

# **United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain**





# HIGHLIGHTS

## *United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain*

**March 27, 2015**

### **Why We Did This**

To protect the Nation's maritime interests and environment, United States Coast Guard (USCG) employees, contractors, and partners have access to its operations, systems, and data. Based on job function or role, trusted insiders could be given elevated access to mission-critical assets. Trusted insiders could use their access or insider knowledge to exploit USCG's physical and technical vulnerabilities with the intent to cause harm.

### **What We Recommend**

Our report had three recommendations that, if implemented, should strengthen USCG's management of the threat posed by trusted insiders.

#### **For Further Information:**

Contact our Office of Public Affairs at (202) 254-4100, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)

### **What We Found**

USCG has taken some steps to address the risk of insider threats to its information systems and data. For example, USCG established an Insider Threat Working Group designed to implement a holistic program focused on the insider risk. In addition, USCG implemented a process to verify that system administrators have the appropriate level of access to information technology systems and networks to perform their assigned duties. Further, USCG established the Cyber Security Operations Center to monitor and respond to potential insider threat risks or incidents against USCG information systems and networks.

However, additional steps are needed to further address the risk posed by trusted insiders at USCG by:

- implementing software to protect against the unauthorized removal of sensitive information through the use of removable media devices and email accounts;
- implementing stronger physical security controls to protect USCG's information technology assets from possible loss, theft, destruction, or malicious actions; and
- providing insider threat security awareness training for all USCG employees.

### **USCG Response**

USCG concurred with all of our recommendations.



OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

**Table of Contents**

[Results of Audit](#) ..... 2

[Background](#) ..... 3

[Steps Taken To Mitigate the Insider Risk](#) ..... 5

[USCG Insider Threat Working Group](#) ..... 5

[USCG Insider Threat Program](#) ..... 6

[Privileged User Management Program](#) ..... 7

[Cyber Security Operations Center](#) ..... 8

[Challenges Remain in Addressing the Insider Risk](#) ..... 8

[Unauthorized Data Removal](#) ..... 8

[Physical Security Controls](#) ..... 10

[Insider Threat Security Awareness Training](#) ..... 17

[Recommendations](#) ..... 18

**Appendixes**

[Appendix A:](#) Transmittal to Action Official ..... 20

[Appendix B:](#) Scope and Methodology ..... 21

[Appendix C:](#) USCG Comments to the Draft Report ..... 23

[Appendix D:](#) Major Contributors to This Report ..... 25

[Appendix E:](#) Report Distribution ..... 26

**Abbreviations**

CERT	Computer Emergency Response Team
CGITWG	Coast Guard Insider Threat Working Group
CSOC	Cyber Security Operations Center
DHS	Department of Homeland Security
IT	information technology
NIST	National Institute of Standards and Technology
NITTF	National Insider Threat Task Force
OIG	Office of Inspector General
TISCOM	Telecommunication and Information Systems Command
USB	universal serial bus
USCG	United States Coast Guard



## Results of Audit

We reviewed the efforts of the United States Coast Guard (USCG) to address the risk posed by trusted insiders. Our objective was to assess USCG's progress toward protecting its information technology assets from threats posed by its employees, especially those with trusted or elevated access to sensitive but unclassified information systems or data.

USCG has taken some steps to address the risk of insider threats to its information systems and data. Specifically, USCG:

- established an Insider Threat Working Group designed to implement a program focused on identifying and remediating insider risk;
- implemented a process to verify that system administrators have the appropriate level of access to information technology systems and networks to perform their assigned duties; and
- established the Cyber Security Operations Center to monitor and respond to potential insider threat risks or incidents against USCG information systems and networks.

Additional steps are needed to further reduce the risk of insider threats to information technology assets. We performed testing that revealed potential vulnerabilities in technical and physical security controls that could allow for:

- unauthorized data removal from USCG information systems; and
- loss, theft, or destruction of information technology assets.

In addition, insider threat security awareness training is needed for USCG employees.

We are making three recommendations that, if implemented, should strengthen USCG's management of the threat posed by trusted insiders.



## Background

The USCG is one of the five armed forces of the United States and the only military organization within the Department of Homeland Security (DHS). The USCG is responsible for protecting the public, the environment, and the U.S. economic interests in the Nation's ports and waterways, international waters, and in maritime regions required to support national security. As of May 2014, the USCG consisted of 39,657 active duty personnel, 7,835 reserve personnel, 8,505 civilian personnel, and 4,240 contractor personnel. USCG personnel serve nationwide and internationally.

Trusted insiders could be given elevated access to mission-critical assets, including personnel, facilities, information, equipment, networks, or systems. Potential threats can include damage to the United States through espionage, terrorism, and unauthorized disclosure of national security information. Trusted insiders may also be aware of weaknesses in organizational policies and procedures, as well as physical and technical vulnerabilities in computer networks and information systems. This institutional knowledge poses a continual risk to the organization. In the wrong hands, insiders use this knowledge to facilitate malicious attacks on their own or collude with external attackers to carry out such attacks.

According to USCG officials, a malicious insider could do the most harm to the USCG mission by:

- compromising sensitive and classified information;
- damaging operational infrastructure and resources; and
- causing loss of life through workplace violence.

The unauthorized disclosure of sensitive information could adversely affect the security of USCG's information systems, assets, resources, employees, and the general public. In the case of USCG, an internal breach by a trusted employee could impact its ability to protect the Nation's maritime interests and environment. As a result, the USCG must be constantly aware of adversaries, especially those with the expertise and means to create opportunities for insider attacks.

## Requirements and Best Practices for Addressing Insider Risks

Issued in October 2011, *Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* requires agencies to implement a threat detection program consistent with guidance and standards developed by a government-wide insider threat task force. DHS will be responsible for implementing this program consistent with the task force's guidance. The





OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

---

November 2012 *Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* promotes the development of effective insider threat programs within the U.S. Government.

National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, issued in April 2013, includes new requirements for agencies to address the risk posed by the insider threat. Federal agencies had up to 1 year from April 2013 to comply with these requirements. According to NIST, the standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of controlled unclassified information in non-national security systems.

Since 2001, the Computer Emergency Response Team (CERT) Insider Threat Center of the Software Engineering Institute at Carnegie Mellon University has researched and gathered data about malicious insider acts, including information technology (IT) sabotage, fraud, and theft of confidential or proprietary information, espionage, and potential threats to our Nation's critical infrastructures. CERT has researched approximately 400 insider threat cases, including fraud, sabotage, and theft of intellectual property. These cases were all prosecuted within the United States.

CERT's research resulted in developing best practices that provide a framework for establishing an insider threat program within an organization, including Federal agencies. In addition, CERT devised a list of defensive measures that could help detect or prevent insider attacks. CERT recommends that organizations:

- include insider threat as part of an enterprise-wide risk assessment;
- conduct a security awareness campaign to ensure that the insider threat is understood across the organization;
- develop and clearly define organizational policies relevant to the insider threat, enforcing those policies consistently and fairly; and
- secure both the physical and electronic environment, including account and password management, separation of duties, controls for the software development process, change controls, remote access, and privileged user accounts, especially those used by system administrators.



## **Steps Taken to Mitigate the Insider Risk**

USCG has taken some steps to address the risk of insider threats to its information systems and data. Specifically, USCG established an Insider Threat Working Group designed to implement a holistic program focused on identifying and remediating insider risk. USCG has implemented a process to verify that system administrators have the appropriate level of access to IT systems and networks to perform their assigned duties. Further, USCG established the Cyber Security Operations Center to monitor and respond to potential insider threat risks or incidents against USCG information systems and networks.

### **USCG Insider Threat Working Group**

In December 2009, the USCG formed a working group to begin the process of implementing a component-wide insider threat program. A formal charter was signed in February 2012 for the Coast Guard Insider Threat Working Group (CGITWG) to serve as a focal point for addressing insider threat issues. Part of that charter includes collaborating across the USCG, the Intelligence Community, and the U.S. Government to identify insider threat best practices and promote awareness of insider threat issues throughout the USCG.

The working group meets on a quarterly basis. The group's primary objectives are to:

- represent the interests and actions of the USCG for insider threat programming and related issues;
- align CGITWG with mandated Intelligence Community directives and requirements;
- identify, recommend, and implement necessary insider threat related resourcing and resource prioritization;
- capture, evaluate, and document all insider threat program capability requirements for necessity, impact, and urgency;
- review, recommend, and maintain a model of functional elements of an effective insider threat program;
- draft and execute insider threat program support documentation and updates; and
- document and implement program requirements with full explanation, justification, prioritization, and proposed resource allocation.

The CGITWG garners consensus on insider threat issues across the USCG to provide a collaborative environment to integrate and



OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

---

synchronize insider threat efforts. The CGITWG consists of member offices and organizations that include, but are not limited to:

- Coast Guard Counterintelligence Service;
- Office of Security Policy and Management;
- Office of Intelligence Security Management;
- Office of Intelligence Surveillance and Reconnaissance Systems and Technology;
- Coast Guard Investigative Service;
- Information Assurance Policy Division;
- Office of Work-Life;
- Office of Counterterrorism and Defense Ops; and
- Office of Intelligence and Criminal Investigations Legal.

## **USCG Insider Threat Program**

The CGITWG is developing the Coast Guard Insider Threat Program to address the insider threat for unclassified and classified domains. They created a draft policy document entitled, *Commandant Instruction 5500.20, Coast Guard Insider Threat Program*.

Once approved by USCG senior officials and implemented, it would:

- establish the program;
- promulgate policy;
- assign responsibilities;
- provide guidance for stakeholders and members of the program;
- designate a senior official in charge of the program; and
- institute insider threat working groups.

According to the draft policy document, the insider threat program will take measures to prevent, detect, respond to, and mitigate insider threats to USCG personnel, facilities, information, equipment, networks, and systems. Once implemented, this program will be responsible for:

- incorporating insider threats into existing security awareness training requirements;
- establishing procedures for reporting indicators of potential insider threat activity to the appropriate office;
- establishing and promoting an internal website accessible to all USCG employees that provides insider threat information, reference materials, and a means to report insider threat issues electronically;





## OFFICE OF INSPECTOR GENERAL Department of Homeland Security

---

- establishing an insider threat audit program for unclassified and classified domains that uses technical capabilities to monitor certain user activity on USCG information systems;
- developing information-sharing policies and procedures to gather, integrate, review, assess, and respond to information derived from counterintelligence, security, IT, human resources, legal, and other sources as necessary;
- establishing procedures for documenting and retaining reported insider threat issues and incidents and response actions taken;
- developing policy and procedures to address workplace violence and active shooter concerns; and
- establishing a means for employees to report potential insider threat concerns electronically.

Further, the *Commandant Instruction 5500.20, Coast Guard Insider Threat Program* includes a list of insider threat indicators. The instruction requires USCG personnel to be trained to identify indicators of questionable and suspicious activity concerning behaviors and potential insider threat activity.

The USCG created a website that provides employees insider threat reference materials, training aids, and links to report insider threat incidents.

### **Privileged User Management Program**

In order to minimize the risk of potential insider threats to IT assets, USCG has implemented a Privileged User Management Program. It is designed to verify that system administrators (Privileged Users) have the appropriate level of access to information technology systems and networks to perform their assigned duties. USCG military, civilians, and contractors with privileged access to information systems pose a greater risk to perform insider attacks, as their elevated access may give them the opportunity to bypass system controls intended to help mitigate unauthorized access or malicious activities.

The Privileged User Management Program requires system administrators to follow specific requirements. The program outlines roles and responsibilities for each privileged user that mandates accountability, separation of duty, least privilege, and adherence to the highest standards for protection of information systems, networks, and data. USCG officials responsible for approving privileged user requests are required to review each request to verify that it meets the justification for the access level requested.



## **Cyber Security Operations Center**

USCG established the Cyber Security Operations Center (CSOC) to monitor and respond to potential insider threat risks or incidents against USCG information systems and networks. According to CERT research, monitoring employees' behavior while they are using computers or network resources may help to identify insider threat activity before a serious breach of security occurs.

The CSOC serves as a command center that:

- performs 24/7 network monitoring, analysis, and incident response;
- consists of a 24/7 operational floor that oversees the protection of USCG information systems and networks; and
- acts on all reported computer-related disclosures including sensitive but unclassified, classified, and personally identifiable information.

Further, center representatives are members of the CGITWG and coordinate the implementation of IT areas within the insider threat program.

## **Challenges Remain in Addressing the Insider Risk**

Additional steps are needed to further reduce the risk of insider threats to IT assets. We performed testing that revealed potential vulnerabilities in technical and physical security controls of USCG information systems that could allow for:

- unauthorized data removal from USCG information systems; and
- loss, theft, or destruction of IT assets.

In addition, insider threat security awareness training is needed for USCG employees.

### **Unauthorized Data Removal**

Using unauthorized removable media devices, employees can remove controlled (i.e., sensitive or personally identifiable) information from unclassified USCG systems. Using government issued email accounts, employees can send controlled information to external personal email accounts.



OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

---

## **Removable Media Devices**

Our technical testing demonstrated that unauthorized removable media devices can be connected to USCG IT assets and used to remove simulated sensitive information.<sup>1</sup> Using login accounts supplied by USCG, we were able to transfer simulated sensitive information to and from USCG IT assets using unauthorized removable media devices at multiple USCG locations.

The *DHS 4300A Sensitive Systems Policy* requires the USCG to ensure that information systems and its data are sufficiently protected. Further, the policy prohibits DHS personnel and contractors from using non-government issued removable media devices and connecting them to DHS IT assets. According to CERT, organizations must implement safeguards to prevent unauthorized data removal or transfers.

The USCG has not fully implemented software to protect against the unauthorized removal of sensitive information through removable media devices. Currently, the USCG is using the McAfee Device Control Module to monitor, log, and block removable media devices from being connected to the USCG network. Technical testing demonstrated, however, that the software has not been fully implemented across USCG sites to protect against unauthorized data removal.

By not fully implementing the software, insiders could transfer controlled information via unauthorized removable media devices. This unauthorized transfer of sensitive information is a constant threat to any organization. Malicious insiders can carry out attacks on an organization's information systems and networks through unauthorized leakage and transfer of information through removable media devices.

## **Email Accounts**

Our technical testing demonstrated that simulated sensitive information could be sent from a USCG issued email account to an external personal email account.<sup>2</sup> A subsequent Office of Inspector General (OIG) request for USCG to provide evidence that this activity was detected by the USCG CSOC was not received.

---

<sup>1</sup> The testing used a variety of manufactured universal serial bus (USB) devices. A USB device, also known as a USB drive or thumb drive, is popular for storing and transporting data. These devices are small, readily available, and portable. These characteristics make them appealing to insider attackers.

<sup>2</sup> Simulated sensitive information – During testing, we created documents that appeared to contain controlled information, not actual USCG sensitive documents.



## OFFICE OF INSPECTOR GENERAL Department of Homeland Security

---

In addition, testing revealed that employees located at the USCG Headquarters could connect a USCG issued laptop to the USCG's wireless network. This network uses a commercial Internet Service Provider to access internet sites, including personal email websites.

A USCG official said that the wireless network is used primarily by contractors hired by the USCG to access their corporate email accounts. It is also used by the USCG Office of Public Affairs to access social media websites.

Although USCG's primary enterprise network (Coast Guard One Network) blocks access to external personal email websites, there currently is no monitoring for unauthorized data transfer or email content on the wireless network.

The *DHS 4300A Sensitive Systems Policy* requires USCG to ensure that information systems and its data are sufficiently protected. Further, the policy requires USCG to secure and filter all email content.

This vulnerability allows for the opportunity to transfer sensitive information from a USCG issued laptop to a non-USCG personal email account. According to CERT, malicious insiders could use email to covertly disseminate sensitive information to competitors or conspirators. Sensitive or mission-critical information in the wrong hands could have adverse effects on USCG employees, resources, business partners, or the general public. The failure to prevent the unauthorized removal or transfer of sensitive information through email provides a malicious insider the opportunity to carry out such an attack, making it difficult for an organization to protect itself.

### **Physical Security Controls**

Steps to protect USCG IT assets from unauthorized access, misuse, or destruction from malicious insiders were not always in place.<sup>3</sup> We identified multiple sites where adequate physical controls were not implemented to protect USCG IT resources from unauthorized access, theft, or destruction. Examples of situations that needed attention included inadequate physical safeguards, exposed and unsecure network equipment, and unsecure backup media.

---

<sup>3</sup> Insiders are legitimate users of a system. When they use that access to circumvent security, that act is known as an insider attack.



---

**USCG Telecommunication and Information Systems Command  
(TISCOM)**

TISCOM is responsible for maintaining the USCG-wide unclassified network, local area networks, USCG Cutter IT connectivity, and enterprise servers and services.<sup>4</sup> We inspected selected TISCOM buildings that did not have adequate physical safeguards such as access card readers to control or restrict unauthorized personnel from accessing those buildings. In addition, we identified doors to areas that housed IT resources left unlocked, increasing the risk of unauthorized access to sensitive information and IT resources.

- As shown in figure 1, we found a USCG IT network equipment room door closed, but unlocked and unattended, increasing the risk for unauthorized access. As shown in figure 2, there was no access card reader, so USCG relied instead on employees to apply due diligence by using a key to lock the room when unattended.



**Figure 1: Unlocked USCG Network Equipment Room**

---

<sup>4</sup> A "Cutter" is any Coast Guard vessel at least 65 feet in length.

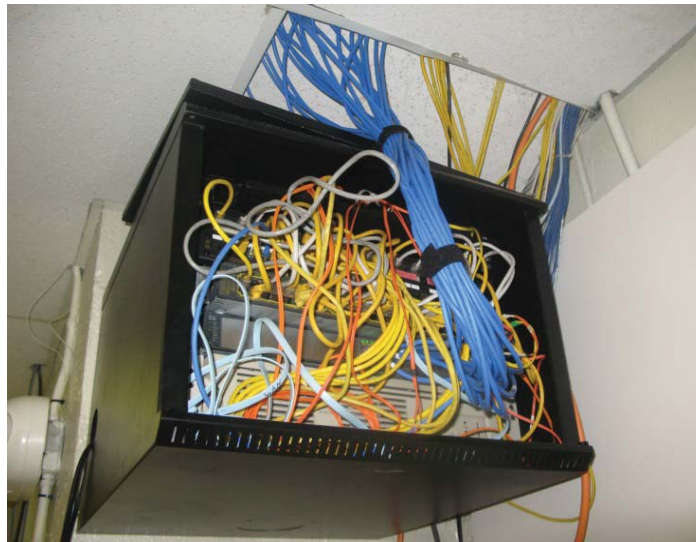




**Figure 2: Network Equipment Room Door with No Access Card Reader**

#### **USCG Air Station Washington**

- We inspected USCG network equipment at the USCG Air Station Washington. As shown in figures 3 and 4, we found USCG network equipment and cables exposed and physically unsecured against potential unauthorized access and use.



**Figure 3: Exposed and Unsecured Network Equipment**



**Figure 4: Exposed and Unsecured Network Equipment**

- We inspected USCG network equipment at the USCG Air Station Washington. As shown in figures 5 and 6, we found multiple routers used for wireless network connectivity that were not physically secured and were exposed to potential unauthorized access and use. According to USCG policy, each wireless access point device needs to be secured in a locked enclosure or space that is resistant to tampering, theft, and unauthorized access to console ports, power supplies, and reset buttons.



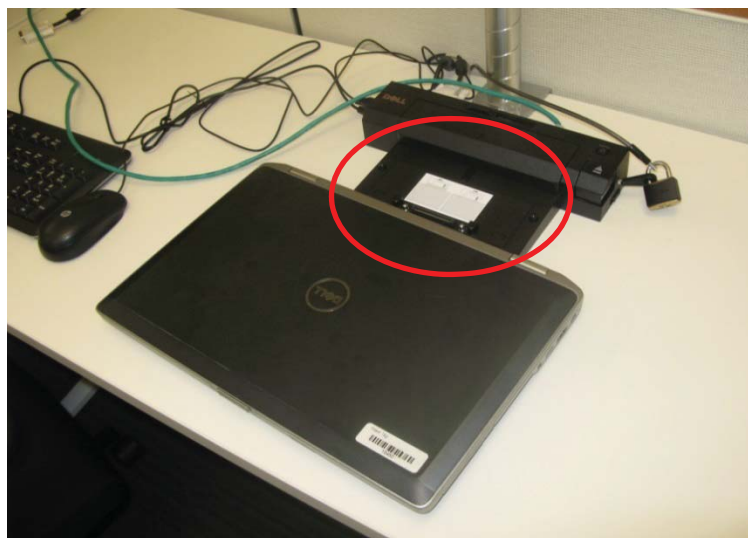
**Figure 5: Exposed and Unsecured USCG Wireless Router**



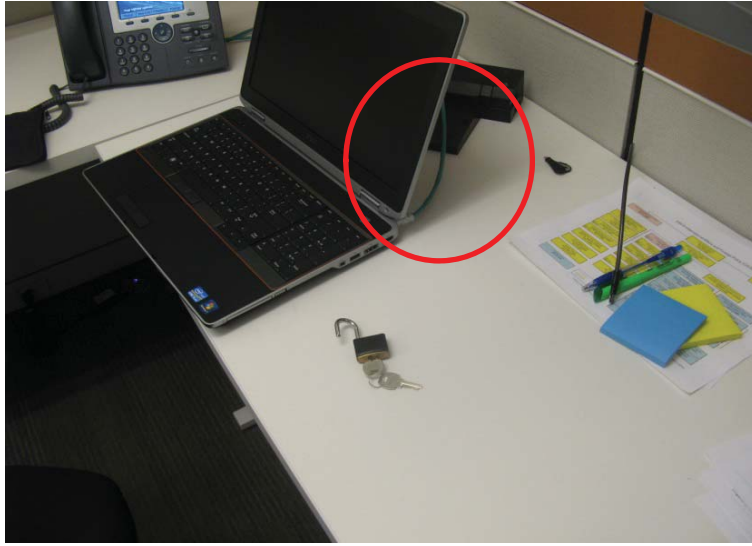
**Figure 6: Exposed and Unsecured USCG Wireless Router**

**USCG Headquarters (St. Elizabeths Campus)**

- We inspected USCG network equipment at the USCG Headquarters (St. Elizabeths Campus). As shown in figures 7 and 8, we found multiple unattended USCG workstation laptops that were not properly secured and locked. According to *DHS 4300A Sensitive Systems Handbook*, unattended laptop computers and other mobile computing devices shall be secured in locked offices, secured with locking cables, or in locked cabinets or desks. When laptop computers are not properly secured, the risk of unauthorized access or theft from insiders increases.



**Figure 7: Unsecured Laptop Computer**



**Figure 8: Unsecured Laptop Computer**

- We inspected USCG network equipment at the USCG Headquarters (St. Elizabeths Campus). As shown in figure 9, we found external hard drives that were unattended and not properly locked and secured. According to USCG policy, when not in use, external hard drives shall be removed from workstations, and stored in locked offices, secured with locking cables, or in locked cabinets or desks. When external hard drives are not properly secured, the risk of unauthorized access or theft from insiders increases.



**Figure 9: Unsecured Backup Media**





OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

- We inspected USCG network equipment at the USCG Headquarters (St. Elizabeths Campus). As shown in figure 10, we found backup media that were not properly stored in a protected and secure location. According to *DHS 4300A Sensitive Systems Handbook*, components shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as USB drives, are stored when not in use in a secure location. A secured location includes a locked office, room, desk, bookcase, file cabinet, locked tape device, or in other storage that prohibits access by unauthorized persons. When backup media are not properly secured, the risk of unauthorized access or theft of sensitive information by insiders increases.



**Figure 10: Unsecured Backup Media**

According to *DHS Sensitive Systems Policy Directive 4300A*, controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and shall be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.

On September 2, and again on September 16, 2014, OIG sent email requests to USCG asking for an explanation as to why adequate physical controls were not implemented to protect its IT equipment at the sites selected for review. USCG did not provide an official response within the timeframe required to be included in this report.

Without strong physical safeguards implemented at locations that contain IT equipment, malicious insiders could intentionally exploit those





OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

---

deficiencies resulting in the loss, theft, or destruction of IT systems or information. A security incident could result in the compromise of the confidentiality, integrity, and availability of controlled information.

### **Insider Threat Security Awareness Training**

The USCG has not fully implemented insider threat based security awareness training for all employees. This would provide USCG personnel with knowledge necessary to better recognize and respond or report potential indicators of insider threat activity. Organizations should include security awareness training on recognizing and reporting potential indicators of insider threat. In addition, CERT recommends that insider threat awareness training is incorporated into periodic security awareness training for all employees.

USCG is progressing towards implementing the insider threat awareness training requirements outlined by the National Insider Threat Task Force (NITTF). This task force is responsible for assisting agencies in developing and implementing their insider threat program.

The NITTF, in coordination with the Department of Defense's Defense Security Service and the Office of the National Counterintelligence Executive's Training and Assistance Group, has provided agencies with an insider threat awareness training course that meets the November 2012 *Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*. The training course includes areas, such as indicators of insider threat actions and behavior, and the appropriate process to report suspicious insider threat activities.

According to the Coast Guard Counterintelligence Service responsible for the USCG Insider Threat Program, the USCG has until September 30, 2015, to implement insider threat awareness training for USCG employees.

Until such training is fully implemented, USCG employees may not be aware of or have the knowledge to recognize insider threat behavior, or the appropriate process to report potential insider threats or actual attacks.



## Recommendations

**Recommendation 1.** We recommend that the USCG CIO: Implement software to protect against the unauthorized removal of sensitive information through removable media devices and email accounts.

**Recommendation 2.** We recommend that the USCG CIO: Implement stronger physical security controls to protect USCG's IT assets from possible loss, theft, destruction, and malicious actions.

**Recommendation 3.** We recommend that the USCG CIO: Provide documentation that all USCG employees received insider threat security awareness training.

## USCG Comments

We obtained written comments on a draft report from the Acting Assistant Commandant for Resources (CG-8) for USCG. We have included a copy of the comments, in their entirety, in appendix C. USCG concurred with all of the recommendations.

## OIG Analysis of USCG Comments

### Management Comments to Recommendation 1

USCG concurs with recommendation 1. USCG officials said that they have implemented the Department of Defense mandated Host Based Security System that monitors every USCG system and alerts the USCG Cyber Command Security Operations Center of unauthorized or illegal USB connections to USCG systems. This software based system provides the USCG protection against unauthorized connection of removal media devices, and blocks the communication between device and system to prevent unauthorized removal of sensitive or non-sensitive information. Additionally, USCG has implemented cybersecurity policy that directs the audit of CD/DVD drive activity by network users and monitors copying actions by CD/DVD drives on USCG information systems. Furthermore USCG has implemented Department of Defense mandated Data Loss Prevention, which features the ability to monitor emails and identify any potential release of sensitive information. If the Data Loss Prevention system is triggered, email is delayed, reviewed, and sanitized as necessary. USCG requested that the OIG close the recommendation.



OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

---

**OIG Analysis**

We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USCG provides support that the Department of Defense mandated Host Based Security System and the Data Loss Prevention have been fully implemented to identify unauthorized USB connections to USCG systems and potential unauthorized transfer of sensitive information at USCG Headquarters, USCG Air Station Washington, and USCG TISCOM.

**Management Comments to Recommendation 2**

USCG concurs with recommendation 2. USCG officials said they are developing a Course of Action that coincides with this recommendation and aligns with the recently revised *Physical Security Manual*. USCG anticipates publishing interim guidance to improve physical security controls by June 30, 2015. USCG intends to issue final policy and guidance in February 2016.

**OIG Analysis**

We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USCG provides specific actions that the USCG has taken or plans to take to address the physical security issues identified in this report at USCG Headquarters, USCG Air Station Washington, and USCG TISCOM. Additionally, USCG should provide the OIG a copy of the final policy and guidance to improve physical security controls.

**Management Comments to Recommendation 3**

USCG concurs with recommendation 3. USCG officials said that all USCG personnel are mandated to complete the Department of Defense Federal Cyber Awareness Challenge training annually. The training specifically contains a module that addresses insider threat awareness. This training is highly interactive and requires users to pass the Federal Cyber Awareness Challenge certification test prior to receiving credit for course completion. Reports are documented in the USCG Learning Management System, which enables the USCG to track annual compliance. Documentation will be provided separately. USCG requested that the OIG close the recommendation.

**OIG Analysis**

We agree that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until USCG provides the OIG with a copy of the insider threat awareness module included in the Federal Cyber Awareness Challenge training. Additionally, the USCG should provide support that all USCG personnel have completed this mandatory training.



OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

## Appendix A

### Transmittal to Action Official

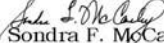


OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

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

March 27, 2015

TO: Rear Admiral Marshall B. Lytle III  
Chief Information Officer  
U.S. Coast Guard

FROM:   
Sondra F. McCauley  
Assistant Inspector General  
Office of Information Technology Audits

SUBJECT: *United States Coast Guard Has Taken Steps to Address  
Insider Threats, but Challenges Remain*

Attached for your action is our final report, *United States Coast Guard Has Taken Steps to Address Insider Threats, but Challenges Remain*. We incorporated the formal comments from the United States Coast Guard (USCG) in the final report.

The report contains three recommendations aimed at improving USCG's insider threat posture. The USCG concurred with all of the recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 3 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please email a signed PDF copy of all responses and closeout requests to [OIGITAuditsFollowup@oig.dhs.gov](mailto:OIGITAuditsFollowup@oig.dhs.gov). Consistent with our responsibility under the *Inspector General Act*, we will provide 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 Richard Saunders, Director, Advanced Technology Division, at (202) 254-5440.



## Appendix B

### 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.

Our objective was to assess the progress made towards protecting the Department's IT assets from the threat posed by its employees, especially those with trusted or elevated access to these assets. During the audit, we assessed USCG's:

- insider threat management process;
- selected employees' ability to monitor and report suspicious employee behavior;
- insider threat security policies;
- insider threat security training and awareness; and
- unclassified network critical to the mission of USCG.

We reviewed USCG and DHS policies, procedures, management plans, and wireless network security policies and documents. In addition, the assessment team reviewed system and security logs for unauthorized devices and wireless activities. We interviewed selected USCG personnel and management officials stationed at the following fieldwork locations:

- USCG Headquarters (St. Elizabeths Campus), Washington, DC;
- USCG Air Station Washington (Ronald Reagan Washington National Airport), Arlington, Virginia; and
- USCG TISCOM, Alexandria, Virginia.

Technical fieldwork performed at selected locations included the following activities:

- Physical and Visual Inspection Check: We inspected offices and designated IT areas to determine how effectively information systems and workstations were logically and physically protected from the threat of exposed sensitive information being accessed or obtained by a malicious insider. Our inspection included checking for exposed or unattended user accounts (e.g., user names and password information), unprotected personally identifiable information, sensitive or classified USCG





OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

---

information, and the presence of locking mechanisms for IT assets in accordance with Department policy.

- Unauthorized Removable Media Device Testing: We selected and tested a sample of information systems and workstations to determine whether sensitive information could be removed from the USCG network infrastructure using unauthorized removable media devices and without detection. Without controls in place to detect, deter, or prevent this type of activity, malicious insiders could remove sensitive information with the intent to compromise the security and mission of USCG.
- Sensitive Email Content Testing: We conducted testing to determine whether emails with sensitive and personally identifiable information markings and caveats, as defined in DHS Management Directive 11042.1 and *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, could be sent outside of USCG without being detected. Without controls in place to deter or prevent this type of activity, malicious insiders could remove sensitive unclassified information through USCG's electronic mail service with the intent to compromise the security and mission of USCG.
- Wireless Security Checks for Unauthorized Devices: We performed visual inspections and conducted security testing using tools that run wireless scans. The testing assessed whether wireless security is controlled and monitored to prevent unauthorized systems and devices from connecting to USCG networks. Without controls in place to deter or prevent this type of activity, a malicious insider could use unauthorized wireless activities to compromise the security and mission of USCG.

We conducted this performance audit between March 2014 and September 2014 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. We appreciate USCG's efforts to provide the necessary information and access to accomplish this audit. Appendix D contains major OIG contributors to this report.



OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

## Appendix C

### USCG Comments to the Draft Report




Commandant  
United States Coast Guard

2703 Martin Luther King, Jr. Ave SE  
Washington, DC 20593-7000  
Staff Symbol: CG-8  
Phone: (202) 372-3533  
Fax: (202) 372-4960

5730  
MAR - 6 2015

#### MEMORANDUM

From:   
C. A. Bennett  
Acting COMDT (CG-8)

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

To: Sondra F. McCauley  
Assistant Inspector General  
Office of Information Technology Audits

Subj: DHS OIG DRAFT REPORT: UNITED STATES COAST GUARD HAS TAKEN  
STEPS TO ADDRESS INSIDER THREATS BUT CHALLENGES REMAIN

Ref: (a) *OIG Project No. 13-078-ITA-USCG of January 2015*

1. This memorandum transmits the Coast Guard's response to the draft report identified in reference (a).
2. The Coast Guard concurs with all the recommendations listed in the draft report. Our response in enclosure (1) demonstrates that the Coast Guard has measures in place or underway to ensure that Insider Threats are managed properly and eliminated. Request you close Recommendations one and three as implemented.
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 to OIG Draft Report on Insider Threats



OFFICE OF INSPECTOR GENERAL  
Department of Homeland Security

---

**UNITED STATES COAST GUARD STATEMENT ON DHS OIG DRAFT REPORT:  
*United States Coast Guard Has Taken Steps to Address Insider Threats but Challenges  
Remain***

**OIG Project *OIG Project No. 13-078-ITA-USCG***

**OIG Recommendation #1:** Implement software to protect against the unauthorized removal of sensitive information through removable media devices and email accounts apportionment of cost.

**Response: Concur.** USCG has implemented the Department of Defense (DoD) mandated Host Based Security System (HBSS) that monitors every USCG system and alerts the USCG Cyber Command Security Operations Center (SOC) of unauthorized or illegal USB connections to USCG systems. This software based system provides the USCG protection against unauthorized connection of removal media devices, and blocks the communication between device and system to prevent unauthorized removal of sensitive or non-sensitive information. Additionally, USCG has implemented cybersecurity policy that directs the audit of CD/DVD drive activity by network users and monitors copying actions by CD/DVD drives on USCG information systems. Furthermore USCG has implemented DoD-mandated Data Loss Prevention (DLP), which features the ability to monitor emails and identify any potential release of sensitive information. If the DLP system is triggered, email is delayed, reviewed and sanitized as necessary. Recommend closure.

**OIG Recommendation #2:** Implement stronger physical security controls to protect USCG's IT assets from possible loss, theft, destruction, and malicious actions.

**Response: Concur.** USCG is developing a Course of Action (COA) that coincides with this recommendation and aligns with the recently revised Physical Security Manual. USCG anticipates publishing interim guidance to improve physical security controls by June 30, 2015. USCG intends to issue final policy and guidance in February 2016.

**OIG Recommendation #3:** Provide documentation that all USCG employees received insider threat security awareness training.

**Response: Concur.** All USCG personnel are mandated to complete the DoD Federal Cyber Awareness Challenge (FCAC) training annually. The FCAC specifically contains a module that addresses insider threat awareness. This training is highly interactive, and requires users to pass the FCAC certification test prior to receiving credit for course completion. Reports are documented in the USCG Learning Management System, which enables the USCG to track annual compliance. Documentation will be provided separately. Recommend closure.

Enclosure (1)



## **Appendix D**

### **Major Contributors to This Report**

Richard Saunders, Director  
Philip Greene, Auditor-In-Charge  
Jason Dominguez, IT Specialist  
Bridget Glazier, Referencer



## **Appendix E**

### **Report Distribution**

#### **Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
DHS Component Liaison

#### **United States Coast Guard**

Commandant  
Audit Liaison

#### **Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

#### **Congress**

Congressional Oversight and Appropriations Committees



## ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: [www.oig.dhs.gov](http://www.oig.dhs.gov).

For further information or questions, please contact Office of Inspector General Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov). Follow us on Twitter at: @dhsoig.



### OIG HOTLINE

To report fraud, waste, or abuse, visit our website at [www.oig.dhs.gov](http://www.oig.dhs.gov) and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security  
Office of Inspector General, Mail Stop 0305  
Attention: Hotline  
245 Murray Drive, SW  
Washington, DC 20528-0305