Operations Systems Center Computer Security and Controls

U.S. Coast Guard

Report Number: FI-2001-089
Date Issued: September 7, 2001

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: **ACTION**: Report on Operations Systems Center Computer Security and Controls, U.S. Coast Guard
FI-2001-089

Date: September 7, 2001

From: Alexis M. Stefani
Assistant Inspector General for Auditing

Reply To Attn Of: Meche:x61496

To: Chief of Staff
U.S. Coast Guard

This report presents the results of our audit of computer security and controls at the U.S. Coast Guard (Coast Guard) Operations Systems Center (OSC) at Martinsburg, West Virginia. OSC has been Coast Guard's principal computer center since 1991. Twenty-three computer systems operate at OSC, which provide information essential to Coast Guard's critical missions including search and rescue, marine safety, law enforcement, logistics support, and personnel management functions. None of the 23 systems contain classified information.

This report is one in a series of computer security audits conducted to meet the statutory requirements of the Government Information Security Reform Act (Act). The Act assigns responsibility of evaluating Department of Transportation (DOT) information security to the Office of Inspector General. Our objectives for this audit were to determine whether OSC operations are adequately secured to ensure integrity, confidentiality, and availability of mission-critical systems.

OSC is a Government-owned and contractor-operated facility and accomplishes its mission with a combination of Government and contractor personnel. The OSC facility and three OSC systems have been designated to be critical to the Nation's infrastructure, in accordance with Presidential Decision Directive (PDD) 63. This PDD-63 facility and the three systems are used to support Coast Guard search and rescue missions, and marine safety inspections.

Coast Guard relies on secured operations at OSC to ensure integrity, confidentiality, and availability of computer systems and system-dependent operations. For example, without reliable operations of the search and rescue system at OSC, rescue authorities would not have timely and accurate information on the positions and characteristics of vessels near a reported distress. As a result, Coast Guard's ability to perform rescue missions could be impaired, resulting in loss of life.

RESULTS

We found computer security weaknesses[1] at OSC and Coast Guard-wide. Coast Guard has not enforced its own policy for periodically reviewing computer systems for security certification. Only one of the 23 systems operating at OSC was certified. The OSC facility itself was not certified as adequately secured to support mission-critical system operations. We also identified concerns with Coast Guard's capability to meet requirements for having the Nation's critical infrastructure protected by May 2003, as required by PDD-63.

We found adequate network firewall security at OSC to prevent unauthorized Internet users from entering Coast Guard's private networks. However, insiders, including Coast Guard employees, contractors, industry associations, and other Government employees could gain access to OSC systems that they are not authorized to use. A survey performed by the Federal Bureau of Investigation in 1998 reported that insiders constitute the greatest intruder threat. Our prior reviews also identified vulnerabilities to attack and abuse by DOT insiders.[2]

Specifically, we found weak personnel security, physical security, and technical security at OSC. We also identified vulnerabilities in OSC computers and the lack of disaster recovery capability, which could affect continuity of Coast Guard's critical missions. These weaknesses indicate that Coast Guard needs to assign a higher priority to computer security. The following summarizes our findings:

- ➢ **Increased commitment to the system certification process could enhance computer security**. The Office of Management and Budget (OMB), DOT, and Coast Guard all issued requirements that major systems should be periodically reviewed for security certification. We found that 22 of the 23 OSC systems did not have the security review and were not certified as adequately secured for operations. The OSC facility itself was not certified for supporting critical system operations. Coast Guard does not have a plan or schedule to have these systems certified, including the PDD-63 critical systems.

[1] For security reasons, specifics concerning the weaknesses and our audit procedures are not discussed in this report, but were provided to Coast Guard managers during the audit.

[2] Statement of Inspector General Kenneth M. Mead before the Committee on Science, U.S. House of Representatives, Computer Security within DOT, September 27, 2000.

Coast Guard also needs to enhance employee training on system certification, which requires a structured review to determine whether systems are secured commensurate with risk resulting from the loss, misuse, unauthorized access to, or modification of, the system. This security review is intended to help management decide what corrective actions, if any, are needed to adequately secure the system. However, Coast Guard employees expressed concerns about doing certification reviews because their systems may not "pass" security tests, which could result in decommissions. Another concern was that these systems might not be able to handle the workload caused by the certification process.

- **Using a structured methodology to identify infrastructure-critical assets is vital to meet PDD-63 requirements**. In 1998, Coast Guard, in conjunction with the Department's Chief Information Officer (CIO), identified the OSC facility and five systems as critical to the Nation's infrastructure. However, Coast Guard did not use a structured methodology to identify critical assets, and did not identify all of its critical assets. For example, we found that Coast Guard's primary computer network, on which other PDD-63 systems depend, was excluded from the list.

  Protecting this primary network is vital to Coast Guard for meeting PDD-63 requirements. If this primary network goes out of service due to an intentional act or a natural disaster, Coast Guard would not be able to access information in critical systems. For example, without access to the information in a search and rescue system, the Coast Guard Rescue Coordination Center could not accurately and timely identify the positions and characteristics of vessels near a reported distress. As a result, Coast Guard's search and rescue mission could be impaired. Having a structured methodology also would help ensure newly developed systems are being considered for PDD-63 protection.

- **Personnel, physical, and system access security needs to be enhanced to protect critical systems from unauthorized access**. OSC has about 200 contractor employees performing day-to-day computer operations, including critical functions like system security administration. We found contractor employees lacked background checks and key contractor employees did not have the proper level of background checks. As a result, Coast Guard could be missing valuable information that might keep some personnel who are at risk from working on certain computer systems. Our previous reviews found that the Federal Aviation Administration (FAA) and other parts of DOT also need to enhance background checks on contractor employees.[3] DOT officials

[3] Interim Report on Computer Security, DOT, Report Number FI-2000-108, July 13, 2000.

agreed to complete background checks on contractor employees by September 2001. During this audit, OSC took corrective actions by ordering more background checks; however, they have not yet been completed.

For physical security, we found that access to the OSC facility is adequately controlled; however, access to the computer room needs to be reviewed. Only personnel responsible for performing technical work, such as monitoring computer operations or maintaining hardware, should be given unsupervised access to the computer room. Once inside the computer room, personnel could easily cause disruptions by issuing special commands on operator consoles or by simply sabotaging computer equipment.

Currently, OSC allows more than 100 personnel unsupervised access to the computer room, including human resource personnel who conduct facility tours for new employees. We also noticed that OSC used the computer room to store furniture. During the audit, OSC took corrective actions by reducing the number of people allowed to access the computer room.

Our review of six OSC systems identified deficiencies in password controls, password files were not protected, and all people with access to the Coast Guard network could gain unauthorized remote access to two systems, including a payment system. These weaknesses make Coast Guard systems vulnerable to unauthorized access. For example, during the audit, we were able to obtain the database system administrator's password on a development machine because its password file was not protected. With stolen passwords, intruders could masquerade as privileged users, such as system or database administrators, to change or delete information. During the audit, OSC initiated actions to improve password and remote access controls.

- **Network security and intrusion detection capabilities need to be enhanced to reduce computer vulnerabilities.** While OSC has adequate firewall security to protect its private networks, we found that OSC computers were vulnerable to attack by insiders. Using commercial scanning software, we scanned about 700 devices on the network, including computers, printers, switches, and routers; and found 150 confirmed vulnerabilities, 59 of which were among the top 10 security threats identified by Government experts. These high-risk vulnerabilities allow attackers to execute a computer program remotely or gain root-level access privileges. As a result, unauthorized users could easily access, modify, or delete critical system information causing disruptions to Coast Guard operations.

Coast Guard also has installed intrusion detection systems to monitor network traffic from the Internet, but needs to develop procedures for better review coverage. Our review of the access log for Coast Guard's key web site disclosed intensive hacking attempts from a foreign source. While the hacker was not able to break in, the intrusion detection personnel were not aware of the attempts.

- **Enhancing systems disaster recovery capability needs immediate attention to ensure continuity of critical missions**. In response to PDD-63, Coast Guard designated the OSC facility and five systems as critical to the Nation's critical infrastructure. Three of these systems operate at OSC--a search and rescue system and two marine safety systems. If OSC experiences service disruptions due to a catastrophe or disaster, Coast Guard would need to quickly recover these systems at an alternative processing site to avoid mission disruptions. OSC currently does not have an adequate disaster recovery plan, an alternative processing site, or contingency plans for its PDD-63 systems.

  Coast Guard agreed that an alternative processing site is needed and has included a feasibility study in the Fiscal Year 2003 budget submission. However, this may not meet the time frame for protecting PDD-63 systems by May 2003. During the audit, we learned that Coast Guard has a smaller data center at Chesapeake, Virginia—the Finance Center (FINCEN), which has similar technical setup and network connections as OSC. While FINCEN may not have the capacity to be the recovery site for all OSC systems, its readiness could enable Coast Guard to quickly establish disaster recovery capabilities for PDD-63 systems.

In view of the deficiencies identified, we recommend that the Coast Guard CIO assign a priority for having all critical systems certified for adequate security; enhancing employees' understanding of the purpose for security certification; and using a structured methodology to re-evaluate identification of critical infrastructure assets, including new systems. OSC also should evaluate the feasibility of using FINCEN as an interim alternative processing site for PDD-63 systems while developing a full recovery plan; and establish target dates to correct personnel, physical, password, and network security deficiencies we identified.

The Coast Guard agreed with the findings and has taken, or is taking, reasonable corrective actions on all of our recommendations.

BACKGROUND

OSC has been Coast Guard's principal computer center since 1991. OSC is a Government-owned and contractor-operated facility and accomplishes its mission with a combination of Government and contractor personnel. Coast Guard personnel monitor contractor personnel who perform day-to-day computer operations including hardware maintenance and software development.

Twenty-three major Coast Guard computer systems operate at OSC, which support search and rescue, marine safety, law enforcement, logistics support, and personnel management functions. OSC had hosted a classified system for the U.S. Navy, but that system was decommissioned in July 1999. None of the OSC systems contain classified information; however, the OSC facility and three OSC systems have been designated as critical to the Nation's infrastructure, in accordance with PDD-63. These systems are used to support Coast Guard search and rescue missions, and marine safety inspections. Any degradation of OSC's capabilities could significantly impact Coast Guard's ability to perform its missions, and could result in loss of life.

OSC also plays an important role in overall management of Coast Guard computer networks. Coast Guard relies on a primary network, with multiple Internet connection points, to transmit data among Coast Guard Headquarters and field offices. In addition to managing one of the Internet connections, OSC serves as the network central point for transmitting data and is responsible for the Coast Guard's key web site.

SCOPE AND METHODOLOGY

We used the General Accounting Office's Federal Information Systems Controls Audit Manual as a guide for this audit. We identified and reviewed OSC's information system policies and procedures, observed controls in operation, and verified about 200 personnel security background checks performed on Coast Guard and contractor employees. We physically inspected environmental control systems such as fire extinguishing; physical access control; backup power systems; and the backup file storage site.

We selected six major OSC systems for detailed testing of system-level access controls. We interviewed system users at Coast Guard Headquarters and field offices. We inspected these systems' security through hands-on testing and review of system design documentation at OSC. We also interviewed both DOT and Coast Guard CIO officials for identification of infrastructure-critical assets, as required by PDD-63.

We reviewed OSC network infrastructure, firewall security rules, and intrusion detection operations. We interviewed key network personnel at OSC, the Coast Guard Telecommunications and Information Systems Command, and other field locations. Using commercial scanning software, we scanned about 700 devices on the network, including computers, firewalls, web servers, printers, switches, and routers. We also used special software to perform detailed review of configuration (setup) of four major systems. To test the effectiveness of Coast Guard intrusion detection capabilities, we performed detailed analyses of all access activities recorded for Coast Guard's key web site between June 1 and June 6, 2001.

The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Audit work was performed between March and July 2001 at OSC; Coast Guard Telecommunications and Information Systems Command at Alexandria, Virginia; and Coast Guard Headquarters at Washington, DC.

FINDINGS AND RECOMMENDATIONS

A. Increased Commitment to the System Certification Process Could Enhance Computer Security.

OMB Circular A-130 requires that agencies use a systematic approach to evaluate the adequacy of computer system security. DOT Order H1350.253, "Departmental Guide to Certification/Accreditation of Information Systems," provides detailed guidance on assessing whether controls and security in a computer system are commensurate with the risk resulting from the loss, misuse, unauthorized access to, or modification of, the system. The Coast Guard Entity-wide Security Plan also requires computer systems to be certified before installation and periodically thereafter.

- **Lack of certification for system security**

  For the 23 OSC systems, only one went through a systematic review of its security and was certified for operations in 1996. Although both OMB and Coast Guard require that systems be periodically re-certified, this system has not yet been re-certified.

  System certification is intended to help management decide what corrective actions, if any, are needed to adequately secure the system commensurate with risks. To reach such a decision, OMB Circular A-130 requires a 4-step process—assigning security responsibility, developing a security plan, testing the security, and authorizing the system for operations. Without going through this process, the Coast Guard has no assurance that OSC systems are adequately secured to ensure integrity, confidentiality, and availability of operations. Three of OSC systems are critical to Coast Guard key missions and the Nation's critical infrastructure protection.

  During the audit, we found that Coast Guard had no plan or schedule to have OSC systems, including PDD-63 critical systems, reviewed for security certification. We also found that Coast Guard needs to enhance employee training on system certification. Some employees expressed concern that their systems may not "pass" security tests, which could result in decommissions. Another concern was that these systems might not be able to handle the workload caused by the certification process.

- **Lack of plans to have OSC properly certified**

  OSC is designated as a PDD-63 critical facility because it is the processing center for multiple PDD-63 systems. In accordance with OMB Circular

A-130, OSC needs to be certified to operate as a "general support system." However, there is no plan to have OSC certified.

Coast Guard conducted a physical vulnerability assessment of the OSC facility in 1998, and network vulnerability assessments during 2001. However, these assessments did not address other requirements such as system security plans, personnel controls, technical controls, incident response capability, and continuity of support. We also found OSC's security plan was inadequate because it addressed only security issues concerning desktop personal computers at the facility, but not major computer systems for which OSC has the custodian responsibility.

- **Lack of schedule to secure PDD-63 critical assets**

  The OSC facility and three application systems are designated as critical to the Nation's infrastructure and need to be protected from intentional acts by May 2003, as required by PDD-63. In DOT's Fiscal Year 2002 Performance Plan, DOT committed to have an overall PDD-63 compliance schedule developed by June 30, 2001. However, we found the schedule had not been developed for Coast Guard infrastructure-critical systems as of July 31, 2001.

  During the audit, Coast Guard stated that a contractor would be selected to help assess system vulnerability. Until the assessment is completed, Coast Guard will not know what resources are needed for remediation and system testing. To meet the May 2003 deadline, Coast Guard needs to accelerate development of the PDD-63 compliance schedule.

Recommendations:

We recommend that the Coast Guard Chief Information Officer:

1. Enforce Coast Guard Entity-wide security plan requirements and enhance employee training for conducting OMB Circular A-130 system certification reviews.

2. Develop a schedule by September 30, 2001, for evaluating, testing, and certifying PDD-63 systems and the OSC facility for adequate security by May 2003.

3. Develop a schedule by December 31, 2001, to have other OSC computer systems certified for adequate security, in accordance with departmental guidance.

B. Using A Structured Methodology to Identify Infrastructure-critical Assets Is Vital to Meet PDD-63 Requirements.

On May 22, 1998, PDD-63 was issued calling for a national effort to protect our nation's critical infrastructures from intentional acts that could significantly diminish the abilities of the Federal Government to perform essential national security missions and ensure the general public health and safety.

In July 1998, the Department's CIO office issued guidance defining critical infrastructure as "those physical and cyber-based systems essential to the minimum operations of the economy and the government."[4] To assist DOT Operating Administrations in identifying critical infrastructure, the Department's CIO office provided listings of mission-critical systems identified for Year-2000 fixes, systems included in DOT's 5-year Information Resources Management Plan, and a list of DOT-owned data centers. Based on this information, Coast Guard and DOT jointly identified critical infrastructure systems and facilities under Coast Guard control.

However, neither DOT nor Coast Guard used a structured methodology when identifying infrastructure-critical assets. As a result, the Coast Guard did not adequately identify its PDD-63 critical systems, and their inter-dependent systems, for protection.

- **A key infrastructure system was excluded from the PDD-63 list**

  The Coast Guard CIO office initially identified 18 systems as critical to the Nation's infrastructure. After reviewing the Coast Guard submission, the Department's CIO office reduced the list to five systems. There was no documentation explaining the decision-making in either case. One of the systems deleted was the Coast Guard's primary network system (CGDN+). However, four of the five PDD-63 critical systems rely on CGDN+ to operate.

  Coast Guard's life saving mission has a clear dependency on CGDN+. If the CGDN+ network system goes out of service due to an intentional act or a natural disaster, Coast Guard would not be able to access information critical to its key missions. For example, without access to the information in a search and rescue system, the Coast Guard Rescue Coordination Center could not accurately and timely identify the positions and characteristics of vessels near a reported distress. As a result, the search and rescue efforts could be impaired.

[4] In 1999, the Department re-defined DOT critical infrastructures as ". . . those DOT-owned, controlled, or operated facilities and information-based systems that are essential to the nation's defense, economic security, or public confidence in such facilities or systems."

- **The PDD-63 list has not been updated since November 1998**

  Between 1998 and 1999, the Coast Guard identified additional mission-critical systems for Year-2000 fixes (increased from 45 to 74 systems). Also, new systems have been deployed. However, because of the lack of a structured methodology, the Coast Guard has not evaluated these additional systems for PDD-63 consideration.

  A March 2001 report issued by the President's Council on Integrity and Efficiency identified a similar problem in other Federal agencies for not adequately identifying their critical assets. A recommendation was made to OMB that agencies should consider using a structured methodology[5] to ensure complete identification of PDD-63 systems.

Recommendations:

We recommend that the Coast Guard Chief Information Officer:

4. Designate the CGDN+ network as infrastructure-critical and develop a plan to protect it by May 2003.

5. Develop a more structured methodology, with a focus on system dependencies, for identifying potential PDD-63 systems. Re-evaluate Coast Guard systems, including newly deployed systems, and facilities for PDD-63 consideration based on this methodology.

[5] A methodology recommended by the Critical Infrastructure Assurance Office is the Project Matrix, which would identify all assets, nodes and networks, and associated infrastructure dependencies and interdependencies required for the Federal Government to fulfill its national security, economic stability, and critical public health and safety responsibilities to the American people.

C. Personnel, Physical, and System Access Security Needs to Be Enhanced to Protect Critical Systems from Unauthorized Access.

OMB requires agencies to adequately secure Government computer systems to ensure confidentiality, integrity, and availability of operations. To achieve this goal, agencies need to implement a combination of management, personnel, operational, and technical controls. The National Institute of Standards and Technology and DOT have issued guidance for implementing specific controls. Our review of system operations at OSC identified weaknesses in personnel, operational, and technical security areas.

- **Weak personnel security in background checks**

  DOT Order 1630.2B, "Department of Transportation Personnel Security Manual," May 30, 2001, requires that key computer positions, especially with significant involvement in life-critical or mission-critical systems, be designated as high risk and receive a higher-level background check (Background Investigation). For lower-level computer positions, when the work is technically reviewed by a higher authority at the high-risk level, they should be designated as moderate risk and receive a lower-level background check (National Agency Check and Inquiry). DOT policy also requires the same type of background checks on contractor employees that perform comparable duties to DOT employees.

  There are about 200 contractor employees and 60 Coast Guard employees working at OSC. Contractor employees perform most of the day-to-day operations of computer systems. During our review, we found:

  - Lack of Background Checks. We found 87 contractor employees did not have any background checks. They were associated with both primary contractors and subcontractors.

  - Inadequate Background Checks. Fifteen contractor employees in high-risk positions, such as functional area managers and system administrators, had received only low-level background checks. These individuals should have received higher-level background checks because their jobs allow them to bypass regular system controls or their technical work is not reviewed by others.

  Without proper level of background checks, OSC could be missing valuable information about people placed in key positions to ensure the integrity and security of computer operations. Our previous reviews found that FAA and other parts of DOT also need to enhance background checks on contractor employees. DOT officials agreed to complete background checks on contractor employees by September 2001. During this audit, OSC took corrective actions by ordering more background checks; however, they have not yet been completed.

- **Weak operational security in computer room access controls**

  Controlling physical access is a critical part of operational security. It applies to both exterior entrances into the facility and access to interior parts of the facility. OMB Circular A-130, "Security of Federal Automated Information Resources," recognizes that the greatest harm to computer systems is from authorized individuals engaged in improper activities, whether intentional or accidental. Thus, OMB promotes the concept that restricts a user's access to processing functions to the minimum for job performance.

  OSC uses a magnetic card system to control and monitor physical access to the facility and selected areas within the facility. The most vital area in the facility is the computer room because it houses the computer hardware that runs the systems. While access to the OSC facility is adequately controlled, we found weaknesses in controlling access to the computer room. Currently, OSC allows more than 100 personnel to access the computer room. Not all of these authorized personnel have technical reasons to enter the computer room. For example, human resource personnel are granted unlimited access because they conduct facility tours for new employees.

  Access to the computer room should be closely supervised and only computer technicians, operators, or their supervisors should be granted unsupervised access. Once inside the computer room, employees could circumvent security controls by issuing commands on operator consoles or by simply sabotaging computer equipment to disrupt operations. We also noticed that OSC used the computer room to store furniture. During the audit, OSC took corrective actions by reducing the number of people allowed to access the computer room.

- **Weak technical security in system access controls**

  System access controls are critical in today's interconnected environment. The commonly used system control techniques are password security and remote network access security. Passwords are used to authenticate users attempting to access computer systems. Federal Information Processing Standards Publications 112, "Password Usage," recognizes weaknesses associated with passwords and sets a standard for password use. DOT Order H1350.2

"Information System Security Program" (Internet policy) requires that network computers be accessible only to authorized users.

Among all OSC systems, we selected the following six systems to review the adequacy of technical security—a search and rescue system, a marine safety system, two personnel systems, and two financial systems. Table 1 shows we identified security deficiencies in all but one system.

Table 1
OSC System Weaknesses

Security Deficiencies	Search and Rescue	Marine Safety System	Personnel System	Personnel System	Financial System	Financial System
Unlimited password attempts allowed	X	X		X		X
No automatic password expiration	X			X	X	
Password file not protected	X	N/A		N/A		X
Unauthorized system changes allowed		N/A		N/A	X	X
Inactive sessions not terminated	X			X	X	X

N/A: not reviewed because of technical incompatibility with the audit software

- Unlimited password attempts allowed: To prevent unauthorized users from guessing at passwords, computer systems should be programmed to automatically suspend access after three unsuccessful password attempts. Four systems allowed unlimited password attempts. As a result, an individual could continue guessing until access is gained. Coast Guard has initiated corrective actions, including system upgrades.

- No automatic password expiration: Because password security can be easily compromised (stolen or guessed), the same password should be used for only a short time, usually 90 days. Three systems did not have automatic password expiration control. This automated control feature was available on one system but was not being used. Security on the other two systems could be enhanced with software upgrades. Coast Guard has initiated corrective actions, including system upgrades.

- Password file not protected: Two systems did not protect password files. Without such protection, passwords contained in these files could be easily "cracked" with free software available on the Internet. By using stolen passwords, intruders could masquerade as privileged users, such as system or database administrators, to change or delete information. For example, during the audit, we were able to obtain the database system administrator's password on a development machine because its password file was not protected.

- Unauthorized system changes allowed: Two systems did not properly control the use of a commonly available remote network service on their computers. As a result, all people having access to the Coast Guard network, estimated to be about 40,000, could access, modify, or delete information stored in these systems from remote locations. This is a critical concern because one system is used to process payments.

- Inactive sessions not terminated: Once an individual logs on a system with proper user account and password, the system stays connected until the session is terminated. In this duration, if the individual leaves the computer unattended, other people could use the machine to gain unauthorized access to the system, as evidenced in a recent embezzlement case in DOT. A commonly used control technique is to automatically terminate the session after a specified period of inactivity. Four systems did not have this control. This is a critical concern because one system contains sensitive human resources information and another is used to process payments.

As a result of combined personnel, operational, and system access security weaknesses, critical OSC systems are exposed to unauthorized access and changes. Coast Guard core missions depending on these systems could be disrupted or compromised. During the audit, OSC initiated actions to improve password and remote access controls.

Recommendations:

We recommend that the Coast Guard Chief Information Officer:

6. Direct OSC to (a) identify and complete higher-level Background Investigations on key staff responsible for maintaining, modifying and securing computer systems, and (b) complete lower-level National Agency Check and Inquiry on all other Coast Guard and contractor employees.

7. Require OSC to review the authorized access list and limit unsupervised access to the computer room only to personnel who need to perform on-going technical work.

8. Direct OSC to improve password security by allowing limited password attempts, enforcing automatic password expirations, and protecting password files for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether same corrective actions are needed.

9. Direct OSC to improve remote network access security by eliminating uncontrolled use of remote network services for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether same corrective actions are needed.

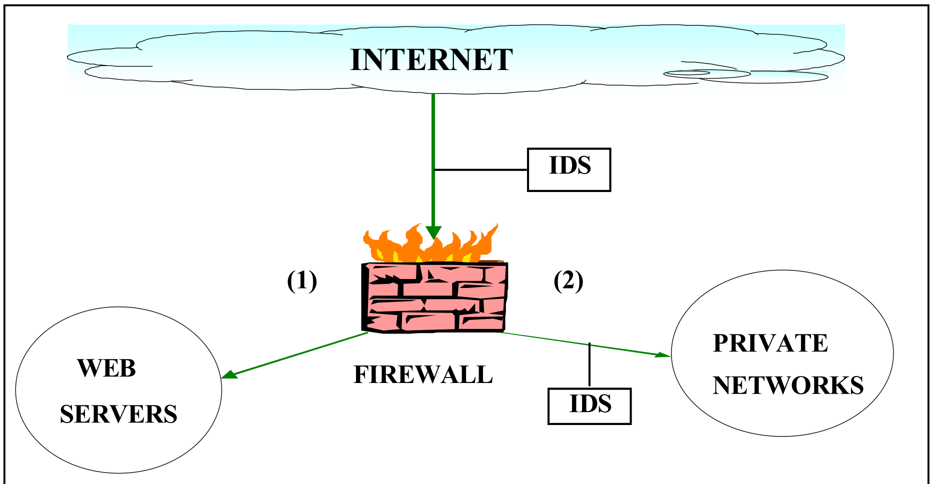
10. Direct OSC to improve access controls by automatically terminating inactive sessions for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether same corrective actions are needed.

D. Network Security and Intrusion Detection Capabilities Need to Be Enhanced to Reduce Computer Vulnerabilities.

Coast Guard relies on a primary network (CGDN+) to transmit data to support its missions including search and rescue, marine safety, human resources, and other administrative functions. There are multiple Internet connection points on this Coast Guard network. OSC plays an important role in the overall management of Coast Guard's networks. In addition to managing one of the Internet connections, OSC serves as the network central point for transmitting data over CGDN+ and is responsible for the Coast Guard's key web site.

As shown in Figure 1, OSC has implemented firewall security and Intrusion Detection Systems (IDS) to help control network access activities. The firewall, acting as a "security guard," directs network traffic into either Coast Guard private networks or public web servers. The Coast Guard internal network should be accessed only by authorized users. However, the public is encouraged to access the public web sites without restrictions. The IDS, acting as a "surveillance camera," monitors network traffic and reports abnormal activities for management follow-up.

Figure 1
OSC Network Overview



(1) Access by the public is encouraged without restrictions.
(2) Only authorized Coast Guard users should be allowed access.

- **OSC computers vulnerable to attack by insiders**

  Using commercial scanning software, we scanned about 700 OSC devices on the network, including computers, firewalls, web servers, printers, switches, and routers. These devices are used to support critical systems such as Coast

Guard search and rescue or financial systems as well as Coast Guard web servers. While OSC has adequate firewall security to prevent unauthorized access to its private networks, our test found that computers are vulnerable to attack by insiders[6] and Coast Guard intrusion detection capabilities need to be enhanced.

Our scanning results identified 89 high, 38 medium and 23 low confirmed vulnerabilities[7] on OSC computers. Fifty-nine of the high vulnerabilities were among the "Top Ten Most Critical Internet Security Threats" identified by the Federal CIO Council. Eleven of the 59 high vulnerabilities are in OSC production systems. These high vulnerabilities could allow attackers to execute a computer program remotely or gain root-level access privileges. As a result, unauthorized users could easily access, modify, or delete critical system information on Coast Guard production systems and cause disruptions to Coast Guard operations. Coast Guard should give priority to fix these high vulnerabilities.

During the audit, we also brought it to Coast Guard's attention that the medium and low confirmed vulnerabilities need to be corrected. These vulnerabilities do not appear to be major threats to Coast Guard network security. However, when they co-exist with high vulnerabilities, the security exposure can be significantly increased.

For example, we were able to obtain the database system administrator's password on a development machine due to the combination of high, medium, and low vulnerabilities on that machine. These combined vulnerabilities allowed us to copy the system password file from a remote location by using a default setup on that computer. Since the passwords in the file were not protected, we obtained the database system administrator's password by using a free tool on the Internet. With the password, we could access, modify, or even delete the entire development database system.

These confirmed vulnerabilities occurred because of weak configuration management controls[8] over OSC computers. For example, the high confirmed

[6] Attacks by people with either direct access to OSC computers or remote access through the Coast Guard's primary network.

[7] A high vulnerability may provide an attacker with immediate access into a computer system, such as allowing execution of remote commands. Medium and low vulnerability may provide an attacker with useful information, such as password files, to compromise DOT computers.

[8] Configuration management is a process of adding, deleting, modifying and documenting changes to connections, addresses and commands based on changing business needs and manufacturers' advice such as release of software upgrades/fixes.

vulnerabilities we identified could be eliminated by either applying manufacturers' software patches or reconfiguring system software. In view of the importance of configuration management controls, the Department's CIO office issued a "Server Security Checklist" on June 6, 2001, to assist Operating Administration's configuration management controls. While this checklist was intended for developing new systems, it also could be used to examine existing computers.

- **Outsider attack not detected**

  Since 1999, Coast Guard has been using commercial IDS software to monitor network traffic from the Internet. A team composed of Coast Guard and contractor employees is responsible for monitoring, reporting, and taking necessary actions against intrusion activities.

  We reviewed the log recording access activities against the Coast Guard's key web site between June 1 and June 6, 2001, and found intensive hacking attempts from a foreign source. While the hacker was not able to break into the Coast Guard web site, the intrusion detection team was not aware of these attempts. Therefore, no actions were taken to block access from that source, which could further exploit the Coast Guard web site.

Recommendations:

We recommend that the Coast Guard Chief Information Officer:

11. Direct OSC to correct all 150 confirmed vulnerabilities.

12. Direct OSC to use the Department's "Server Security Checklist" to enhance configuration management controls on existing computers, including timely installation of computer manufacturers' software fixes and upgrades.

13. Direct the Coast Guard network management team to develop and implement intrusion detection review procedures to ensure comprehensive review coverage.

E. Enhancing Systems Disaster Recovery Capability Needs Immediate Attention to Ensure Continuity of Critical Missions.

OMB Circular A-130 requires continuity of operations planning for every information system to rapidly and effectively deal with potential disruptions of mission-critical business functions. This planning effort is critical because OSC is part of the Nation's critical infrastructure.

The OSC facility and three OSC systems are designated as PDD-63 critical. Coast Guard relies on these PDD-63 systems to perform its critical missions. For example, Coast Guard uses a search and rescue system to quickly provide authorities with accurate information on the positions and characteristics of vessels near a reported distress. If OSC experiences prolonged service disruptions, Coast Guard's search and rescue mission would be significantly impaired because of poor disaster recovery planning at OSC and a lack of contingency planning for individual systems.

- **OSC disaster recovery plan unreliable and not tested**

  OSC developed a disaster recovery plan in December 1994. The plan contains inaccurate and unreliable information regarding recovery procedures. For example, the plan referenced use of a contractor-supplied "hotsite" as an alternative processing site for recovery during emergency situations. However, a contract had never been signed for such an arrangement. Currently, OSC does not have any alternative processing facilities for use during emergency situations. If a catastrophic event occurred at the data center or surrounding region, OSC would have difficulty in initiating an effective response.

  Coast Guard agreed that an alternative processing site is needed and has included a feasibility study in its Fiscal Year 2003 budget submission. However, this action may not meet the timeframe for protecting PDD-63 systems, which are required to be secured by May 2003. During the audit, we learned that Coast Guard has a smaller data center at Chesapeake, Virginia. This data center, FINCEN, has similar technical setup and network connections as OSC. While FINCEN may not have the capacity to be the recovery site for all OSC systems, its readiness could enable Coast Guard to quickly establish disaster recovery capabilities for PDD-63 systems.

- **System level contingency plans not available**

  Coast Guard key missions are critically dependent on computer systems. In case of system disruptions, manual processing generally is not a viable backup option. System owners should develop detailed contingency plans specifying how they will perform their mission if they lose existing application support. We found such plans are not available for any of the PDD-63 critical systems at OSC. As a result, in case of system disruptions, Coast Guard's capability to deliver its key missions could be significantly impaired.

- **Backup files stored too close to OSC**

  Backup files are used to recover system operations in case of disasters or operational problems. OSC stores backup files at an off-site facility 5 miles away. Since the off-site facility is not geographically distant from OSC, catastrophic events affecting the local area could make both OSC and the off-site facility unavailable to Coast Guard. For example, a natural, chemical, or biological disaster could require total evacuation of the area for an indefinite period. As a result, Coast Guard would not be able to recover its critical systems because both current and backup files would become unavailable.

Recommendations:

We recommend that Coast Guard Chief Information Officer:

14. For PDD-63 critical systems, direct OSC to (a) use a reciprocal agreement with FINCEN management to be each other's recovery processing site, and work with system owners to develop system-level contingency plans in 6 months, and (b) perform system recovery testing for PDD-63 systems in 12 months.

15. Direct OSC to develop and test a disaster recovery plan, including selection of a recovery site, for all of its operations.

16. Direct OSC to finalize the selection of a more geographically distant location to store backup files.

MANAGEMENT RESPONSE

A draft of this report was provided to the Coast Guard Chief of Staff on August 10, 2001. Coast Guard concurred with 11 of our 16 recommendations and concurred-in-part with the remaining 5. Coast Guard provided these comments.

Recommendations 1, 2, 3, and 4. Concur. The Coast Guard is building an enterprise-wide security plan that will include rigorous identification of PDD-63 mission critical systems, and provide for their certification and accreditation. This plan will also prescribe employee training and security protections for non-PDD-63 systems. The Coast Guard considers the OSC and the CGDN+

network as PDD-63 facilities, and will officially designate them as such in the enterprise security plan, which is scheduled to be in place by December 31, 2001.

Recommendation 5. Concur. The Coast Guard is incorporating the Critical Infrastructure Assurance Office's methodology as described in *Practices for Securing Critical Information Assets.*

Recommendation 6. Concur. The majority of personnel working at OSC have had background checks completed. The remaining personnel have initiated the paperwork necessary to complete the process. Each government and contractor employee will have a background check commensurate with the level of system/data floor access.

Recommendation 7. Concur. OSC has reviewed the access list and reduced the number of employees that have uncontrolled data floor access to those with a need to operate or service equipment in the computer room or their supervisors.

Recommendation 8. Concur-in-part. OSC initiated actions to improve password security, and rectified password vulnerabilities on all systems for which remedies are available. Coast Guard does not intend to correct the deficiency in two of the systems since they are scheduled for decommissioning in early FY 2002. The replacement systems will have functionality to provide password aging, password retry limits, and other password policy enforcement such as blocks on passwords not conforming to length/character specifications.

Recommendation 9. Concur. OSC initiated actions to improve remote access controls. OSC will remove FTP (file transfer protocol) access controls from users that do not require them for computer operations.

Recommendation 10. Concur-in-part. Coast Guard understands the need for terminating inactive sessions. The Coast Guard's standard desktop (SWIII) operating system automatically disables the user session after a pre-determined period of time. OSC users access production systems via SWIII workstations. Since the relative risk on developmental systems is low, termination of inactive sessions on developmental systems is a managed risk.

Recommendation 11. Concur. OSC has already taken for action the elimination of these vulnerabilities on systems that carry production data. The Office of the Chief Information Officer will follow up to ensure that these key vulnerabilities have been eliminated.

Recommendation 12. Concur. The DOT Server Security Checklist will be implemented as a matter of standard security procedure for production systems.

Recommendation 13. Concur-in-part. This is part of the process of developing a Coast Guard enterprise-wide security plan. However, Coast Guard takes issue with the inference that the intrusion detection team was unaware of hacking attempts during the period reviewed by the audit team. As part of our risk management posture, intrusion attempt thresholds are set, above which our teams are notified. The attempts recorded during the review period simply did not reach the pre-set threshold.

Recommendations 14 and 15. Concur-in-part. The Coast Guard, as part of its enterprise-wide security plan, will include a full risk assessment of the systems designated as PDD-63, including the need for high-availability alternative processing at a remote site. If determined necessary, OSC and FINCEN will most likely be specified as mutual disaster-recovery sites for designated PDD-63 systems. These plans will be in at least draft form by April 2002. It is not possible yet to determine if adequate funding is available -- or necessary -- to support full alternative-processing disaster-recovery capabilities. That necessity will be determined by the security analysis in the enterprise-wide security plan.

Recommendation 16. Concur. In the interim, critical OSC data files will be shuttled to a site in the Washington DC area. In the long term, backups may occur through a high-speed dedicated line serving FINCEN and OSC as mutual backup sites.

The complete text of Coast Guard comments is in the Appendix to this report.

OFFICE OF INSPECTOR GENERAL COMMENTS

Although Coast Guard concurred-in-part with 5 recommendations, actions taken and planned on all 16 recommendations are reasonable and satisfy the intent of our recommendations. Please provide, within 30 days, estimated completion dates for planned actions on Recommendations 5, 6, 9, 11, 12, and 16.

Concerning comments to Recommendation 13, we asked for the pre-set thresholds on the hacking attempts we identified, but Coast Guard was unable to tell us what the thresholds were and why more than 200 attacks in 1 day did not alert the intrusion detection team. Coast Guard needs to determine whether thresholds were actually set, and consider a lower limit for detecting hacking especially from foreign sources.

We appreciate the courtesies and cooperation of Coast Guard representatives. If you have questions concerning this report, please call me at (202) 366-1964 or John Meche at (202) 366-1496.

-#-

U.S. Department
of Transportation

**United States
Coast Guard**

Memorandum

Subject: Draft Report On Computer Security And Controls At The Operations Systems Center

Date: 4 SEP 2001
7500

From: Commandant, U.S. Coast Guard

Reply to Attn. of: G-CCS
VADM Josiah
267-1642

To: Deputy Assistant Inspector General for Financial, Information Technology, and Departmentwide Programs

Ref: (a) DOT OIG Memorandum, Draft Report Project No. 01F3005F000 of Aug 10, 01

1. Enclosed you will find the U.S. Coast Guard response to the findings and recommendations presented in the Department of Transportation Inspector General (DOTIG) draft report on computer security and controls at the Coast Guard's operations systems center.

2. For additional information concerning this response, please contact the office of RADM Vivien Crea, G-CIT, 202-267-2767.

T. W. JOSIAH
Vice Admiral, U. S. Coast Guard
Chief of Staff

Encl: (1) U.S. Coast Guard Response to DOTIG Recommendations

Statement on Department of Transportation

Inspector General Report

I. TITLE: *Draft Report On Computer Security And Controls At The Operations Systems Center, Report No. 01F3005F000, August 10, 2001*

II. U.S. COAST GUARD POSITION

Information security is not a matter of eliminating risk, but managing it. Many of the deficiencies cited in the report are managed risks, and do not result in significant security vulnerabilities. The Coast Guard takes a careful approach to managing the risks inherent in its deployed information systems, by assessing the threats, balancing vulnerability against probability of occurrence, and determining options for management action to mitigate the risks, in order to manage security within the constraints of limited Coast Guard resources. In the case of disaster recovery, for example, the Coast Guard has thus far decided that the return on investment in fully redundant processing systems, when balanced against the remote possibility of complete incapacitation of the Operations Systems Command (OSC), is not the top priority use of scarce resources.

The audit report focuses on internal security at OSC. In light of recent studies showing that most enterprises experience 75% of their security attacks from the inside, it is understandable that the audit team would be focused on the Coast Guard's exposure to threats from the inside. In the past 24 months, however, the Coast Guard has not experienced a single insider attack. (Security incidents that appeared to be employee attacks were, upon investigation, reclassified as configuration problems, or application misbehavior.) At the same time, the Coast Guard's secure public perimeter has been under constant attack, like all military public presences. Despite this 7x24 assault, the Coast Guard's secure public perimeter has been highly successful in blocking Internet attacks that have brought other agencies to their knees. This is an important consideration as the Coast Guard weighs risks, threats, and appropriate security countermeasures.

On balance, the vulnerability of our internal information systems—especially developmental information systems that do not carry production applications or data—should be considered to be very low risk relative to our public systems directly exposed to the Internet. Even Coast Guard's production systems should be considered low risk relative to the threats posed to our public systems. For example, of the 11 high-risk vulnerabilities (now eliminated) found on production systems—described on page 18 of the audit report—all were on systems located behind Coast Guard's secure perimeter. These internal production systems are not easily identifiable, even by internal personnel. The IG audit staff located these system because they were told exactly where and how to find them among the thousands of devices on the Coast Guard Intranet. Only Coast Guard's technical personnel would be able to locate these production systems easily, and these staffers are already entrusted with "the keys to the castle." In this important sense, the Coast Guard's existing security posture is not significantly at risk when balanced against other threats posed by hostile hackers.

III. FINDINGS AND RECOMMENDATIONS

In this section, we respond to the recommendations made in the report.

Recommendation 1. "Enforce Coast Guard Entity-wide security plan requirements for, and enhance employee training on the purpose of, conducting OMB Circular A-130 system certification review." **Concur.** The Coast Guard is building an enterprise-wide security plan that will include rigorous identification of PDD-63 mission critical systems, and provide for their certification and accreditation. This plan will also prescribe employee training as appropriate.

Recommendation 2. "Develop a schedule, by September 30, 2001, for evaluating, testing, and certifying PDD-63 systems and the OSC facility for adequate security." **Concur.** The Coast Guard considers the OSC a PDD-63 facility, and will officially designate it as such in the enterprise security plan.

Recommendation 3. "Develop a schedule, by December 31, 2001, to have other OSC computer systems certified for adequate security." **Concur.** The Coast Guard is building an enterprise-wide security plan that will include rigorous identification of PDD-63 mission critical systems, and provide for their certification and accreditation. Security protections for non-PDD-63 systems will also be specified in the Plan. The schedule for the Plan will be in place by December 31, 2001.

Recommendation 4. "Designate the CGDN+ network as infrastructure-critical and develop a plan to protect it by May 2003." **Concur.** The Coast Guard considers the CGDN+ a PDD-63 facility, and will officially designate it as such in the enterprise security plan.

Recommendation 5. "Develop a more structured methodology, with a focus on system dependencies, for identifying potential PDD-63 systems and re-evaluate Coast Guard systems and facilities for PDD-63 consideration based on this methodology." **Concur.** The Coast Guard is incorporating the Critical Infrastructure Assurance Office's methodology as described in *Practices for Securing Critical Information Assets.*

Recommendation 6. "Direct OSC to (a) identify and complete higher-level Background Investigations on key staff responsible for maintaining, modifying and securing computer systems, and (b) complete lower-level National Agency Check and Inquiry on all other Coast Guard and contractor employees." **Concur.** The majority of personnel working at OSC have had background checks completed. The remaining personnel have initiated the paperwork necessary to complete the process. Each government and contractor employee will have a background check commensurate with the level of system/data floor access.

Recommendation 7. "Have OSC review the authorized access list and limit unsupervised access to the computer room to only personnel who need to perform on-going technical work." **Concur.** The OSC has reviewed the access list and reduced the number of employees that have uncontrolled data floor access to those with a need to operate equipment in the computer room, to those who service the equipment, or their supervisors.

Recommendation 8. "Direct OSC to improve password security by allowing limited password attempts, enforcing automatic password expirations, and protecting password files for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether same corrective actions are needed." **Concur-in-part.** OSC initiated actions to improve password security, and rectified password vulnerabilities on all systems for which remedies are available. The next upgrade to the operating system for two of the identified systems will correct the problems with unlimited password attempts as well as automatic password expirations. We do not intend to correct the deficiency in two of the systems since they are scheduled for decommissioning in early FY02. The replacement systems will have functionality to provide password aging, password retry limits, and other password policy enforcement such as blocks on passwords not conforming to length/character specifications.

Recommendation 9. "Direct OSC to improve remote network access security by eliminating uncontrolled use of remote network services for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether same corrective actions are needed." **Concur.** OSC initiated actions to improve remote access controls. OSC will remove FTP access controls from users that don't require them for computer operations.

Recommendation 10. "Direct OSC to improve access controls by automatically terminating inactive sessions for the systems we identified. OSC should also examine other systems, which we did not select for detailed review, to determine whether same corrective actions are needed." **Concur-in-part.** We understand the need for terminating inactive sessions. The Coast Guard's standard desktop (SWIII) operating system's standard image automatically disables the user session after a pre-determined period of time. OSC users access production systems via SWIII workstations with this feature. This recommendation's remedy, however, adversely affects development efforts on our systems used for this purpose. Since the relative risk on developmental systems is low, termination of inactive sessions on developmental systems is a managed risk.

Recommendation 11. "Direct OSC to examine potential vulnerabilities identified and correct all confirmed vulnerabilities." **Concur.** OSC has already taken for action the elimination of these vulnerabilities on systems that carry production data. The office of the Chief Information Officer will follow up to ensure that these key vulnerabilities have been eliminated.

Recommendation 12. "Direct OSC to use the Department's "Server Security Checklist" to enhance configuration management controls on existing computers, including timely installation of computer manufacturers' software fixes and upgrades." **Concur.** This is in the planning phases already, and the DOT Server Security Checklist will be implemented as a matter of standard security procedure for production systems.

Recommendation 13. "Direct the Coast Guard network management team to develop and implement intrusion detection review procedures to ensure comprehensive review coverage." **Concur-in-part.** This is part of the process of developing a Coast Guard enterprise-wide security plan. However, we take issue with the inference that the intrusion detection team was unaware of hacking attempts during the period reviewed by the audit team. As part of our risk management posture, intrusion attempt thresholds are set, above which our teams are notified. The attempts recorded during the reviewed period simply did not reach the pre-set threshold.

Recommendation 14. "For PDD-63 critical systems, direct OSC to (a) use a reciprocal agreement with FINCEN management to be each other's recovery processing site, and work with system owners to develop system-level contingency plans in 6 months, and (b) perform system recovery testing for PDD-63 systems in 12 months." **Concur-in-part.** The Coast Guard, as part of its enterprise-wide security plan, will include a full risk assessment of the systems designated as PDD-63. That assessment will determine the need for high-availability alternative processing at a remote site. If such extreme high-availability is determined to be necessary, OSC and FINCEN will most likely be specified as mutual disaster-recovery sites for designated PDD-63 high-availability systems. These plans will be in at least draft form by April 2002. It is not possible yet to determine if adequate funding is available – or necessary -- to support full alternative-processing disaster-recovery capabilities. That necessity will be determined by the security analysis capture in the enterprise-wide security plan.

Recommendation 15. "Direct OSC to develop and test a disaster recovery plan, including selection of a recovery site, for all of its operations." **Concur-in-part.** Please see the response immediately above.

Recommendation 16. "Direct OSC to finalize the selection of a more geographically distant location to store backup files." **Concur.** In the interim, critical OSC data files will be shuttled to a site in the Washington DC area. In the long term, backups may occur through a high-speed dedicated line serving FINCEN and OSC as mutual backup sites.