Department of Homeland Security
Office of Inspector General

Coast Guard Has Taken Steps To Strengthen Information Technology Management, but Challenges Remain

OIG-11-108

September 2011

Office of Inspector General

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

Homeland Security

September 7, 2011

Preface

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

This report addresses the effectiveness of United States Coast Guard's planning, acquisition, implementation, and use of technology to support its mission. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank Deffer
Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

AIS	Automatic Identification System
C2PC	Command and Control Personal Computer
C3CEN	Command, Control, and Communications Engineering Center
C4IT	Command, Control, Communications, Computers, and Information Technology
CAS	Core Accounting System
CBP	Customs and Border Protection
CIO	Chief Information Officer
DHS	Department of Homeland Security
FPD	Financial Procurement Desktop
FY	fiscal year
IT	information technology
ITAR	Information Technology Acquisition Review
ITIL	Information Technology Infrastructure Library
MISLE	Marine Information for Safety and Law Enforcement
MD	Management Directive
MSAM	Major Systems Acquisition Manual
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OSC	Operations Systems Center
SDLC	Systems Development Life Cycle

Table of Contents/Abbreviations

SELC	Systems Engineering Life Cycle
TASC	Transformation and Systems Consolidation
TISCOM	Telecommunications & Information Systems Command

List of Figures

Executive Summary

We audited the United States Coast Guard's management of information technology. The objective of our audit was to determine the effectiveness of the Coast Guard's planning, acquisition, implementation, and use of technology to support its mission. The scope and methodology of this audit are discussed further in appendix A.

The Coast Guard has made progress establishing effective information technology management practices. Specifically, the Coast Guard has an up-to-date strategic plan for information technology that is in line with federal requirements and departmental guidance. In addition, the Coast Guard has implemented the department's system life cycle management and acquisition review processes. As a result, the Chief Information Officer is positioned to support the Coast Guard's mission, and has controls in place to allow for effective acquisition decisions.

The Chief Information Officer has also taken steps to centralize and standardize implementation of information technology across the Coast Guard. Achieving a standard information technology environment, however, has been hampered by the Chief Information Officer's limited authority over some information technology assets and spending. Consequently, the Chief Information Officer cannot fully ensure that the information technology environment is functioning effectively and efficiently.

Still, the Coast Guard could improve information technology management in a number of areas. Specifically, Coast Guard systems and infrastructure do not fully meet mission needs. For example, Coast Guard field personnel do not have sufficient network availability, and the aging financial system is unreliable. In addition, command center and partner agency systems are not sufficiently integrated. These limitations have various causes, including technical and cost barriers, aging infrastructure that is difficult to support, and stovepiped system development. As a result, field personnel rely on inefficient work-arounds to accomplish their mission.

Background

The United States Coast Guard, one of the Nation's five armed services, is a maritime military service within the Department of Homeland Security (DHS). The Coast Guard has 11 missions: Ports, Waterways, and Coastal Security; Drug Interdiction; Aids to Navigation; Search and Rescue; Living Marine Resources; Marine Safety; Defense Readiness; Migrant Interdiction; Marine Environmental Protection; Ice Operations; and Other Law Enforcement.[1] In fiscal year (FY) 2010, the Coast Guard's budget was $10.1 billion, approximately 18% of DHS' overall requested budget of $55.1 billion.

The Coast Guard has 50,256 full-time personnel (42,389 military and 7,867 civilian) and 36,946 reservists and auxiliary personnel stationed across the country at Coast Guard headquarters units and operations units. The operations units are organized under the Atlantic and Pacific Area commands, which are composed of nine districts that are further broken down into 35 sectors with supporting stations. Coast Guard assets consist of 250 cutters, 1,784 boats, and 198 aircraft.[2]

The Coast Guard headquarters units are organized under the central command of the Commandant and eight Assistant Commandants: Human Resources; Intelligence & Criminal Investigations; Engineering and Logistics; Marine Safety, Security, and Stewardship; Command, Control, Communications, Computers, and Information Technology (C4IT); Capability; Resources; and Acquisition. Figure 1 shows the Coast Guard's organizational structure.

[1] 6 U.S.C. 468(a).
[2] A cutter is any Coast Guard vessel at least 65 feet in length, and a boat is any vessel under 65 feet in length.

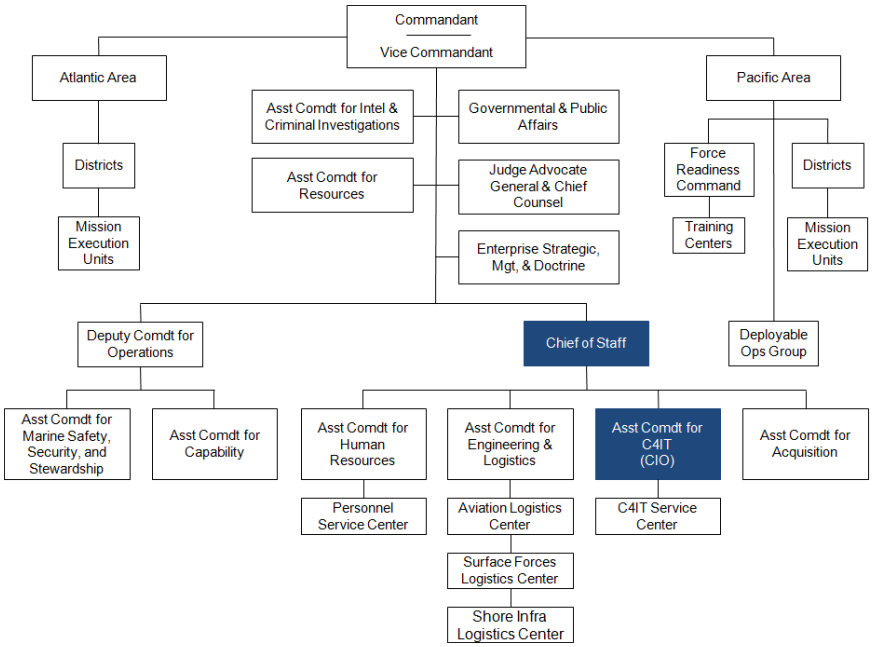

Figure 1: Coast Guard Organizational Structure

Under the Coast Guard Chief of Staff, the Assistant Commandant for C4IT, who serves as the Chief Information Officer (CIO), designs, develops, deploys, and maintains information technology (IT) solutions for the entire Coast Guard. The Office of the CIO (OCIO) comprises approximately 110 staff at headquarters, including military and civilian personnel, who work in one of six IT offices: Information Management; Enterprise Application Management; Enterprise Infrastructure Management; Information Assurance & Spectrum Policy; Enterprise Architecture & Governance; and Enterprise System Development Policy. Figure 2 shows the Coast Guard OCIO organizational structure.

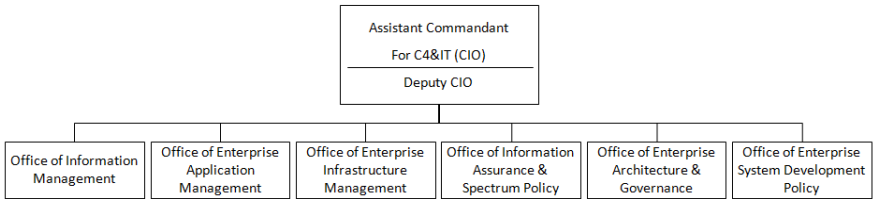

Figure 2: Coast Guard OCIO Organizational Structure

In 2009, the CIO established the C4IT Service Center. The C4IT Service Center is responsible for operations and maintenance of IT systems and assets across the Coast Guard. The mission of the Service Center is to provide full life cycle support for Coast Guard IT applications, systems, and infrastructure, enabling Coast Guard personnel to have the information they need to perform their jobs.

The Service Center has an annual budget in excess of $400 million, with 3,100 employees (including military, government, and contractor), located in more than 70 locations within the United States. Figure 3 shows the organizational structure of the Service Center, which is composed of four shared-services offices, a field services division, and three centers of excellence.

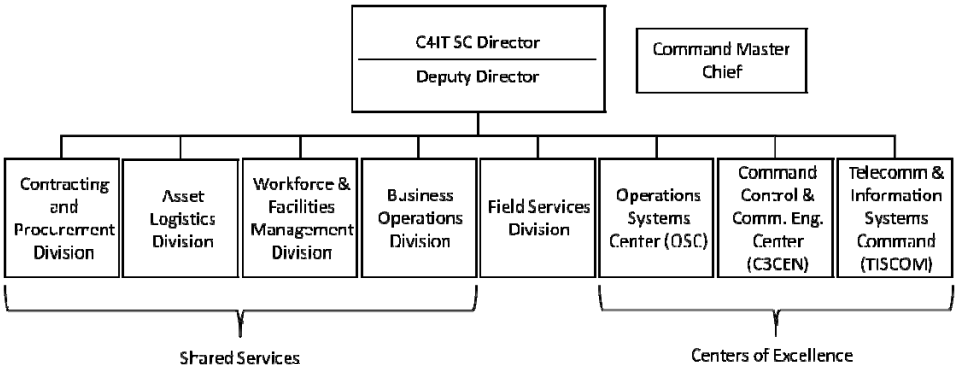

Figure 3: C4IT Service Center Organizational Structure

The four shared-services offices enable delivery of mission capability and service to customers located throughout the Coast Guard. The Field Services Division oversees 11 IT support units and their subordinate detachments located at the Coast Guard's operations units. The centers of excellence include the Operations Systems Center (OSC), which is responsible for enterprise IT systems; the Command, Control, and Communications Engineering Center (C3CEN), which is responsible for command, control, and navigation systems; and the Telecommunications & Information Systems Command (TISCOM), which is responsible for enterprise IT infrastructure.

The Coast Guard relies heavily on technology to meet its safety, security, and stewardship missions. The CIO has program management responsibility for 140 enterprise applications, including law enforcement databases such as Marine Information for Safety and Law Enforcement (MISLE) and search and rescue tools such as the Search and Rescue Optimal Planning System. The Coast Guard also relies on numerous command and control systems, as well as navigation systems, to support tactical units, including systems such as Rescue 21, a direction-finding communication network for search and rescue. In addition, the Coast Guard relies on enterprise infrastructure capabilities, such as messaging systems and network connectivity to deployed cutters. The Coast Guard had an FY 2010 IT budget of approximately $590 million to support its IT environment.

Over the past several years, a number of audit reports have identified key IT challenges within the Coast Guard. In August 2006, we reported that the Coast Guard's efforts to develop its Deepwater Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems could be improved with regard to requirements management, system security, and testing.[3] In addition, in July 2009, we reported that the Coast Guard had made progress in developing its enterprise architecture; however, the enterprise architecture had not been fully integrated across the organization.[4]

Results of Audit

Coast Guard IT Planning and Acquisition Processes

The Coast Guard has implemented IT planning and acquisition processes. Specifically, the Coast Guard CIO has an up-to-date strategic plan that is in line with federal requirements and departmental guidance. In addition, the Coast Guard has implemented the DHS life cycle process for major IT acquisitions, as well as an IT acquisition review process. As a result, the CIO will be strongly positioned to provide effective IT support to meet mission requirements, has controls in place to allow for effective acquisition decisions, and has improved visibility of IT acquisitions throughout the Coast Guard.

IT Planning

The *Government Performance and Results Act of 1993*, as amended, holds federal agencies responsible for strategic planning to ensure efficient and effective operations and use of resources to achieve mission results.[5] Additionally, Office of Management & Budget Circular A-130, as revised, instructs agency CIOs to create a strategic plan that demonstrates how information resources will be used to improve the productivity, efficiency, and effectiveness of government programs.[6] Finally, *DHS Management Directive (MD) 0007.1* requires component CIOs to develop and implement an IT strategic plan that clearly defines how IT supports a

[3] *Improvements Needed in the U. S. Coast Guard's Acquisition and Implementation of Deepwater Information Technology Systems* (OIG-06-55), August 2006.
[4] *Review of U.S. Coast Guard Enterprise Architecture Implementation Process* (OIG-09-93), July 2009.
[5] Public Law 103-62 (1993).
[6] Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, November 28, 2000.

component's mission and drives investment decisions, guiding the component toward its goals and priorities.[7]

The Coast Guard CIO has an up-to-date strategic plan that is in line with federal requirements and departmental guidance. Specifically, the CIO implemented the *C4IT Strategic Plan FY11–FY15* in January 2010. The C4IT strategic plan identifies five broad goals for achieving the OCIO's mission over the next 4 years. Figure 4 shows these five goals.

C4IT Strategic Plan Goals				
Goal 1 Information	**Goal 2 Technology**	**Goal 3 Security**	**Goal 4 Governance**	**Goal 5 Organizational Excellence**
Improve and encourage information sharing, quality, efficiency, and compliance with internal and external partners.	Deliver mission-focused, interoperable, and innovative C4IT solutions for the enterprise.	Enhance mission effectiveness by preventing C4IT security incidents, such as Cyber attacks and intrusions, and enhancing C4IT security mitigation, awareness, and compliance.	Govern C4IT enterprise through the execution of technical authority and effective processes for enterprise architecture, capital planning and investment control, system development, project management, performance measurement, and requirements.	Achieve C4IT organizational excellence by continually developing our workforce, collaborating with internal and external partners, and improving business processes.

Figure 4: C4IT Strategic Plan Goals

To accomplish these broad goals, the CIO has established specific initiatives in an annual performance plan. For example, in order to meet the governance goal, the CIO is implementing a systems development life cycle (SDLC) process to ensure the selection, validation, and fulfillment of IT requirements. The performance plan identifies key quarterly milestones for each specific initiative. In addition to milestones, the CIO has identified the critical success factors that must be completed and operational levels that must be maintained for the OCIO to achieve its goals.

The C4IT Strategic Plan aligns with federal, DHS, and Coast Guard strategic plans and guiding strategies, such as the federal homeland security and maritime security strategies and the DHS and Coast Guard strategic plans. The plan is also aligned with the *DHS Information Technology Strategic Plan 2011–2015* to ensure that the Coast Guard supports the DHS CIO's department-wide IT goals. Finally, the plan aligns with *The Commandant's Guiding Principles,* which are intended to challenge Coast Guard personnel

[7] Department of Homeland Security, Management Directive 0007.1, *Information Technology Integration and Management,* March 15, 2007.

to refocus on their missions. Figure 5 shows the alignment of the C4IT Strategic Plan with federal, DHS, and the Coast Guard plans.

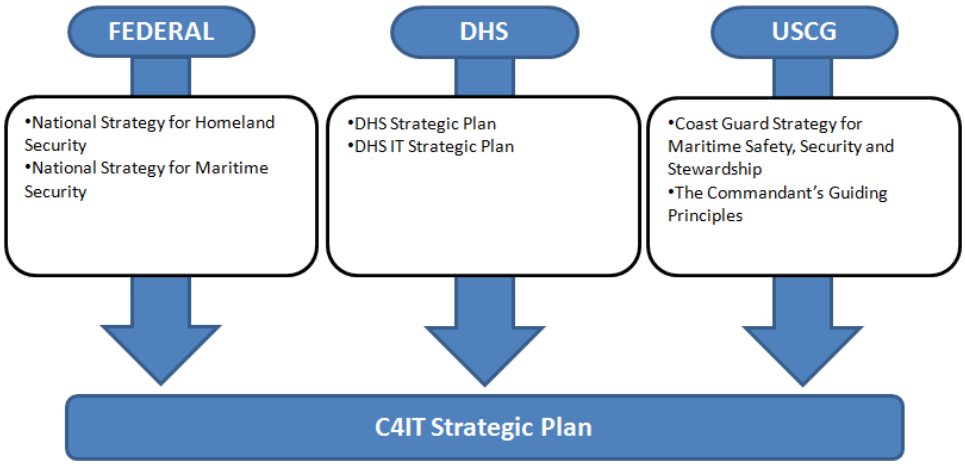

Figure 5: C4IT Strategic Plan Alignment

The CIO's implementation of a well-aligned, up-to-date strategic plan positions the CIO to provide effective IT support to meet mission requirements. An effective IT strategic plan helps focus limited resources and guide the direction of the OCIO. Further, organizational alignment with the plan cascades down throughout the OCIO. For example, division and office plans contain goals to help accomplish the C4IT strategic goals, and individual performance plans for Coast Guard personnel are tied to the division and office plans. This structure affords alignment at all levels of Coast Guard IT personnel activity. As long as the milestones are met and initiatives are put into practice, the IT strategic plan will help Coast Guard personnel fulfill their mission responsibilities.

IT Acquisition

The *Clinger-Cohen Act of 1996* requires that IT acquisition be a simplified, clear, and understandable process to the maximum extent practicable.[8] To support this requirement, DHS Acquisition Directive 102-01, appendix B, requires agencies to follow a systems engineering life cycle (SELC) process.[9] The purpose of the DHS SELC is to establish a standard system life cycle framework across DHS components and to ensure that DHS IT capabilities are efficiently and effectively delivered.

[8] Public Law 104-106 (1996).
[9] DHS AD 102-01, Interim Version 1.9, *Acquisition Directive*, Instruction Appendix B, November 7, 2008.

The Coast Guard has implemented the DHS SELC process for major IT acquisitions, which are acquisitions with a life cycle cost of $300 million and above. Specifically, the Coast Guard developed the Major Systems Acquisition Manual (MSAM) to establish policies and procedures and provide guidance for the implementation of an acquisition management and review process as defined by Acquisition Directive 102-01. The MSAM process has five major phases. These phases require that the Coast Guard identify a capability gap before formally beginning the acquisition of a major system, define the functional capabilities needed to address that gap, analyze alternate solutions, demonstrate the feasibility of the preferred alternative, and deploy the operational capability.

The Coast Guard has also defined an SDLC for non-major IT acquisitions with a life cycle cost below $300 million. The SDLC has seven major phases. The process begins with conceptual planning to identify high-level business needs, propose and validate a concept to fulfill those needs, and commit resources. The next phase, planning and requirements, involves collecting, defining, and validating business requirements and developing initial life cycle management plans. The design phase translates business requirements into system requirements to develop the detailed system design. During the development and testing phase, systems are developed or acquired and validated through a variety of tests. The objective of the implementation phase is to produce and deploy the operational capability. The operations and maintenance phase involves ensuring that the system continues to perform according to specifications. Finally, the disposition phase involves the termination of the system at the end of the life cycle.

As shown in figure 6, the major phases of the MSAM are aligned with the major phases of the DHS SELC. Likewise, the major phases of the SDLC are aligned with the MSAM and the DHS SELC.

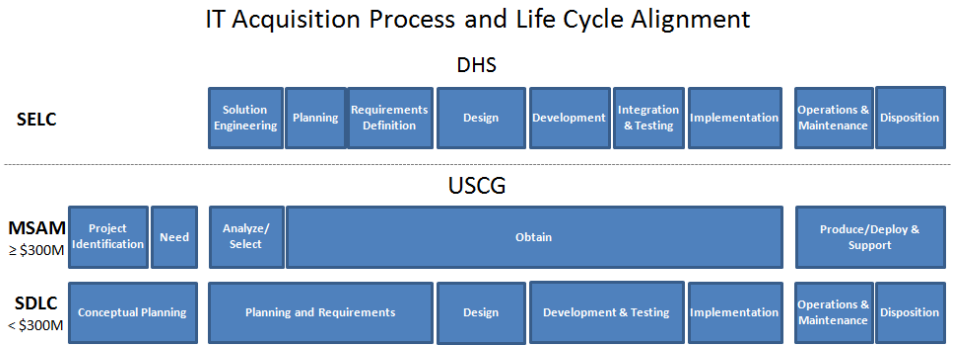

Figure 6: IT Acquisition Process and Life Cycle Alignment

In addition to aligning with the DHS SELC, the Coast Guard's IT acquisition governance processes are streamlined and clearly laid out in order to ensure adherence and compliance. These IT acquisition governance processes enable the Coast Guard to make IT acquisition decisions that will support both Coast Guard and DHS strategic goals.

IT Acquisition Review Process

DHS MD 0007.1, issued in March 2007, requires IT acquisitions valued at $2.5 million or greater to be submitted to the DHS CIO for review. The directive also requires agency CIOs to implement an IT Acquisition Review (ITAR) process for IT acquisitions below $2.5 million. ITAR is required before the award of an IT procurement. The purpose of the ITAR process is to ensure alignment of acquisitions with IT policy, standards, objectives, and goals across DHS.

The Coast Guard CIO began submitting IT acquisitions valued at $2.5 million and above to the DHS CIO in FY 2007. That year, the Coast Guard CIO submitted 15 IT acquisitions for review. The number of acquisitions submitted had increased to 63 in FY 2010. Figure 7 shows the increase in the number of IT acquisitions submitted to the DHS CIO from FY 2007 to FY 2010.

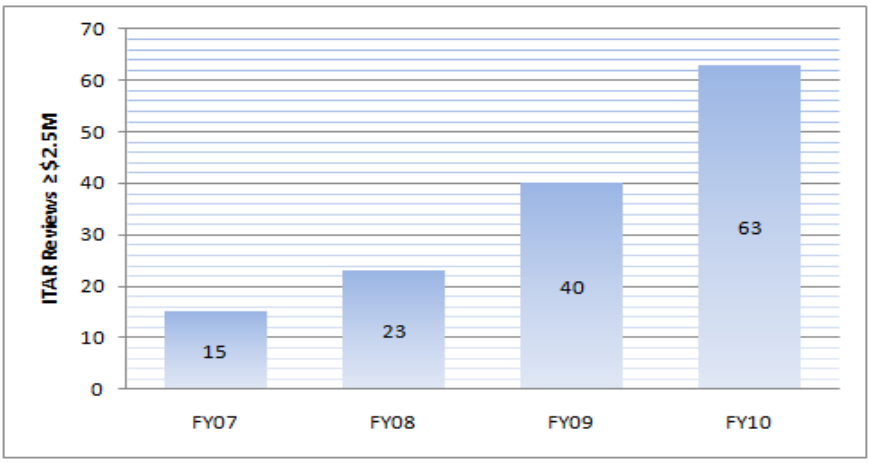

Figure 7: IT Acquisition Reviews ≥ $2.5 Million Submitted to the DHS CIO (FY 2007 to FY 2010)

The Coast Guard has also taken steps to ensure compliance with the ITAR requirement by implementing an ITAR process in FY 2008 to review IT acquisitions with costs below $2.5 million and above $100,000. The Coast Guard Commandant issued a Commandant Instruction in December 2009 mandating compliance with the ITAR process throughout the Coast Guard. In addition, the CIO published an ITAR Practices Guide in 2010 to help guide personnel through the process.

The number of IT acquisitions below $2.5 million going through the ITAR process has increased steadily since the Coast Guard implemented the review process. In FY 2008, the Coast Guard CIO reviewed 40 IT acquisitions. By FY 2010, the CIO reviewed 233 IT acquisitions, an increase of nearly 500%. Figure 8 shows the number of ITAR reviews below $2.5 million from FY 2008 through FY 2010.

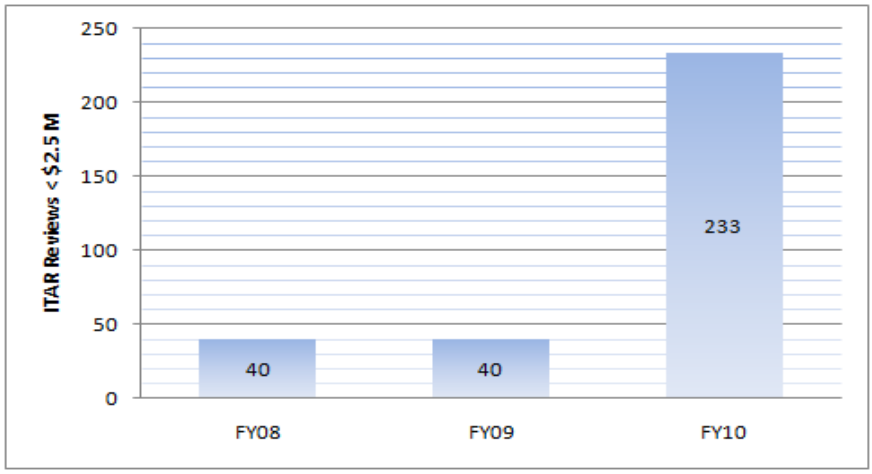

Figure 8: IT Acquisition Reviews < $2.5 Million Conducted by the Coast Guard CIO (FY 2008 to FY 2010)

These reviews have enabled the CIO to align IT acquisitions with Coast Guard IT policies, standards, objectives, and goals. ITAR also helps the CIO validate the Coast Guard's alignment with DHS Enterprise Architecture and ensure compliance with security and accessibility requirements.

IT Implementation

The CIO has taken steps to centralize and standardize IT implementation across the Coast Guard, but more progress is needed. The Coast Guard historically has had a decentralized IT environment, with personnel at each Coast Guard district implementing IT to meet their unique requirements. In response to the evolving need for increased interoperability throughout the Coast Guard, the CIO established the C4IT Service Center in February 2009 as a central authority to promote enterprise-wide IT standardization. The C4IT Service Center has unified the Coast Guard's three IT centers of excellence, defined standard processes for field IT units, and defined standard IT portfolios with product lines and core technologies. In addition, C4IT Service Center leadership has several initiatives under way to further improve IT operations and maintenance.

Although the Coast Guard has made progress, achieving a standard IT environment has been hampered by the CIO's limited authority over some IT assets and spending. Specifically, not all IT personnel have been moved under the CIO, and the CIO does not have sufficient oversight of IT spending by field units. The 2006 Coast Guard modernization plans called for the CIO to have authority over IT personnel and spending. However, there is no overall plan of action and target dates to complete the transition of authority. Without such authority, the CIO cannot fully

ensure that the Coast Guard IT environment is functioning effectively and efficiently.

Progress Centralizing IT Implementation

The *Clinger-Cohen Act of 1996* gives the CIO responsibility for developing, maintaining, and facilitating the implementation of a sound and integrated IT architecture and promoting the effective and efficient design and operation of all major information resources management processes. Furthermore, a centralized approach to IT implementation is a government and industry best practice to improve performance and lower cost.

The Coast Guard has taken steps to centralize and standardize IT implementation enterprise-wide. The Coast Guard began a modernization effort in 2006 with the goal of creating a more unified service, in part to address the challenges faced in responding to Hurricane Katrina. To realize the vision of a modernized Coast Guard, Commandant Intent Action Order #10 directed the CIO, as the single Coast Guard director of C4IT, to standardize the IT environment across the Coast Guard.

As part of the modernization effort, the CIO established the C4IT Service Center in February 2009, bringing together the operating units, logistics centers, and other support units that performed the engineering, management, and service resources and functions previously distributed across OCIO offices. The Service Center provides full life cycle support for Coast Guard IT applications, systems, and infrastructure, providing Coast Guard personnel with the information they need to perform their jobs.

Unified Three Centers of Excellence

The C4IT Service Center brings together under one reporting structure the following three organizations (known as centers of excellence) that are responsible for headquarters-level operations and maintenance of enterprise-wide IT infrastructure and systems:

- OSC – Develops, fields, maintains, and provides user support for Coast Guard enterprise information systems to improve Coast Guard mission performance through the innovative application of technology.

- TISCOM – Develops, deploys, secures, and supports the Coast Guard's IT infrastructure for both the sensitive but unclassified and secret enterprises. Solutions are divided

into three areas: (1) enterprise networks, (2) information systems, and (3) organizational messaging.

- C3CEN – Develops, builds, fields, trains, and supports advanced electronic command, control, and navigation systems.

Communication and coordination among OSC, TISCOM, and C3CEN was a challenge before the C4IT Service Center was established. For example, TISCOM is in charge of implementing security patches for the enterprise IT infrastructure.[10] When a security patch is implemented, it can affect OSC's enterprise systems. In one case, TISCOM implemented a patch that caused a malfunction in the MISLE system. The OSC told users to remove the security patch to restore MISLE functionality. However, the patch was a required security update, and when TISCOM personnel scanned the network to identify where the patch was still needed, they reinstalled it and once again affected MISLE functionality.

Although the three centers of excellence remain independent commands under the Coast Guard's military organizational structure, they report to the director of the Service Center. Coast Guard IT officials said that the centers of excellence are working more closely together. The centers' consolidation under the C4IT Service Center enables improved communication and coordination, which are critical to effective IT support.

Standard IT Field Services

Prior to the Coast Guard modernization effort, responsibility for IT operations and maintenance was decentralized. Each Coast Guard district had its own IT support unit that reported directly to its local operational command and provided IT solutions tailored to the priorities and mission set of that location. The decentralized approach tailored infrastructure design, deployment, service levels, and support delivery to more individualized needs. Although a decentralized approach was able to meet the Coast Guard's needs at first, it became less effective as the need developed for increased interoperability and enterprise-wide information sharing.

The director of the C4IT Service Center established the Field Services Division to oversee the 11 district IT support units and

[10] A patch is a small piece of code designed to be inserted into a program in order to fix errors in or update the program or its supporting data.

lead the standardization of IT support processes and activities. Field Services Division personnel have defined standard processes for various IT support activities. For example, division personnel defined a standard IT service desk process guide to replace the unique processes being used by each IT support organization. Field Service Division personnel have defined nine such process guides to improve standardization of IT support service across the Coast Guard districts. These process guides cover a range of topics, including response to system failures, IT system backup procedures, and standard configuration of IT systems on cutters. Field Services Division personnel have also identified eight more processes to standardize, including management of network access and radio tower maintenance. Field IT personnel said that process standardization has been beneficial. For example, when Coast Guard personnel transfer to another location, they continue to receive the same level and type of IT help desk service.

Product Lines and Core Technologies

The C4IT Service Center established a portfolio management approach to improve standardization by defining a set of product lines and core technologies that are supported throughout the Coast Guard. The product line concept is intended to provide better focus on customers by putting the personnel responsible for product engineering, maintenance planning, procurement, and supply into a single organization with a singular focus on service. Core technologies are IT assets that are used to support several product lines. For example, the radio communications core technology provides radio communications systems to product lines supporting command centers, communications stations, small boat stations, boats, and cutters. This model allows for accountability and control of the use, maintenance, and upgrades of IT infrastructure. Coast Guard field personnel said that IT standardization through core technologies and accountability through product lines is beneficial. With fewer different technologies to support, the C4IT Service Center will be able to provide better support, and personnel will require less training when they transfer between districts.

Ongoing C4IT Service Center Standardization Initiatives

The C4IT Service Center leadership has begun other initiatives to improve Coast Guard IT operations and maintenance. The C4IT Service Center plans to complete implementation of the service delivery best practice (the Information Technology Infrastructure Library (ITIL)), strengthen configuration management, and

implement a centralized service desk. The director of the C4IT Service Center said that the organization remains a work in progress as it has been in place for only about 2 years. The C4IT Service Center is scheduled to complete standardization and centralization initiatives by 2014.

Service Delivery

In March 2010, the C4IT Service Center leadership adopted ITIL to manage IT service delivery. ITIL is a set of concepts and practices for managing IT services, development, and operations. The goal of ITIL is to provide the standard terminology, processes, and continual improvement framework necessary to plan and manage IT services more effectively and efficiently. Further, ITIL will provide a tool to manage the increasingly critical and extensive suite of IT services that the C4IT Service Center provides. The C4IT Service Center continues to work on the standardization of support processes as part of ITIL implementation.

Configuration Standardization

C4IT Service Center leadership is standardizing how field units configure their IT environment.[11] Service Center personnel test IT changes using a standard configuration before deployment to the field. Field units, however, may not have the same IT configuration as headquarters, which causes IT challenges in the field that were not present at headquarters. Field personnel said that when headquarters deploys an IT change, it does not always function in the field as expected. For example, when an upgrade to the standard operating system image was pushed out, some enterprise applications did not perform properly. Field personnel said that headquarters personnel test systems in an ideal environment that does not adequately replicate the challenges in the field environment. The C4IT Service Center's goal is to standardize the IT configuration across field units to avoid such problems going forward.

Centralized Service Desk

C4IT Service Center leadership plans to centralize the Coast Guard's 11 service desks into one centralized service desk located

[11] Configuration management is a process for establishing and maintaining consistency of a system's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life. The configuration management process provides a means to document and control the adaptation and evolution of simple and complex systems. It is the management of changes that are made to the hardware, software, firmware, and documentation throughout a system's life cycle.

in St. Louis, MO. The centralized service desk is a best practice of the IT industry. Once implemented, OCIO officials said that it will support IT modernization and drive cost savings. The initial operating capability for the centralized service desk is scheduled for June 2011.

Once implemented, the centralized service desk is intended to achieve three main objectives. First, it is intended to provide consistent service. All Atlantic and Pacific area procedures for providing IT support would be placed into a single construct to serve the entire enterprise. All users would then have the same interface for IT support, regardless of location. Second, this model is intended to provide a single internal touch point in the C4IT program, giving C4IT product lines at TISCOM, OSC, and C3CEN a unified pathway for incident management and request fulfillment. Third, it is intended to provide increased service at reduced cost. By leveraging the collective strengths of district-level service desks at one location, service can be expanded from a local 8-to-4, Monday-through-Friday operation into a global operation running 24 hours a day, 365 days a year.

Although the C4IT Service Center is still a work in progress, its benefit was evident during the Coast Guard's response to the earthquake in Haiti and the Deepwater Horizon oil spill. The head of the Field Services Division was able to pull both people and equipment from Coast Guard units across the country to respond to these disasters. For Deepwater Horizon, Coast Guard leadership set up a separate command with its own flag officer so that the regular flag officer in the district could continue to work on other missions. In addition, OCIO leadership set up a separate IT support unit within the temporary command with its own around-the-clock IT service.

Additional Progress Needed To Complete IT Centralization

Additional progress is needed to ensure that the CIO has the authority to implement a standardized Coast Guard IT environment. Specifically, the CIO does not have adequate authority over some headquarters IT personnel and discretionary IT spending in the field. Although the 2006 Coast Guard modernization plans called for giving the CIO authority over IT personnel and spending, there is no overall plan of action and target dates. Without authority over all IT resources, the CIO cannot fully ensure that the Coast Guard IT environment is functioning effectively and efficiently.

CIO Authority Over Headquarters IT Personnel and Operations

Although a significant amount of IT resources have been transferred to the CIO, the CIO does not have sufficient authority over some IT personnel and operations at headquarters. Prior to Coast Guard modernization, each Assistant Commandant had an IT office and staff. Coast Guard modernization plans called for program IT operations to be transitioned to the CIO. Some of the programs transferred their IT offices and staff, including about 40 staff from the Deputy Commandant for Operations, Assistant Commandant for Human Resources, and the Assistant Commandant for Resources. In June 2008, the Chief Financial Officer transferred authority over $89,995,000 in headquarters funding for IT investments from program offices to the CIO.

However, approximately 165 personnel working in IT functions within several Coast Guard divisions are not part of the CIO organization. Figure 9 shows the Coast Guard divisions that maintain IT personnel independent from the CIO.

IT Personnel Outside the OCIO		
Coast Guard Division	**Center**	**Number of IT Staff**
Assistant Commandant for Engineering and Logistics	Aviation Logistics Center	29
Assistant Commandant for Engineering and Logistics	N/A	7
Assistant Commandant for Human Resources	Pay and Personnel Center	44
Assistant Commandant for Intelligence and Criminal Investigations	N/A	15
Assistant Commandant for Resources	Finance Center	70
Total		**165**

Figure 9: IT Personnel Outside of the OCIO

In addition, the Finance Center, Pay and Personnel Center, and Aviation Logistics Centers have independent IT operations. For example, the Finance Center maintains its own data center, which is distinct from the Coast Guard data center at the OSC.

Although the Coast Guard divisions with IT personnel coordinate with the CIO, creating a standardized IT environment without direct control remains a challenge. These small IT operations must be moved to establish a clear line of authority to the CIO IT support activities. For example, when the CIO published a Coast Guard-wide notification explaining how the new C4IT Service Center would support IT operations through product lines and core technologies, it was necessary to include exceptions for the IT offices that remain outside the CIO. The notification announced that until Coast Guard modernization is complete, some units retain their own IT support and would remain an exception to the process described.

The CIO does not have authority over these IT personnel and assets because transition plans to align these personnel under the CIO's authority have not been completed. The CIO is discussing the transition of IT personnel with leadership from these divisions. However, there is no documented transition plan that sets forth the actions to be taken and the related milestones. The CIO's current plan is to establish product lines for these functions and then shift operational control of the IT staff to the CIO or C4IT Service Center. Although the initiative to consolidate IT under the CIO began in 2006, one senior Coast Guard official said that responses to major incidents such as the Deepwater Horizon oil spill and the earthquake in Haiti have delayed progress. Without a documented plan of action and milestones, there is risk that consolidation activities will continue to be delayed.

CIO Authority Over Field Unit IT Resources

The CIO also does not have sufficient oversight of IT spending by Coast Guard field units. Field units can purchase IT with discretionary funds without CIO review and approval. OCIO officials said that field units obtain IT and then request that it be connected to the Coast Guard network; however, at that point it is too late for the CIO to prevent investments in IT that does not comply with enterprise standards, such as those relating to security and alignment to the enterprise architecture. For example, personnel from one Coast Guard sector asked to connect a system that they had obtained to the network. However, thousands of security vulnerabilities in the system had to be resolved before the system could be connected. The CIO's standardization effort is also hindered when field units buy items outside of the defined core technologies and product lines.

The CIO does not have sufficient oversight of IT spending by Coast Guard field units because plans to implement this oversight have not been completed. The Chief Financial Officer identified the need to consolidate field IT funding under the CIO through a process similar to that conducted for headquarters. However, this phase of consolidating funds has not been completed even though it was initially scheduled to be accomplished in FY 2009. Ultimately, the CIO's lack of control over field units' IT acquisitions can result in wasted time and money due to uncoordinated, duplicative investments.

IT Use To Support the Coast Guard's Missions

Coast Guard IT systems and infrastructure do not fully meet mission needs. Specifically, Coast Guard field personnel do not have sufficient network availability, and the aging financial system is unreliable. In addition, command center and partner agency systems are not sufficiently integrated. These limitations have various causes, including technical and cost barriers, aging infrastructure that is difficult to support, and stove-piped system development. As a result, field personnel rely on inefficient workarounds to accomplish their mission.

Network Availability

Under the *Paperwork Reduction Act of 1995*, as amended, and the *Clinger-Cohen Act of 1996*, agencies are required to acquire, manage, and use IT to improve mission performance.[12] Coast Guard field personnel, however, face network and data availability challenges in several areas. Specifically, Coast Guard cutters do not have sufficient network connectivity while at sea; command centers do not have systems that can adequately track Coast Guard and partner agency vessels; and the new Rescue 21 system, a direction-finding communication network for search and rescue, suffers from network outages.

Cutter Connectivity

Coast Guard cutters do not have sufficient network connectivity. Specifically, many cutters have not yet been connected to the Coast Guard's network. Network connectivity has been installed in 64 of the 99 cutters that were initially chosen to receive the capability. An additional 141 cutters of various types are included in a planned expansion of broadband communication to the fleet. Currently, however, only 27% of the cutter fleet has connectivity capability installed. Figure 10 shows the cutter fleet network connectivity installation status.

Cutter Network Connectivity Installation Status			
Phase	Number of Cutters with Capability Installed	Number of Cutters Identified for Installation	Percent
Initial Installation	64	99	65%
Planned Expansion	0	141	0%
Total	64	240	27%

Figure 10: Current Fleet Network Connectivity Installation Status

[12] *Paperwork Reduction Act of 1995*, as amended, Public Law 104-13 (1995).

For cutters that have connectivity installed, technical barriers can cause insufficient underway connectivity. Specifically, land-based wireless network connectivity is not feasible for cutters that deploy to distances beyond the range of towers, and as a result the Coast Guard must rely on satellite connectivity, which is more expensive and has limited bandwidth. Other technical barriers include limited space for antenna placement on smaller cutters and the risk of antenna blockage due to the constant movement of the water.

In addition, the high cost of obtaining bandwidth at sea limits connectivity. The Coast Guard relies on private companies for access to bandwidth. The cost of providing connectivity has increased because of the limited number of providers competing to offer bandwidth service at sea and the large amount of bandwidth being purchased by private companies, such as cruise companies. Bandwidth becomes exceedingly expensive when Coast Guard ships travel beyond 200 miles from shore. Although the Coast Guard spends the vast majority of its time within 200 miles of the coast, mission needs may require going beyond this distance. For example, the need for large cutters to travel greater distances has increased recently as shipping passageways have opened in the arctic. Large cutters traveling greater distances require an increase in bandwidth requirements, which increases the cost of obtaining connectivity. The cost of connectivity outside of the 200-mile barrier has been higher than expected. According to a senior Coast Guard official, the funding for increased bandwidth will run out in June 2011, forcing the Coast Guard to shift funds from other areas.

As a result of underway connectivity limitations, Coast Guard personnel face challenges meeting their mission and administrative responsibilities. Personnel work around connectivity limitations in ways that are inefficient. For example, personnel at one Coast Guard sector said that small cutters must run background checks before boarding boats. Without connectivity, these cutters have relied on information being sent over the radio. Sensitive or classified information, however, that may be useful or necessary, cannot be transmitted over unsecured radios. Alternatively, cutters must dock at a nearby port to access needed information, delaying the sharing of information and diverting ships from their posts. For non-secure communication, personnel often use their commercial email provider via a personal wireless device when service is available.

Additionally, Coast Guard personnel without access to underway connectivity are unable to complete required training and

administrative responsibilities while at sea. Technology has been evolving away from stand-alone systems to network-based systems. Consequently, as more administrative IT tools are added to the Coast Guard network, personnel deployed to cutters need greater network availability.

To improve cutter connectivity, the Coast Guard has implemented satellite service using one service provider for global connectivity and a second provider for service within 200 miles of the coast at a lower cost. According to Coast Guard officials, moving to two providers has lowered cost and allowed the Coast Guard to increase both the available bandwidth and download speed, although connectivity is still slow for users accustomed to desktop communication speeds. Personnel in one sector said that the addition of connectivity to their cutter allowed them to view emails and access websites to facilitate mission activities. Although the Coast Guard is working to improve underway connectivity, officials acknowledge that additional bandwidth will be needed to meet the requirements of Coast Guard personnel.

Blue Force Tracking

Coast Guard districts and sectors do not always have adequate information on the location of their own and their partners' assets. The ability to determine the location of assets is referred to as blue force tracking. Coast Guard operational units need to know where Coast Guard assets, including small boats, cutters, and aircraft, are at all times. For tracking purposes, the Coast Guard's waterborne assets are equipped with an Automatic Identification System (AIS) transponder, which is similar to an airplane's black box that provides location information. The Coast Guard encrypts the AIS signal so that only receivers able to decode the signal can see the asset's position. The Coast Guard relies on blue force tracking to create a common operating picture by determining the location of its waterborne assets and to differentiate Coast Guard vessels from commercial or unfriendly ships. Using this information, the Coast Guard can establish which of its assets are in the best position to respond to situations, including search and rescue and law enforcement missions.

One technical barrier to adequate blue force tracking is that the encrypted AIS signal cannot be received beyond a limited range. The range is determined by the height of the ship's antenna and the receiving tower. Consequently, districts or sectors with a large area of responsibility may have cutters that travel more than

15 nautical miles from shore and cannot be tracked without additional transmission options.

In addition to the limited range of the encrypted AIS signal, Coast Guard districts and sectors rely on several different display systems, including the primary system, Command and Control Personal Computer (C2PC), instead of one consolidated display system to view blue force tracking information. Field personnel said that C2PC does not receive a constant signal, and an asset's position can be days old. Some sectors have upgraded from C2PC to the new Coast Guard standard Geographic Information System tool, ArcGIS. Although ArcGIS is a more modern system than C2PC, Coast Guard personnel said that it is slow to load information and that it freezes. Sectors and stations in one district accustomed to using Google Earth found the new ArcGIS system performance so poor that they stopped tracking blue forces using this system.

The blue force tracking system limitations have required command center personnel to resort to non-automated, inefficient workarounds. Specifically, personnel rely on voice communication to obtain the geographic coordinates of deployed assets and plot their locations manually. This process is inefficient and can affect the safety of Coast Guard personnel. For example, without automated tracking, Coast Guard personnel may need to radio in their position during high-speed chases, which can be distracting and dangerous. Additionally, when partner agency vessels are not properly accounted for, the vessels may track and pursue one another, wasting time and resources. Personnel at one Coast Guard sector said that the lack of effective blue force tracking has led to the Coast Guard's pursuit of Customs and Border Protection (CBP) boats.

The Coast Guard has undertaken several initiatives to improve blue force tracking. Specifically, the CIO upgraded the infrastructure for the common operating picture database, which is responsible for displaying the positions for Coast Guard and DHS assets, along with the locations of targets of interest, to improve near real-time tracking ability. In addition, the CIO is fielding a replacement for the C2PC system and is consolidating the various display systems that are used across the Coast Guard.

Rescue 21

Rescue 21, the Coast Guard's direction-finding communication network for search and rescue, has availability limitations. Rescue

21 is a command, control, and communications system developed to improve the Coast Guard's search and rescue capabilities. Rescue 21's predecessor, the National Distress System, was targeted for replacement after a high-profile tragedy in 1997, in which the Coast Guard did not respond to a mayday call from the ship *Morning Dew*. As of June 1, 2011 the Rescue 21 system has been successfully employed in over 26,500 search and rescue cases.

Although Coast Guard personnel said that Rescue 21 is a significant improvement over the National Distress System, they also identified challenges associated with the new system. Specifically, Coast Guard sectors have experienced frequent commercial network outages, which reduced system performance and availability. For example, one Coast Guard sector has experienced a total of 80 network outages since FY 2009, with 24 outages in FY 2011. Another Coast Guard sector had an outage that lasted for approximately 2 days. These outages occur because Rescue 21 was created without redundancy when the primary network becomes unavailable.

In addition, Coast Guard field personnel have experienced coverage gaps and tower misalignment issues. For example, one sector employee said that one of the sector's towers was so misaligned that the location provided for a search and rescue would be significantly off. Another sector identified a significant gap in its area of responsibility following system deployment. In this case, the Coast Guard added a temporary additional tower to improve coverage until a permanent site could be constructed. Recue 21 coverage gaps occur because of limitations on the number of towers, site placement, and obstructions such as large buildings.

As a result of Rescue 21 availability and coverage challenges, field personnel must devote resources to fill in performance gaps. For example, at each Coast Guard sector, security patches and system upgrades are deployed to Rescue 21 once a month to mitigate vulnerabilities and maintain certification and accreditation. While the upgrades are being installed, the Rescue 21 system design does not provide redundancy and becomes temporarily unavailable. During this time sector Commanders may use personnel to manually operate towers. In addition, sector Commanders may coordinate aircraft patrols to maintain search and rescue capabilities at great cost to the Coast Guard.

Reliability

The Financial Procurement Desktop (FPD) is the enterprise-wide accounting and procurement system used by the Coast Guard. FPD is used to create and manage simplified procurement documents and to maintain accurate accounting records. The system offers templates to create and record requisitions, financial obligations, and expenditures. Data from FPD is fed into the Core Accounting System (CAS), and information from the two systems must be reconciled.

According to Coast Guard personnel, FPD is slow, cumbersome, and does not always save information. It is also not integrated with CAS, and regularly displays inaccurate information and creates transaction errors that require the Coast Guard's Finance Center to intervene to correct the problem. These issues are exacerbated during times of increased demand. For example, during the last quarter of FY 2010, FPD became unresponsive during normal working hours. At the same time that the system slowed down, financial personnel at Coast Guard districts said that they encountered transactions that doubled or tripled, commitments and obligations that did not liquidate, blank records, and an inability to reconcile their accounts. Similar to FPD, CAS is slow and cannot handle the high number of users employing the system during times of peak demand.

FPD was developed more than 20 years ago, and its software is no longer supported. The Coast Guard is aware that FPD needs to be updated. Coast Guard personnel, however, are working with DHS officials on the Transformation and Systems Consolidation (TASC) initiative to achieve a department-wide integrated financial solution. The Coast Guard CIO had requested that the Coast Guard be the first DHS component to receive TASC, but it was announced that implementation at the Coast Guard would follow implementation at another agency. There is no timeframe for when this will occur. No major upgrades will be made on FPD while the Coast Guard awaits the implementation of TASC.

In the absence of major upgrades, Coast Guard personnel must continue to rely on FPD, leading to continued inefficiency in reconciling financial information. Specifically, the financial statements audit for FY 2010 found that the Coast Guard had material weaknesses in internal controls due, in part, to system

challenges.[13] Further, during the fourth quarter of FY 2010, Coast Guard budget personnel were not comfortable certifying FPD results because they could not guarantee that accounts were accurate and consistent with recorded transactions. During the same period, FPD slowed down and eventually became unresponsive, forcing some personnel to come to work at 2 a.m. and on weekends. Additional delays were caused by CAS and FPD not being integrated, which required Coast Guard personnel to enter the same information twice. Delays caused by FPD and CAS led one district to use almost 100 hours of overtime in order to close financial accounts at the end of FY 2010.

Integration

The *Clinger-Cohen Act of 1996* requires that agencies plan in an integrated manner for managing their IT architecture. Furthermore, the *Suitability and Accountability for Every Port Act of 2006* requires the establishment of Interagency Operational Centers.[14] For a location to officially achieve designation as an Interagency Operational Center, it must maintain a memorandum of understanding establishing interagency cooperation, including joint awareness and coordination with CBP, along with access to a geographic interface tool providing a common operating picture to achieve situational awareness. However, Coast Guard command center, DHS component, and partner agency systems are not sufficiently integrated.

Coast Guard command centers commonly use between five and ten different systems, many of which are not integrated. For example, the Search and Rescue Satellite Aided Tracking system used to help locate distress signals does not communicate with MISLE, which tracks vessel information. As a result, users must search each system independently. Similarly, the maritime search planning tool, Search and Rescue Optimal Planning System, is not integrated with MISLE. Users said that information from this search and rescue system had to be manually added into MISLE.

Limited integration within Coast Guard command centers has been caused by independently developed stovepipe systems created before the modernization effort. Only recently has the OCIO put in place processes to deter components from developing their own IT systems.

[13] *Independent Auditors' Report on DHS' FY 2010 Financial Statements and Internal Control Over Financial Reporting* (OIG-11-09), November 2010.
[14] Public Law 109-347 (2006).

Without system integration, Coast Guard personnel are forced to write down information and then transfer it manually to a separate system, which can affect accuracy and reduce efficiency. Additionally, Coast Guard personnel must manage a large number of passwords for the command center systems, leading to passwords being written down and possible security issues. To improve integration, Coast Guard personnel are working to standardize command centers and increase OCIO control over operational systems.

Similarly, Coast Guard's IT infrastructure is not integrated with DHS components. For example, Coast Guard systems are not effectively integrated with CBP systems. The Coast Guard is unable to connect IT equipment used by CBP to the Coast Guard network during joint ventures. At one designated Interagency Operational Center location, CBP could not send staff to the center because the facility only had access to the Coast Guard network, and consequently the staff could not connect to their own network. In addition, Coast Guard intelligence personnel are unable to access all available DHS databases. Likewise, DHS components are unable to search all the Coast Guard's databases.

Integration between the Coast Guard and fellow DHS components is hampered due to the Coast Guard's status as a military organization and the corresponding ".mil" website domain, which is not conducive to working with other DHS entities that operate on a ".gov" domain. Additionally, DHS components have stovepipe systems that are not accessible to other components. Coast Guard personnel unable to access certain DHS databases rely on phone calls to DHS components to obtain background information on vessels. If Coast Guard personnel are unable to reach their point of contact within separate DHS components, information may not be available prior to an operation.

In addition, Coast Guard and DHS systems are not integrated with federal partner agencies. The Coast Guard is unable to use the DHS network to share sensitive but unclassified information with the Department of Defense, inhibiting the flow of information and communication between the two agencies. Furthermore, personnel at one Coast Guard district that works with up to eight external agencies said that the Coast Guard is not completely compatible with external agencies' communications, systems, or networks.

The inability of the Coast Guard to utilize the DHS network to share sensitive but unclassified information with the Department of Defense is a result of unique security requirements for each

agency. New systems and system patches approved by the Department of Defense must still be certified by DHS, delaying integration between the two departments. Additionally, although DHS is required to establish Interagency Operational Centers with access to a geographic interface tool providing situational awareness, no integrated common operating picture currently exists for use by different federal agencies. Without an integrated common operating picture, federal partners are forced to pass information from one system to another, leading to accuracy issues and a fear that the information being displayed is no longer current. During the response to the Deepwater Horizon disaster, each agency used a different common operating picture, making it difficult to monitor all incoming information.

The Coast Guard has begun deploying WatchKeeper, an integrated common operating picture, to facilitate the implementation of Interagency Operational Centers. Once fully functional, WatchKeeper is intended to pull information from multiple sources, creating a situational awareness of assets and targets, and can coordinate activities, share the schedule of different assets, and help plan joint inspections. Although WatchKeeper has been deployed to seven areas, Coast Guard personnel are skeptical that adequate funding will be provided to maintain the system. Limited funding has slowed the deployment of WatchKeeper and delayed its installation date for at least one Coast Guard Sector.

Recommendations

We recommend that the Coast Guard Chief of Staff:

Recommendation #1: Complete the transition of IT personnel and oversight of field IT spending under the CIO.

We recommend that the Coast Guard Chief Information Officer:

Recommendation #2: Develop a plan of action and milestones to complete the expansion of broadband communication to the fleet to improve underway connectivity.

Recommendation #3: Develop a plan to address the need for near real-time tracking requirements.

Recommendation #4: Implement a plan to ensure system redundancy to meet availability requirements for Rescue 21.

Recommendation #5: Implement a strategy to improve ease of use and availability of the financial systems.

Recommendation #6: Ensure that new tools, such as WatchKeeper, address command center requirements for improved integration.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Rear Admiral of Planning, Resources, and Procurement. We have included a copy of the comments in their entirety in appendix B.

In the comments, the Rear Admiral concurred with our recommendations and provided details on steps being taken to address specific findings and recommendations in the report. We have reviewed management's comments and provided an evaluation of the issues outlined in the comments below.

In response to recommendation 1, the Rear Admiral concurred and stated that the Coast Guard anticipates that this task will take time to implement owing to the necessity of involving senior Coast Guard leadership in the transition plans. Upon resolution of these issues, the Coast Guard anticipates that it will be better positioned to prepare a Plan of Action and Milestones to complete the transition. We look forward to learning about progress made toward addressing this recommendation.

Responding to recommendation 2, the Rear Admiral concurred and stated that the Coast Guard is in the process of deploying methods that will facilitate the faster exchange of data by 15 times the current speed starting in June 2013 for cutters that are underway. We recognize this action as a positive step toward addressing recommendation 2.

In response to recommendation 3, the Rear Admiral concurred and said that the Coast Guard will continue the testing and implementation of the National Automatic Identification System, which will extend coverage and provide near real-time access to data. The Rear Admiral said the data will be displayed in a variety of Coast Guard and DHS applications. We look forward to learning more about continued progress and improvements in the future.

In response to recommendation 4, the Rear Admiral concurred with the recommendation and stated that the Coast Guard has been

working with the DHS OneNet organization to reduce network outage impacts to the system's performance. Additionally, the Rear Admiral said that the Coast Guard has procured and deployed the Very Small Aperture Terminal satellite system at sites with problematic network connections and plans to expand this or a similar network backup capability to 100% of the Rescue 21 remote sites. We believe that such efforts are good steps toward addressing our recommendation and look forward to learning more about continued progress in ensuring system redundancy for Rescue 21.

Responding to recommendation 5, the Rear Admiral concurred and said that the Coast Guard is continuing to develop plans to optimize the financial, procurement, and asset management environments for improving financial transparency. We look forward to learning more about continued progress and improvements in the future.

In response to recommendation 6, the Rear Admiral concurred and stated that the Coast Guard is using WatchKeeper and another new tool, Mission Asset Scheduling Interface, to integrate command centers. Additionally, the Rear Admiral said that evaluations to determine the appropriate single sensor management system and the geographic information system for enterprise use are ongoing. We recognize this action as a positive step and look forward to learning more about continued progress in the future.

As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted an audit to determine the effectiveness of United States Coast Guard's planning, acquisition, implementation, and use of technology to support its mission.

We researched and reviewed federal laws and executive guidance related to the Coast Guard's support of IT systems, IT management, and IT governance. We obtained published reports, documents, and news articles regarding the DHS CIO operations and IT management throughout the department. Additionally, we reviewed recent Government Accountability Office and DHS OIG reports to identify prior findings and recommendations. We used this information to establish a data collection approach that consisted of focused interviews, documentation analysis, site visits, and system demonstrations to accomplish our audit objectives.

We held interviews at and conducted teleconferences with Coast Guard headquarters, district, and sector units. Collectively, we interviewed more than 100 Coast Guard headquarters officials, field unit officials, and system users to learn about the Coast Guard's IT functions, processes, and capabilities. At headquarters, we met with Coast Guard OCIO officials including the CIO, Deputy CIO, branch chiefs, and program managers to discuss their roles and responsibilities related to Coast Guard IT management. We also met with key personnel from the C4IT Service Center, which is responsible for operations and maintenance of the Coast Guard IT infrastructure. Finally, we met with representatives from Acquisitions and Capabilities to understand communication and coordination activities pertaining to IT requirements and acquisition processes.

At district and sector units, we met with commanding officers, IT branch chiefs, IT specialists, program area specialists, and system users to understand IT development practices, user requirements, and system use in the field. We discussed the current IT infrastructure and modernization efforts, local IT development practices, and user involvement and communication with headquarters. We collected supporting documents about the Coast Guard's IT structure, IT management functions, current initiatives, and improvement initiatives.

We conducted audit fieldwork from November 2010 to February 2011 at Coast Guard headquarters units in Washington, DC; Kearneysville, WV; and Norfolk, VA. We conducted additional

audit fieldwork at Coast Guard district and sector units in Miami and Key West, FL; New Orleans, LA; Alameda, CA; Seattle, WA; Boston, MA; and Cleveland, OH. We also observed capabilities on board the Coast Guard cutters *Key Biscayne* and *Waesche*, as well as in Maritime Information Fusion Centers for both the Atlantic and Pacific areas.

We conducted this performance audit between November 2010 and June 2011 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.

The principal OIG points of contact for this audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, and Richard Harsche, Director of Information Management. Major OIG contributors to the audit are identified in appendix C.

Appendix B
Management Comments to the Draft Report

U.S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

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

7501

AUG 15 2011

MEMORANDUM

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

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

To: Frank Deffer
Assistant Inspector General
Information Technology Audits

Subj: DHS OIG REPORT ON COAST GUARD HAS TAKEN STEPS TO STRENGTHEN INFORMATION TECHNOLOGY MANAGEMENT, BUT CHALLENGES REMAIN

Ref: (a) DHS OIG Draft Report dated May 20, 2011

1. This memorandum transmits the Coast Guard's response to the findings and recommendations identified in reference (a).

2. 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

Copy: Richard Harsche, Division Director
Steven Staats, Audit Manager
Craig Adelman, Auditor
Anna Hamlin, Auditor
Thea Calder, Auditor
Danny McGrath, Auditor

UNITED STATES COAST GUARD RESPONSE TO
DHS OFFICE OF INSPECTOR GENERAL'S
DRAFT REPORT OF MAY 20, 2011

TITLE: "COAST GUARD HAS TAKEN STEPS TO STRENGTHEN INFORMATION TECHNOLOGY MANAGEMENT, BUT CHALLENGES REMAIN"

COAST GUARD'S GENERAL COMMENTS ON DHS OIG FINDINGS:

The Coast Guard generally concurs with the OIG's recommendations and appreciates the opportunity to comment on the draft report. The following corrective actions are being taken to address the recommendations.

COAST GUARD RESPONSES TO DHS OIG RECOMMENDATIONS:

Recommendation #1: We recommend that the Coast Guard Chief of Staff complete the transition of IT personnel and oversight of field IT spending under the CIO.

Concur. The Coast Guard anticipates this task will take time to implement due to the necessity to involve senior Coast Guard leadership in the transition plans for IT personnel and oversight of field IT spending. Upon satisfactory resolution of these issues, the Coast Guard will be better positioned to prepare a Plan of Action and Milestones to complete the transition.

Recommendation #2: We recommend that the Coast Guard Chief Information Officer develop a plan of action and milestones to complete the expansion of broadband communication to the fleet to improve underway connectivity.

Concur. The Coast Guard is in the process of recapitalizing all of the INMARSAT Standard B (STD-B) systems used by the large cutter fleet for underway connectivity to the Coast Guard's data network (CGONE), SIPRNET, and the Internet. Currently, on the WMSL, WHEC, 270' WMEC, POLAR STAR, HEALY, and EAGLE cutters a combination of Ku-Band (which offers higher bandwidth connectivity in many parts of the world) and Fleet Broadband (provides worldwide coverage) systems exist. Our current project plan projection has the C4IT Service Center completing all of the STD-B systems replaced by the combination of Ku and Fleet Broadband by June 2013. This recapitalization will provide at least a 400% improvement in throughput for underway cutters, but can provide up to 15 times more bandwidth if the mission requires it, allowing them improved access to mission-critical applications while underway.

Recommendation #3: We recommend that the Coast Guard Chief Information Officer develop a plan to address the need for near real-time tracking requirements.

Concur: The Coast Guard will continue the testing and implementation of the NAIS permanent system, which will extend receive coverage to 50 nautical miles and add channel management and transmit capabilities to 24 nautical miles. This system provides near real-time data, which will be displayed in a variety of Coast Guard and DHS applications.

Recommendation #4: We recommend that the Coast Guard Chief Information Officer implement a plan to ensure system redundancy to meet availability requirements for Rescue 21 (R21).

Concur: The Coast Guard has been working with the DHS OneNet organization to reduce network outage impacts to the system's performance. The Coast Guard has procured and deployed Very Small Aperture Terminal (VSAT) satellite system at sites with problematic network connections and plans to expand this or a similar network backup capability to 100% of the R21 remote sites. The Coast Guard will continue the procurement and deployment of the VSAT satellite system, as needed, at sites with problematic network connections to ensure 100% back-up capabilities for these remote R21 sites.

Recommendation #5: We recommend that the Coast Guard Chief Information Officer implement a strategy to improve ease of use and availability of the financial systems.

Concur: The Coast Guard is continuing to develop plans to optimize the financial, procurement, and asset management environments for improving financial transparency.

Recommendation #6: We recommend that the Coast Guard Chief Information Officer ensure that new tools, such as WatchKeeper, address command center requirements for improved integration.

Concur: The Coast Guard is using WatchKeeper and another new tool, Mission Asset Scheduling Interface, to integrate data input, retrieval, and display in the command center. There are also ongoing evaluations to determine the appropriate single sensor management system and geographic information system (GIS) for enterprise use.

Information Management Division

Richard Harsche, Division Director
Steven Staats, Audit Manager
Craig Adelman, Auditor
Anna Hamlin, Auditor
Thea Calder, Auditor
Danny McGrath, Auditor
Bridget Glazier, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
USCG, Commandant
USCG, Vice Commandant
USCG, Chief of Staff
USCG, Chief Information Officer
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Director of Local Affairs, Office of Intergovernmental Affairs
USCG Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

• Call our Hotline at 1-800-323-8603;

• Fax the complaint directly to us at (202) 254-4292;

• Email us at DHSOIGHOTLINE@dhs.gov; or

• Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

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