing inventory reviews, and ensuring that laptops are returned when a military member or an employee is transferred to a new unit.

As part of our audit, we used a laptop equipped with wireless scanning software to identify unauthorized networks that could be attributed to USCG. Our scans did not identify any unauthorized wireless networks at selected locations. In addition, USCG has taken the following actions to safeguard the sensitive data stored on and processed by its laptops and wireless networks and devices:

- Developed *Commandant Instruction M5500.13C, Security and Information Assurance Manual*, to define security and information assurance policies for USCG information systems and *Commandant Instruction 2010.2A, Use of Unclassified Wireless Devices, Services, and Technologies*, for the authorized use of wireless devices, services, and technologies.
- Deployed a host-based security system to strengthen security controls and prevent unauthorized access to information stored on the standard laptops connected to CGOne. The host-based security system was effective in thwarting our attempt to gain unauthorized access to information stored on selected standard laptops.
- Encrypted hard drives to protect sensitive USCG data stored on standard laptops.⁹
- Implemented a process to detect attempts to connect unauthorized wireless access points and devices to CGOne. In 2012, USCG detected and took quick remediation actions to respond to 16 attempts to connect unauthorized wireless networks or devices to CGOne. In addition, USCG is implementing a technical solution to automatically block unauthorized wireless access attempts.

Despite the actions taken by USCG to strengthen its inventory and configuration management controls, improvements are needed to ensure the security of its laptops and the sensitive data they process and store. Specifically, USCG must evaluate the effectiveness of its standard laptop recapitalization program and improve the

⁹ Encryption is a technique that uses an algorithm and a password to code and scramble data to prevent sensitive information from being read without proper authorization. When encryption is applied, an algorithm transforms plaintext into a coded equivalent known as ciphertext for transmission or storage. The coded text is subsequently decoded (decrypted) at the receiving or retrieval end and restored to plaintext.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

management oversight of its laptop inventory.¹⁰ Further, USCG needs to address deficiencies in reporting lost and stolen laptops, implementing the required Federal and DHS security control settings on laptops, and establishing procedures to erase and render sensitive data stored on laptop hard drives unrecoverable.

Laptop Acquisition and Inventory Management Controls Need Strengthening

USCG needs to improve its laptop acquisition and inventory management practices, and strengthen laptop security controls. Specifically, it needs to improve its laptop recapitalization program to eliminate excess quantities of unused laptops. In addition, it should reduce the acquisition of non-standard laptops, which represent a significant portion of the inventory. Non-standard laptops are acquired outside of the recapitalization program, and generally do not meet USCG security standards. As a result, having large numbers of non-standard laptops without adequate security may compromise the integrity and confidentiality of USCG data and systems. Finally, USCG needs to ensure that lost or stolen laptops are properly reported as security incidents as well as addressing the deficiencies in property inventory and headquarters' oversight of laptop inventory management at units.

Standard Laptop Recapitalization Program Is Not Effective

USCG needs to manage its laptop recapitalization program more effectively. The intent of the laptop recapitalization program is to modernize USCG's IT infrastructure and improve productivity by replacing obsolete equipment. However, in September 2012, USCG acquired 3,000 additional laptops when more than 2,000 laptops worth more than \$3 million were in storage at a warehouse.

Standard Laptops

As part of its responsibility to manage the USCG IT infrastructure, TISCOM is acquiring new standard laptops through a multi-year purchasing contract, which was recently renewed through fiscal year (FY) 2017, to recapitalize its servers, workstations, and laptops. In September 2011, TISCOM purchased 3,671 standard laptops for \$6.5 million. In September 2012, while most of the laptops purchased 12 months prior had yet to be issued, TISCOM acquired 3,000 additional laptops for \$4.4 million. As of December 3, 2012, 1,572 (43 percent) of the 3,671 laptops purchased in September 2011 had been issued and 5,099 total new laptops were awaiting issuance at a warehouse. According to the

¹⁰ Recapitalization refers to the physical replacement of facilities, aircraft, ships, and mission systems with new assets to meet operational requirements more effectively and efficiently.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

recapitalization schedule, TISCOM plans to replace the laptops purchased in 2011 and 2012 in 2014 and 2015, respectively, when most of these laptops have yet to be issued and more than 52 percent of USCG’s laptops are older than three years. Further, we estimate a laptop with the same processing capabilities as those purchased by TISCOM in September 2011 would have cost USCG \$290 less each, or \$608,710 in total savings, if purchased today. Figure 2 summarizes acquisition and deployment information about the laptops purchased for recapitalization.

Figure 2. Recapitalization Laptop Acquisition and Deployment Information¹¹

Description	Qty	Cost	Date Purchased	Date Received	Laptops Issued as of Dec 2012	Laptops at Warehouse as of Dec 2012
Dell E4310	35	\$66,150	9/15/2011	12/22/2011	15	20
Panasonic CF31	366	\$1,675,182	9/15/2011	11/15/2011	361	5
Dell E6510	3,270	\$4,806,900	9/15/2011	11/29/2011	1,196	2,074
Dell E6520	3,000	\$4,410,000	9/7/2012	10/24/2012	0	3,000
Total	6,671	\$10,958,232			1,572	5,099

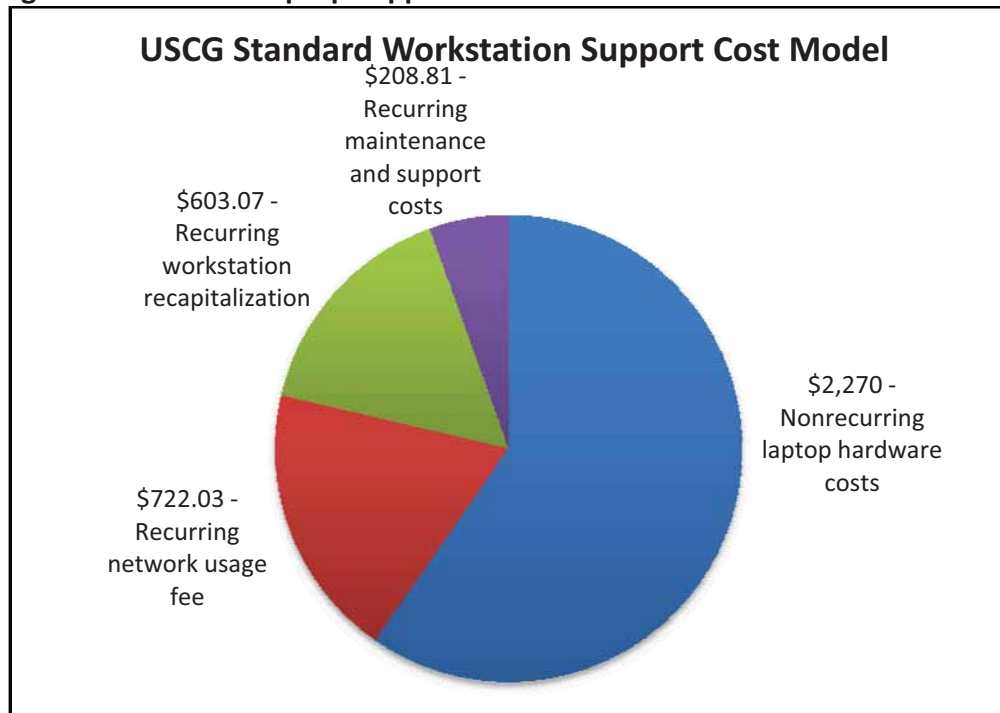
Under USCG’s recapitalization program, when TISCOM designates a standard laptop model as eligible for recapitalization, a memorandum is posted on USCG’s intranet notifying units that the model may be replaced with a new standard laptop. Units may submit a request to TISCOM to obtain the equipment.

For each standard laptop a local unit adds to their inventory, TISCOM charges support costs which include an initial charge of \$2,270 for the laptop hardware as well as the annual recurring costs of \$1,533.91. These fees are also charged when a unit decides to replace a non-standard laptop with a new standard laptop. Figure 3 summarizes of the costs associated with purchasing an additional standard laptop for a unit’s inventory or replacing a non-standard laptop through the recapitalization program.

¹¹ The Dell E6510 and E6520 laptops are stored together at the warehouse. We estimated the number of these laptops deployed and not deployed based on the “first in/first out” shipping method used at the warehouse.



Figure 3. Standard Laptop Support Cost Model



Non-Standard Laptops

As an alternative to requesting new or replacement standard laptops from TISCOM, units can purchase and manage non-standard laptops for uses that fall outside of the scope of standard laptops. Purchasing non-standard laptops allows units to select a preferred model, enable functionality restricted on standard laptops, and obtain laptops more quickly. While TISCOM has implemented a process to evaluate local units' requests to purchase non-standard laptops, the requirement to submit a waiver request before purchasing a non-standard laptop is not being enforced across USCG.

During our fieldwork, we determined that non-standard laptops are used primarily for connecting remotely to user workstations on CGOne. A non-standard laptop is procured and managed locally once a purchase request has been approved by TISCOM through the Information Technology Configuration and Control Board process. Based on our review of purchase requests since January 2008, 1,591 requests for non-standard laptops were approved, whereas only 1,246 standard laptops were approved. Further, CG-6 personnel said that additional laptops have been procured outside of the Information Technology Configuration and Control Board process for special programs and projects.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In many circumstances, support costs associated with recapitalization laptops may make them more expensive for units than acquiring their own non-standard laptops. For example, a field employee involved in the acquisition of recapitalized laptops within his unit noted that he did not understand the pricing model and felt that obtaining standard laptops was a hassle. A TISCOM employee acknowledged that the issuance of new laptops had not proceeded as quickly as planned, as many units preferred to purchase non-standard laptops. Further, a TISCOM employee told us that he believes that the recapitalization program did not have the support from USCG's management, as the units were not required or encouraged to participate.

Charging the units high support costs for standard laptops and allowing them to purchase non-standard laptops undermines the effectiveness of the recapitalization program. As a result, more than 8,200 of the laptops in the component's inventory (52 percent) are older than 3 years, and more than 5,000 new laptops are awaiting issuance at a warehouse. The prevalence of non-standard laptops also exposes USCG to security risks, as these laptops are not configured consistently. Figure 4 shows some of the new laptops purchased for recapitalization awaiting deployment at the warehouse.

Figure 4. Laptops Awaiting Deployment at the Warehouse





Some Lost or Stolen Laptops Are Not Accounted For or Consistently Reported to DHS

USCG is not accounting for all lost or stolen laptops in its inventory or consistently reporting lost or stolen laptops to the DHS Security Operations Center (SOC) as security incidents. Specifically, 7 of the 43 laptops that were reported as lost or stolen in FY 2012 had not been removed from USCG's inventory database as of November 2012. In addition, USCG only reports stolen laptops that are suspected of containing personally identifiable information (PII) to DHS SOC.

DHS requires components to report significant incidents to DHS SOC within one hour after the security event is confirmed as an incident.¹² Minor incidents must be reported within 24 hours. USCG requires that security incidents be reported immediately to the local Information Systems Security Officer, who shall notify the Coast Guard Computer Incident Response Team, the respective command, and the USCG Information Systems Security Manager of suspected or confirmed security incidents. Specifically, USCG's reporting requirements apply to any suspected or confirmed loss of USCG information, whether sensitive or PII.

Currently, individual users must notify their command when a laptop is lost or stolen, and the command in turn notifies CG-84. CG-84 is responsible for acknowledging reports of lost or stolen laptops from field units and tracking the asset and the conditions under which it was lost, and adjudicating the reports of survey. According to a CG-84 official, the Coast Guard Computer Incident Response Team is notified of lost or stolen laptops when they are suspected of containing PII. The official noted that such reports are handled only from a PII perspective. Since DHS SOC does not require components to submit a separate form or designate the incidents as lost or stolen, CG-84 does not track all incidences of lost or stolen laptops or reflect the missing equipment in the USCG inventory database.

Not reporting the loss or theft of laptops to DHS SOC prevents DHS and USCG officials from taking corrective actions to mitigate security risks. Also, it precludes DHS and USCG senior officials from knowing the extent of laptop security issues and may result in underreported security incidents in DHS' FY 2012 *Federal Information Security Management Act* submission.

¹² DHS defines a significant incident as a computer security-related incident that represents a meaningful threat to the Department's mission and requires immediate leadership notification.



Headquarters Does Not Review Laptop Inventory Results

USCG headquarters does not provide adequate oversight of personal property management at USCG units. Specifically, CG-84 does not enforce the requirement to have the units conduct annual inventories of sensitive personal property, including laptops. Because inventory results are not reported to Headquarters, CG-84 may be unaware of deficiencies in property management at units. Laptops are of particular importance because they are portable, are costly, and store sensitive USCG data.

We selected 185 laptops from Surface Force Logistics Center (SFLC), National Pollution Funds Center (NPFC), TISCOM, the District 8 office, and the Sector New Orleans office to determine whether laptops were properly accounted for in USCG's inventory. The results of our review identified instances where USCG's inventory database contained incorrect information, such as serial numbers of selected laptops that did not match the inventory records. Since the asset tags are not being used at the District 8 and Sector New Orleans offices, we could not use them as a means to validate the accuracy of information contained in USCG's inventory database. We were unable to locate 29 of the 185 selected laptops (15.7 percent), as shown in figure 5.

Figure 5. Results of 2012 Office of Inspector General Laptop Inventory Evaluation

Location	Laptops Selected	Laptops Located	Percent Located
SFLC Baltimore, MD	30	29	96.7%
NPFC Arlington, VA	45	40	88.9%
TISCOM Alexandria, VA	60	51	85.0%
District 8 Office New Orleans, LA	25	20	80.0%
Sector Office New Orleans, LA	25	16	64.0%
Total	185	156	84.3%

USCG requires each unit to conduct a physical inventory of all personal property annually. When inventory results indicate that a unit has not complied with the component's inventory policies and procedures, CG-84 is required to develop a plan specifying the steps to correct the deficiencies or discrepancies within a



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

specified time. USCG also requires that all personal property be bar-coded or otherwise labeled.

Although NPFC, SFLC, and TISCOM conduct inventories annually, the Sector and District 8 offices in New Orleans conduct inventories only when there is a change in property custodian. As a result of this practice, most of the laptops at the Sector and District 8 offices in New Orleans had not been subject to an inventory within the past year. Some laptops had not been inventoried since 2009.

According to property custodians, the main reason why selected laptops could not be located during our fieldwork was that users did not inform them to update the inventory database to reflect that assigned laptops had been transferred or disposed of. For most of these unaccountable laptops, documentation was subsequently provided confirming that the laptop had been disposed of or transferred to a different unit.

USCG units are required to report to CG-84 the total dollar amount of personal property that is reported lost, stolen, damaged, or destroyed annually. However, when inventories are not conducted to determine whether laptop computers are properly accounted for, lost, or stolen, the annual reports submitted to headquarters will not contain sufficient information to inform headquarters of inventory management deficiencies. Without this oversight, CG-84 cannot conduct follow-up to address the deficiencies in the management of the laptop inventory.

Weak Laptop Security Controls Put USCG Data at Risk

USCG has not implemented effective security controls on its laptops. Specifically, USCG has not implemented the required DHS and Federal configuration settings on its standard and non-standard laptops. In addition, we identified missing critical and high-risk security patches that are more than 6 months old on more than 95 percent of standard laptops tested.¹³ Finally, USCG has not developed procedures to erase and render sensitive data stored on laptop hard drives unrecoverable or document the execution of this process. Implementing effective security controls on USCG's standard and non-standard laptops will minimize the risk that sensitive information processed by and stored on these laptops can be compromised.

To evaluate USCG's compliance with United States Government Configuration Baseline (USGCB) requirements, we performed vulnerability assessments on 2,114 standard

¹³ Security patches help prevent exploitation of systems by mitigating vulnerabilities in installed software.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

laptops with a USCG-approved Windows Vista image that were connected to CGOne. We also evaluated the effectiveness of USCG's process to deploy security patches on its standard laptop computers. Finally, we reviewed selected non-standard laptops to determine whether required security controls were implemented.

Laptops Are Not Properly Configured

USCG has not configured its laptops with all required USGCB settings, which are needed to maintain an effective and standardized baseline of security controls on Windows workstations and laptops across the Federal Government.¹⁴ The following are examples of missing controls we identified from our testing:

- Telnet, which allows unencrypted communication between two computers where username, password, and subsequent data are transmitted in cleartext, is not disabled on 2,099 USCG laptops. DHS prohibits the use of Telnet.
- Internet Protocol Version 6 source routing protection is not enabled on 2,111 USCG laptops which may allow attackers to obscure the location of their computer and leave USCG unable to identify the source of incoming attacks.¹⁵
- The maximum data retransmission for Transmission Control Protocol is not set on 2,111 USCG laptops, increasing the likelihood of success for a denial-of-service attack.¹⁶

When new standard laptops are deployed locally, the units apply the TISCOM-developed Windows Vista image. Of the 343 applicable USGCB settings we evaluated on laptops configured with this image, USCG has either implemented or granted exceptions for 322, leaving 21 settings out of compliance. TISCOM centrally monitors and manages these standard laptops connected to CGOne by using Active Directory and System Center Configuration

¹⁴ In March 2007, the Office of Management and Budget issued M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, which requires Federal agencies to adopt the federally accepted configurations developed by National Institute of Standards and Technology (NIST), Department of Defense, and DHS.

¹⁵ Internet Protocol Version 6 is a communication protocol used to route traffic over the internet. It was designed to replace the aging Internet Protocol Version 4 communication protocol.

¹⁶ Transmission Control Protocol is a commonly used protocol that allows for the reliable transmission of data over a computer network.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Manager.¹⁷ In September 2010, the DHS Chief Information Security Officer approved USCG's waiver request to exempt the component from implementing six USGCB settings. Some examples of approved USGCB exceptions include renaming the default Windows Administrator account, setting a user session timeout, and disabling a user's ability to install printer drivers. However, USCG could not provide waivers or exceptions to account for the missing 21 (6 percent) USGCB settings, or explain why the waivers or exceptions had not been submitted to DHS.

The Office of Management and Budget requires Federal agencies to implement USGCB configuration settings on laptops and workstations to standardize and strengthen information security across the Federal Government. DHS requires components to submit a Waivers and Exceptions Request Form, signed by the component Chief Information Security Officer, who acknowledges and accepts the risk resulting from the unimplemented controls.

By not implementing all USGCB controls, USCG cannot ensure that the sensitive data processed by and stored on its laptop computers are protected from unauthorized access and potential misuse. A compromised standard laptop could be used to gain unauthorized access to CGOne and increase the risk that security controls could be circumvented.

Standard Laptops Are Missing Security Patches

USCG has not updated timely its standard laptops with the latest security patches. Our vulnerability scans identified 13 missing critical and high-risk security patches that were more than 6 months old for Oracle Java, Adobe Acrobat, Adobe Flash, and Adobe Shockwave software on more than 95 percent of standard laptops tested. Missing security patches may allow unauthorized users to exploit software vulnerabilities and take control of a laptop or gain access to sensitive information stored.

TISCOM is responsible for deploying software patches to all standard laptops connected to CGOne within 30 days of the patch release date. TISCOM uses System Center Configuration Manager to apply software updates within the required timeframe. However, according to TISCOM personnel, some of the missing security patches we identified are incompatible with the component's mission critical applications, such as the Core Accounting System, on some

¹⁷ Microsoft's System Center Configuration Manager software suite provides centralized management capabilities for application delivery, desktop virtualization, device management, and security.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

standard laptops.¹⁸ As a result, these patches were not deployed within the 30-day timeframe as required, and are currently pending deployment until the mission-critical applications can be updated to support the patches.

DHS requires components to mitigate system vulnerabilities by promptly installing security and software patches. Security patches protect systems from potential exploits and vulnerabilities as they are discovered. DHS SOC publishes Information Security Vulnerability Management messages that dictate the timeframe in which these patches must be installed.

Standard laptops remain at risk until the missing critical patches are applied. Failure to deploy software patches exposes laptops to risk depending on the severity of the vulnerability identified. Malicious software designed to exploit vulnerable systems can compromise the integrity of standard laptops. Ensuring that software is up-to-date minimizes this risk and protects standard laptops and the sensitive information they process and store.

Standard Configuration Settings Are Not Enforced on Non-standard Laptops

USCG has not implemented the required configuration control settings on its non-standard laptops as required by applicable DHS, Office of Management and Budget, and NIST guidance. Non-standard laptops, which represent a significant portion of the laptop inventory, are purchased locally and have security controls applied at the discretion of unit commanders and individual users. Insufficient central oversight has resulted in significant risk to the integrity and confidentiality of USCG data contained on these laptops.

We observed instances where non-standard laptops were missing required security controls. For example, our manual review of selected non-standard laptops at NPFC and the District 8 office revealed that the required hard drive encryption had not been enabled to prevent unauthorized users from gaining access to the data stored on the laptop. We determined that USCG was not enforcing the use of a strong password policy, nor was it implementing required USGCB configuration settings.

The *Federal Information Security Management Act* requires Federal agencies to develop, document, and implement policies and procedures that ensure compliance with the minimally acceptable system configuration requirements

¹⁸ USCG's primary accounting system, Core Accounting System, enables the procurement and payment of resources such as assets, services, and logistic support.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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 requires that component information systems comply with its hardening guides for operating systems and configuration guides for applications. In addition, DHS requires that information stored on a laptop be encrypted if the laptop is used at a residence or on travel.

Non-standard laptops are only authorized to connect to CGOne through a remote desktop connection, and thus are not subject to the centralized, network-based system that USCG has in place for managing enterprise wide security. As a result, USCG cannot ensure that the non-standard laptops used to conduct USCG business and that the data they store are secure and protected from potential misuse.

Procedures to Erase and Render Sensitive Data Stored on Laptops Unrecoverable Are Needed

USCG does not have a process to ensure that sensitive data stored on its laptops is rendered unrecoverable before the laptops are transferred or disposed of. Specifically, USCG has not implemented procedures to ensure sensitive data stored on laptops cannot be recovered. Further, USCG does not document or certify execution of this process. When the process to erase sensitive data is not consistently performed, there is greater risk that data may be retrieved and reconstructed from laptop hard drives.

Although records are maintained to document execution of the process at SLFC and NPFC, the District 8 office, Sector New Orleans office, and TISCOM do not maintain documentation. When a laptop is to be disposed of, its hard drive is removed to be either physically destroyed onsite or sent to an off-site facility for destruction. However, when laptops are transferred to another user or unit in USCG or are donated to schools, the methods used to erase data from hard drives vary.

DHS requires components to maintain records of the execution of processes to erase data from storage media. Further, Component Chief Information Security Officers or Information Systems Security Managers are required to develop and implement procedures to erase data from storage media. These procedures ensure that any information systems storage medium containing sensitive information is erased and rendered unrecoverable before it is disposed of, reused, recycled, or returned to the owner or manufacturer.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

When USCG personnel do not erase data from hard drives and record execution of the process consistently, they cannot ensure that laptop hard drives containing sensitive information have either been destroyed or erased to render deleted data unrecoverable. In addition, it is critical that an organization maintain records to document what media were destroyed, when and how they were destroyed, and the final disposition of the media.

Recommendations

We recommend that the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (CG-6):

Recommendation #1:

Restrict the purchase of non-standard laptops to those needed to perform special operations that cannot be conducted with standard laptops.

Recommendation #2:

Implement required USGCB and DHS configuration settings on all USCG laptops or follow applicable DHS policy to submit a waiver to acknowledge and accept the risk of non-compliance.

Recommendation #3:

Resolve the technical incompatibility with mission-critical applications that has caused delays in deploying security patches on USCG standard laptops.

Recommendation #4:

Evaluate the security risks associated with using non-standard laptops and establish a centralized configuration and patch management process according to applicable DHS and NIST guidance.

Recommendation #5:

Develop and implement documented procedures to ensure that data are erased and rendered unrecoverable from laptops before the equipment is disposed of or transferred, including the maintenance of records.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We recommend that the Assistant Commandant for Planning, Resources, and Procurement (CG-8):

Recommendation #6:

Establish procedures to ensure that all occurrences of lost or stolen laptops are reported to DHS SOC as security incidents and reflected in the USCG inventory database as exceptions.

Recommendation #7:

Enforce the requirement to have units submit the results of annual laptop inventories to Headquarters and work with units to correct any identified laptop inventory management deficiencies.

Management Comments and OIG Analysis

USCG concurred with recommendation 1. USCG will draft policy to remove non-standard laptops and develop a waiver process for special purpose equipment that requires a non-standard laptop.

We agree that the steps that the USCG plans to take begin to satisfy this recommendation. This recommendation will remain open until USCG provides documentation to support that planned corrective actions are completed.

USCG concurred with recommendation 2. USCG will establish a provisioning point/process to load USGCB settings.

We agree that the steps the USCG plans to take begin to satisfy this recommendation. This recommendation will remain open until USCG provides documentation to support that planned corrective actions are completed.

USCG concurred with recommendation 3. USCG will resolve the technical incompatibility with mission-critical applications.

We agree that the steps the USCG plans to take begin to satisfy this recommendation. This recommendation will remain open until USCG provides documentation to support that planned corrective actions are completed.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

USCG concurred with recommendation 4. USCG will evaluate security risks and establish a centralized configuration and patch management process according to applicable DHS and NIST guidance.

We agree that the steps that the USCG plans to take begin to satisfy this recommendation. This recommendation will remain open until USCG provides documentation to support that planned corrective actions are completed.

USCG concurred with recommendation 5. USCG will develop and implement procedures to ensure that data are erased and rendered unrecoverable from laptops before the equipment is disposed of or transferred, including the maintenance of records.

We agree that the steps that the USCG plans to take begin to satisfy this recommendation. This recommendation will remain open until USCG provides documentation to support that planned corrective actions are completed.

USCG concurred with recommendation 6. USCG will require that missing laptops be reported to the DHS SOC.

We agree that the steps that the USCG plans to take begin to satisfy this recommendation. This recommendation will remain open until USCG provides documentation to support that planned corrective actions are completed.

USCG concurred with recommendation 7. USCG will place emphasis on laptops and other similar items to ensure that they are identified as property and subject to policy and processes.

We agree that the steps that the USCG plans to take begin to satisfy this recommendation. This recommendation will remain open until USCG provides documentation to support that planned corrective actions are completed.



Appendix A

Objectives, Scope, and Methodology

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 as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The objective of our audit was to determine whether USCG has implemented effective controls to protect the sensitive data stored on and processed by its laptops and wireless networks and devices from potential exploits. Specifically, we determined whether USCG has implemented (1) an effective inventory management process to safeguard its laptop computers, (2) effective controls to protect its laptop computers, and (3) effective controls to ensure that sensitive information processed by its wireless networks and devices is protected from potential exploits.

Our audit focused on requirements specified in the *DHS Sensitive Systems Handbook 4300A*, *United States Government Configuration Baseline*, *Commandant Instruction M4500.5C*, *Personal Property Management Manual*, *USCG Commandant Instruction M5500.13C*, *Security and Information Assurance Manual*, and *Commandant Instruction 2010.2A*, *Use of Unclassified Wireless Devices, Services, and Technologies*. We interviewed selected personnel and management officials from CG-6, CG-8, and at selected fieldwork locations. Fieldwork was performed at USCG Headquarters in Washington, DC; Sector and District 8 Offices in New Orleans, LA; Surface Force Logistics Center in Baltimore, MD; TISCOM in Alexandria, VA; and National Pollution Funds Center in Arlington, VA.

We reviewed USCG policies and procedures for inventory maintenance, incident reporting, erasing and rendering data stored on laptop hard drives unrecoverable, configuration and patch management, and wireless network security. In addition, we conducted vulnerability and USGCB compliance scans using CoreImpact and Nessus on 2,114 standard laptops running Windows Vista operating system that are connected to CGOne. We could not evaluate whether effective controls have been implemented on USCG's wireless networks as the component has not authorized any wireless networks to connect to CGOne. However, we used AirMagnet software to determine whether unauthorized wireless networks are connected to CGOne. We also performed an inventory evaluation of 185 laptops. The laptops identified for our inventory evaluation were randomly selected from USCG's inventory database once we judgmentally identified locations for our site visits based on concentration of laptops.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We conducted this performance audit between October 2012 and February 2013 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Management Comments to the Draft Report

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



Commandant
United States Coast Guard

2100 Second Street, S.W., Stop 7245
Washington, DC 20593
Staff Symbol: CG-823
Phone: (202) 372-3533
Fax: (202) 372-2311

7501

MAY 10 2013

MEMORANDUM

From: S. P. Metruck, RDMC
COMDT (CG-8)

Reply to: Audit Manager
Attn of: Mark Kulwicki
(202) 372-3533

To: F. W. Deffer
Assistant Inspector General
Office of Information Technology Audits

Subj: DHS OIG DRAFT REPORT: "USCG MUST IMPROVE THE SECURITY AND
STRENGTHEN THE MANAGEMENT OF ITS LAPTOPS"

Ref: (a) OIG Project No. 12-172-ITA-USCG, dated April 10, 2013

1. This memorandum transmits the Coast Guard's response to the findings and recommendations identified in reference (a).
2. The Coast Guard concurs with the report's recommendations.
3. If you have any questions, my point of contact is Mr. Mark Kulwicki who can be reached at 202-372-3533.

#

Enclosure: (1) USCG Response



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**UNITED STATES COAST GUARD RESPONSE FOR DHS OIG DRAFT REPORT:
USCG MUST IMPROVE THE SECURITY AND STRENGTHEN THE MANAGEMENT
OF ITS LAPTOPS (OIG PROJECT NO. 12-172-ITA-USCG)**

RECOMMENDATIONS AND USCG RESPONSES

Recommendation #1: *Restrict the purchase of non-standard laptops to those needed to perform special operations that cannot be conducted with standard laptops.*

USCG response: Concur. The Coast Guard will draft policy to remove non-standard laptops and develop a waiver process for special purpose equipment that requires a non-standard laptop.

Recommendation #2: *Implement required USGCB and DHS configuration settings on all USCG laptops or follow applicable DHS policy to submit a waiver to acknowledge and accept the risk of non-compliance.*

USCG response: Concur. The Coast Guard Command, Control, Communications, Computers, and Information Technology Service Center (C4IT SC) will establish a provisioning point/process to load USGCB settings.

Recommendation #3: *Resolve the technical incompatibility with mission-critical applications that has caused delays in deploying security patches on USCG standard laptops.*

USCG response: Concur. The Coast Guard will resolve the technical incompatibility with mission-critical applications.

Recommendation #4: *Evaluate the security risks associated with using non-standard laptops and establish a centralized configuration and patch management process according to applicable DHS and NIST guidance.*

USCG response: Concur. The Coast Guard will evaluate security risks and establish a centralized configuration and patch management process according to applicable DHS and NIST guidance.

Recommendation #5: *Develop and implement documented procedures to ensure data is erased and rendered unrecoverable from laptops before the equipment is disposed of or Transferred, including the maintenance of records.*

USCG response: Concur. The Coast Guard will develop and implement procedures to ensure data is erased and rendered unrecoverable from laptops before the equipment is disposed of or Transferred, including the maintenance of records.

Recommendation #6: *Establish procedures to ensure that all occurrences of lost or stolen laptops are reported to DHS SOC as security incidents and reflected in the USCG inventory database as exceptions.*

USCG response: Concur. The Coast Guard will require that missing laptops be reported to the DHS SOC.

ENCLOSURE (1)



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendation #7: *Enforce the requirement to have units submit the results of annual laptop inventories to Headquarters and work with units to correct any identified laptop inventory management deficiencies.*

USCG response: Concur. The Coast Guard has a property management system in place. The Service will place emphasis on laptops and other similar items to ensure they are identified as property and subject to policy and processes.



Appendix C

Major Contributors to This Report

Chiu-Tong Tsang, Director
Mike Horton, IT Officer
Amanda Strickler, Lead IT Specialist
Thomas Rohrback, IT Specialist
Bridget Glazier, IT Auditor
David Bunning, IT Specialist
Gregory Wilson, Management/Program Assistant
Daniel McGrath, Referencer



Appendix D

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commandant, USCG
Chief Information Officer, DHS
Chief Information Security Officer, DHS
Chief Information Officer, USCG
Chief Administrative Officer, USCG
Chief Information Security Officer, USCG
Director, Compliance and Oversight, DHS OCISO
Director, GAO/OIG Liaison Office
Acting Chief Privacy Officer, DHS
Audit Liaison, CIO, DHS
Audit Liaison, CISO, DHS
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 document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

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