DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improvements Needed in the U. S. Coast Guard's Acquisition and Implementation of Deepwater Information Technology Systems

Office of Information Technology

OIG-06-55 August 2006

Office of Inspector General

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

Homeland Security

August 11, 2006

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, effectiveness, and efficiency within the department.

This report assesses the development and implementation of information technology (IT) systems to support the U.S. Coast Guard's Integrated Deepwater System program. It is based on interviews with employees and officials at Coast Guard headquarters and the Maritime Domain Awareness Center as well as other relevant agency facilities, vessels, and contractor organizations 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. It is our hope that 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.

Richard L. Skinner
Inspector General

Contents/Abbreviations

Appendices

Abbreviations

C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
COMOPTEVFOR	Commander, Operational Test and Evaluation Force
DHS	Department of Homeland Security
DITSCAP	Department of Defense Information Assurance and Defense Information Technology Security Certification and Accreditation Process
GAO	Government Accountability Office
ICGS	Integrated Coast Guard Systems
IT	Information Technology
LIMS	Logistics Information Management System
OIG	Office of Inspector General
SIPRNET	Secret Internet Protocol Router Network
USCG	United States Coast Guard
USCGC	United States Coast Guard Cutter

Figures

Contents/Abbreviations

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

Declining readiness of "Deepwater" assets, including aircraft and cutters of various sizes, has hindered the Coast Guard's effectiveness in accomplishing its homeland security, law enforcement, and regulatory missions. To meet the demand for improved communications, interoperability, and maritime security in today's environment, the Coast Guard has embarked on an estimated 20-year, $20 billion acquisition to modernize and strengthen its aging Deepwater fleet.

We audited the Coast Guard's efforts to design and implement command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems to support the Integrated Deepwater System program. As a result of our audit, we determined that the Coast Guard's efforts to develop its Deepwater C4ISR systems could be improved. Although Coast Guard officials are involved in high-level Deepwater IT requirements definition processes, they have limited influence over contractor decisions toward meeting these requirements. A lack of discipline in requirements change management processes provides little assurance that the requirements remain up-to-date or effective in meeting program goals. Certification and accreditation of Deepwater C4ISR equipment has been difficult to achieve, placing systems security and operations at risk. Further, although the Deepwater program has established IT testing procedures, the contractor has not followed them consistently to ensure that C4ISR systems and the assets on which they are installed perform effectively.

Additionally, the Coast Guard faces several challenges to implementing effectively its Deepwater C4ISR systems. Due to limited oversight as well as unclear contract requirements, the agency cannot ensure that the contractor is making the best decisions toward accomplishing Deepwater IT goals. Insufficient C4ISR funding has restricted accomplishing the "system-of-systems" objectives that are considered fundamental to Deepwater asset interoperability. Inadequate training and guidance hinder users from realizing the full potential of the C4ISR upgrades. Instituting effective mechanisms for maintaining C4ISR equipment have been equally challenging.

Background

According to the *Homeland Security Act of 2002*, the U.S. Coast Guard's eleven missions cover both homeland and non-homeland security matters.[1] Homeland security missions include ensuring security of ports, waterways, and coasts; defense readiness; drug and migrant interdiction; and other law enforcement duties. Non-homeland security missions include maintaining marine safety; coordinating search and rescue; providing aids to navigation; promoting marine resources and protection; and, overseeing ice removal operations.

To accomplish its deepwater missions, the Coast Guard maintains a variety of assets, including 186 aircraft and 88 cutters of various sizes, capable of sustaining operations 50 miles offshore in severe maritime conditions. These assets must be available long-term, 24 hours a day, everyday, and everywhere that the Coast Guard's humanitarian, law-enforcement, national security, maritime safety, or military presence is needed. Typically, however, the assets have been unavailable and lacked the capabilities necessary to perform traditional and homeland security missions effectively. The assets are experiencing declining readiness due to worn out equipment; their lack of essential speed, interoperability, and sensor and communications capabilities severely limits overall mission effectiveness and efficiency.

In the mid-1990s, the Coast Guard began planning a recapitalization program to replace or modernize these aging and technologically obsolete deepwater-capable assets. The primary objectives of the recapitalization program were to maximize operational effectiveness and minimize total ownership costs while satisfying the needs of Coast Guard customers. Customers included the operational commanders, aircraft pilots, cutter crews, maintenance personnel, and others who use the assets.

This earlier recapitalization effort formed the basis for the Coast Guard's Integrated Deepwater Systems program. Established in 2002, the "Deepwater" acquisition program is estimated to take between 20 and 25 years and cost $19 to $24 billion to complete. The Coast Guard awarded the Deepwater contract to a prime contractor, Integrated Coast Guard Systems (ICGS), a joint venture between Lockheed Martin and Northrop Grumman Ship Systems. The prime contractor identified the assets in need of modernization and is using tiers of subcontractors to design and build new assets. (See Figure 1.) The Deepwater program is not only replacing old ships and aircraft, but is offering an integrated approach to upgrading other

[1] Public Law 107-296, November 25, 2002.

existing assets with improved C4ISR equipment and innovative logistics support systems, too.

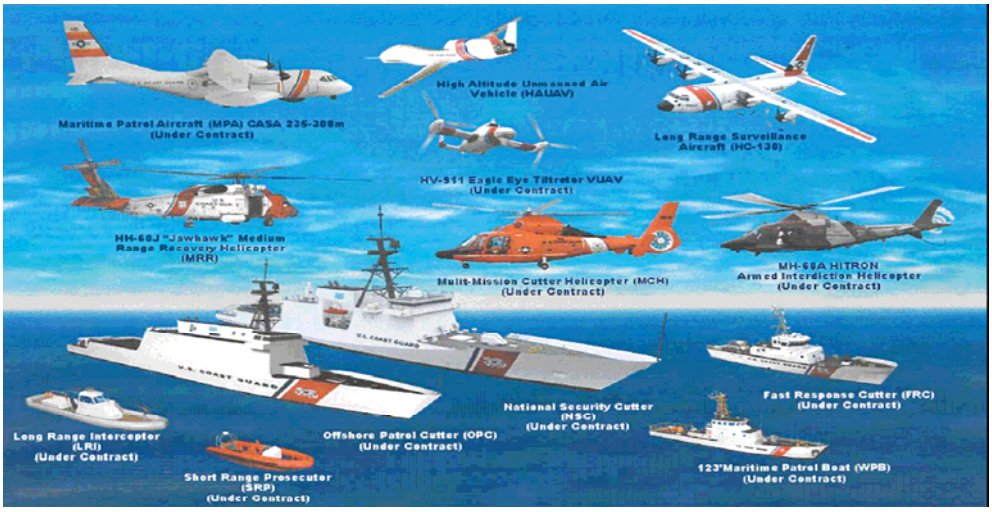

Figure 1: Ships and Aircraft Included in the Deepwater Program

The Deepwater program consists of five domains:

- **Surface**—consists of updating legacy assets and building new classes of cutters, such as the National Security Cutter, the Offshore Patrol Cutter, and the Fast Response Cutter. These newer, more seaworthy cutters will include reconfigurable spaces that can be tailored for specific missions.
- **Air**—consists of modernizing aircraft and building a comprehensive, long-term aviation force, including maritime patrol aircraft, unmanned aerial vehicles, and high-altitude endurance unmanned aerial vehicles.
- **C4ISR**—consists of modernizing the Coast Guard's command, control, communications, computers, intelligence, surveillance, and reconnaissance systems to promote seamless communications between assets.
- **Logistics**—comprised of the Integrated Logistics Support System, which is a requirements-driven, performance-based approach to integrating the support processes and capability needed to improve operational effectiveness and reduce total ownership costs in each of the preceding three domains.
- **System-of-Systems**—serves as an umbrella domain, encompassing the other four domains to ensure that all assets can interoperate. As the focal part of the Deepwater program, this domain was created to provide central management of program performance, cost, schedule, and risk.

The Deepwater C4ISR platform is a fundamental building block to improving maritime domain awareness by focusing on the information needs of operators and decision makers. The C4ISR program manager oversees all facets of C4ISR implementation including resource management, strategic planning, and organizational performance measurement activities and processes. The C4ISR platform is designed to ensure seamless interoperability among all Coast Guard units and DHS components as well as with other federal agencies, especially the Navy. Modernization efforts to date demonstrate that legacy assets upgraded with new C4ISR systems enable earlier awareness, coordination, and response to possible threats by gathering and fusing terrorist-related information and analysis and increasing communications.

When Deepwater is fully implemented, the Coast Guard's assets will no longer operate as independent platforms with only limited awareness of their surroundings in the maritime domain. Instead, the assets will have improved capabilities to receive information from a wide array of mission-capable platforms and sensors. They will share a common operating picture as part of a network-centric force, operating in tandem with other cutters, boats, manned aircraft, and unmanned aerial vehicles. (See Figure 2.)

Figure 2: Proposed Seamless Interoperability Among Deepwater Assets

The C4ISR implementation plan outlines a strategy for upgrading shore, air, and surface assets in the following phases.

- **Increment one**, implemented from 2002 to 2005, included satellite voice and data communication capability, Coast Guard command and control systems, and law enforcement radios added to surface and shore assets. Coast Guard command and control systems include the following

functions: sensor and systems interfaces; operator support and display; mission support; track management; and command and control support services.

- **Increment two**, to be implemented from 2004 to 2007, includes adding C4ISR equipment, radios, and radar to multi-mission cutter helicopters, unveiling the first maritime patrol aircraft, and adding Coast Guard command and control systems upgrades to international ice patrol shore assets.

- **Increment three**, beginning in 2007, includes implementing additional Coast Guard command and control systems as well as planning a hardware technology refresh.

- **Increment four**, scheduled for 2009 to 2012, includes strategic and operational planning for Coast Guard command and control systems, high frequency surface wave radar integration, mission support, and data query.

In recent years, the Government Accountability Office (GAO) has evaluated Deepwater program efforts, citing management oversight problems in each of its reports. In March 2004, GAO reported that the integrated product teams charged with overseeing the system integrator had struggled to effectively collaborate and accomplish their missions.[2] Specifically, GAO reported that the Coast Guard had not yet begun to measure the system integrator's performance on the three overarching goals of the Deepwater program: operational effectiveness, total ownership cost, and customer satisfaction. GAO recommended that the Coast Guard take the necessary steps to make the Deepwater integrated product teams effective, improve contractor accountability, and review the human capital plan to ensure adequate staffing.

Also, in June 2004, GAO reported that Deepwater program officials had not updated the initial 2002 integrated acquisition schedule.[3] During its review, GAO attempted to identify a current acquisition status and found that a number of selected Deepwater assets had experienced delays and were at risk of being delivered later than anticipated. Therefore, GAO recommended that the DHS Secretary require the Coast Guard to update its integrated acquisition schedule as part of its FY 2006 budget submission. Further, in a 2005 report,

[2] *Contract Management: Coast Guard's Deepwater Program Needs Increased Attention to Management and Contractor Oversight,* U.S. Government Accountability Office (GAO-04-380, March 2004).
[3] *Deepwater Program Acquisition Schedule Update Needed,* U.S. Government Accountability Office (GAO-04-695, June 2004).

GAO said the Coast Guard had not captured, to the full extent possible, the decline in the condition of its assets. [4]

More recently, in April 2006 GAO reported that the Coast Guard has made progress in addressing some of the management oversight issues identified in previous reports.[5] Specifically, GAO noted that the Coast Guard has provided additional guidance, training, criteria, and measures to improve its program management assessments of the system integrator's performance. Additionally, the Coast Guard has changed award fee measures to better hold the system integrator accountable for ensuring effective integrated product teams. Award fee criteria have been expanded to incorporate administration, management commitment, collaboration, training, and empowerment of these teams. GAO reported that the Coast Guard has taken steps to implement the recommendations, however it is too early to determine the effectiveness of these efforts.

As part of our ongoing responsibility to assess the efficiency and effectiveness of departmental programs and operations, we conducted an audit of the Coast Guard's Deepwater information technology. The objectives of our audit were to evaluate the effectiveness of Coast Guard efforts to identify C4ISR systems requirements, and to determine how well these systems are being implemented to support the Deepwater program. The scope and methodology of this audit are discussed in Appendix A.

Results of Audit

System Development Approach Could Be Improved

The Coast Guard's efforts to develop its Deepwater C4ISR systems could be improved. Although agency officials are involved in high-level Deepwater requirements definition processes, they have limited influence over the decisions that the contractor makes toward meeting those IT requirements. Due to a lack of discipline in adhering to systems requirements change management processes, there is little assurance that the requirements are complete or effective in meeting program goals. Ensuring consistent certification and accreditation of Deepwater C4ISR equipment has been difficult to achieve, thus placing systems security and capabilities at risk. Further, although the Deepwater program has established procedures for IT

[4] *Preliminary Observations on the Condition of Deepwater Legacy Assets and Acquisition Management Challenges*, U.S. Government Accountability Office (GAO-05-307T, April 20, 2005).
[5] *Changes to Deepwater Plan Appear Sound, and Program Management Has Improved, but Continued Monitoring Is Warranted*, U.S. Government Accountability Office (GAO-06-546, April 2006).

testing, the contractor has not consistently applied these procedures to ensure effective performance of C4ISR systems and the assets on which they are installed.

Requirements Definition Process Not Fully Effective

Office of Management and Budget Circular A-11 establishes policies for planning and managing IT investments to ensure that funds expended achieve intended benefits.[6] Specifically, a supplement to the circular directs agencies to reduce project risk by involving stakeholders in the definition of requirements and the design of IT assets to meet mission needs.[7] While Coast Guard officials are involved in initial requirements definition processes at an operational level, the users have little input into subsequent efforts to identify the Deepwater IT systems needed to meet those requirements. Instead, the contractor has sole responsibility for determining systems functionality at the next level, and outlining the steps toward implementing the systems in line with the functional requirements.

The Coast Guard has a structured process in place to help support Deepwater requirements definition (see Figure 3). The process begins when the Office of Response, considered the Deepwater program sponsor, provides a mission needs statement for approval by senior DHS and Coast Guard management. Deepwater program officials provided the initial mission needs statement for approval in 1996, but subsequently updated it in 2000 and 2005 to address increased homeland security needs since the September 11, 2001, terrorist attacks. The mission needs statement broadly outlines high-level requirements to align the Deepwater program with the department's mission, vision, and strategic goals. After the DHS Deputy Secretary signed the mission needs statement, the Coast Guard was authorized to develop technology to meet its Deepwater program requirements.

Deepwater officials subsequently divided the overarching program requirements into various functional areas, such as the C4ISR domain. The first step in breaking down Deepwater C4ISR requirements entailed producing a system performance specification document based on the mission needs statement. This system performance specification document, created by Coast Guard officials, discussed the high level operational capabilities that it expects the technology to provide. For example, the command and control system

[6] Circular A-11, Part 7, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, Executive Office of the President, Office of Management and Budget, June 2005.
[7] *Capital Programming Guide*, version 1.0, supplement to Circular A-11, Executive Office of the President, Office of Management and Budget, July 1997.

shall provide tools for developing operational mission and crisis action plans to assist in prioritizing and adjusting the use of available assets.

Further, the Deepwater contractor mapped the operational capabilities document to a system requirements specification document that it created, outlining the specific technologies and functions that it planned to provide to meet the contract requirements. Subsequently, the contractor divided its system requirements specification document into several C4ISR "asset performance specifications documents," defining the hardware and software requirements for each Deepwater asset (e.g., ship or aircraft). Working through this structured process, the Coast Guard has been able to trace its Deepwater program requirements, at least at a high level, back to the department's strategic homeland security goals.

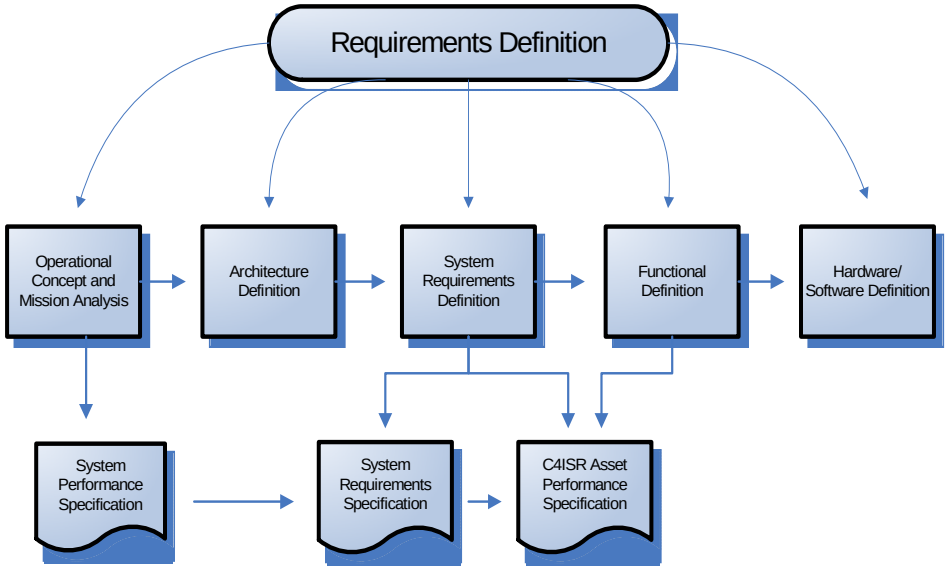

Figure 3: Requirements Definition Process

However, beyond this process, the contractor has principal authority to further define system requirements and the steps needed to meet those requirements. Per the Deepwater contract, many IT requirements documents do not require prior Coast Guard approval. For example, according to one contract official, the contractor generally gives the Coast Guard 30 days to review documents. However, because of a shortage of personnel to conduct the document reviews, the agency has difficulty responding within that time frame. By the time that the Coast Guard is able to review the documents, the contractor has moved ahead with its plans to keep on schedule. One Coast Guard official stated that the agency must then either accept the work that the contractor has performed or submit a change request, which may require additional funding.

Initially, when the contractor presented the C4ISR increment one test and evaluation program plan to the Coast Guard, agency officials identified deficiencies with the plan and did not accept it. These deficiencies included inadequate explanation of C4ISR increment one domain level testing, no test schedule, and inadequate requirements traceability to the test events. After the contractor submitted the test and evaluation program plan a second time with revisions, Coast Guard officials were forced to accept the document due to schedule pressures. Nonetheless, Coast Guard officials commented that several corrections still needed to be made to the document, but they were minor and likely would not impinge on program areas such as scheduling or performance specification completion.

Per contract agreements, the contractor also controls the integrated product teams formed to provide cross-representational input to Deepwater program requirements. These teams serve as a venue for discussing specific C4ISR issues and technologies. Although the teams are comprised of contractors and Deepwater program and operational staff, the ultimate authority for the teams rests with the chairperson who is a contractor. As such, the contractor drives the discussions regarding fundamental program requirements and controls the technology change decisions forwarded for implementation. In response to our draft report, Coast Guard officials noted that since 2005 they have taken steps to address these issues concerning integrated product team involvement in the requirements definition process. Specifically, they said that Coast Guard representatives now participate on all four integrated product teams to help formulate contractor decisions toward meeting IT requirements. Coast Guard representatives also participate in Technical Solution Reviews hosted by the contractor.

Lack of Discipline in Requirements Change Management

According to federal guidelines, IT architectures should be used to guide changes for new and operational systems.[8] Failure to follow effective change management or configuration management processes can lead to systems availability problems. Specifically, the Gartner Group, a leading provider of IT industry research and analysis, reports that an average of 80 percent of unplanned systems downtime is caused by people and process issues, including poor change management practices.[9] Enterprises that have strong change management practices typically have the highest levels of systems availability.

[8] Memorandum 97-16, *Information Technology Architectures*, Executive Office of the President, Office of Management and Budget, June 18, 1997.
[9] *NSM: Often the Weakest Link in Business Availability*, Gartner, Inc., July 3, 2001.

The Deepwater program faces a constant challenge in ensuring adherence to its process for submitting, reviewing, approving, and implementing changes to systems requirements to ensure that they remain up-to-date and effective in meeting program goals. There are at least two types of systems requirements changes—those affecting high-level operational requirements and those affecting functional capabilities. Deepwater integrated product teams or Coast Guard officials responsible for managing the C4ISR domain can only recommend changes to functional requirements. A Deepwater program sponsor is required to initiate all changes to operational requirements, which then must be approved by the Coast Guard's acquisition executive for further consideration.

In either case, the requirements changes must be cleared through the contractor's peer review process and then presented for discussion at an engineering technical review. Following the engineering technical review, the changes are forwarded to the Deepwater Specification Change Review Implementation Baseline and Evaluation board, where the contractor and the Coast Guard discuss the new or revised requirements. Upon approving the requirements change, the board also determines the associated cost and submits the change request to a joint change control board for review; the C4ISR asset piece back document is then modified. If the board disapproves the requirements change, the request is placed in a holding file for discussion at a later date.

A number of Coast Guard officials stated that this requirements change process is not always followed. One official stated that some people circumvent the process by requesting changes directly of the contractor staff on site. For example, one Deepwater C4ISR official told us that if changes are needed to the National Security Cutter being built in Pascagoula, Mississippi, the Coast Guard staff there will talk directly to the contractors on site to obtain the changes rather than seek approval through the program office. A C4ISR official expressed concern at sometimes not learning about the changes made by the surface domain until the contractor requests payment for the deviations, which can lead to potential cost and schedule overruns without Coast Guard management's awareness.

Several critically needed changes to the C4ISR approach and requirements have been overlooked. A number of Coast Guard officials stated that some C4ISR requirements, which were identified after September 11, 2001, have not been introduced into the Deepwater program. For example, the contractor continues to focus on the original requirement to use the automatic identification system to ensure safety of life at sea rather than the exchange of sensitive but unclassified tactical information, as more recently directed by the Coast Guard. Because of the delay in implementing such requirements

changes, the Coast Guard may not have what it needs to meet its post 9-11 homeland security missions.

Similarly, one Coast Guard official stated that requirements generated from a Deepwater program performance gap analysis, directed by the Commandant in 2003, have not been implemented. The report resulting from the gap analysis states that, although the Deepwater concept of operations stresses interoperability, it does not outline plans for ensuring that both technical and operational interoperability requirements are met. For example, technical interoperability requirements for items such as sensors, radios, and radar are covered; however, there are few clear examples of how the various Deepwater assets equipped with the C4ISR systems will work together. This lack of clarity can hinder seamless interoperability between Deepwater systems and other key initiatives, such as the Coast Guard's "Rescue 21" command, control, and communications system. Additionally, the interoperability discussion in the Deepwater concept of operations is Coast Guard-centric and does not address interoperability with other DHS components or the Department of Defense.

At times, Coast Guard policy modifications can necessitate involuntary changes to Deepwater C4ISR systems design to ensure continued interoperability across agency assets. The Coast Guard decided to implement the Automatic Messaging Handling System at its Communications Area Master Stations instead of adopting a messaging system that the Deepwater program was in the process of acquiring. As a result, the Deepwater program had to switch to using the same system so that its assets could continue to communicate with other Coast Guard components. This change may affect not only the design of the Deepwater C4ISR system but the contract cost and schedule as well.

Systems Certification and Accreditation Issues

Federal guidelines require that agencies establish processes to authorize and ensure the security of the IT systems that they implement.[10] As part of these processes, IT systems must undergo certification and accreditation—a risk-management framework for meeting federal information security requirements.[11] Certification and accreditation is comprised of four distinct phases: systems initiation, security certification, security accreditation, and continuous monitoring. Each phase in the process consists of a set of well-defined tasks including testing, inspections, and documented agreements

[10] *Federal Information Security Management Act of 2002* (FISMA), Public Law 107-347, Title III, December 17, 2002.
[11] *Guide for the Security Certification and Accreditation of Federal Information Systems*, National Institute of Standards and Technology, Special Publication 800-37, May 2004.

among responsible authorities. Three types of accreditation decisions can be rendered at the end of the process: authorization to operate, interim authorization to operate, or denial of authorization to operate. The Deepwater contractor is required to build, test, and implement computer systems in compliance with the Department of Defense Information Assurance and Defense Information Technology Security Certification and Accreditation Process (DITSCAP) to ensure that they achieve authorization to operate.

However, achieving such authorization has proven difficult for Deepwater C4ISR systems. For example, the contractor is having problems achieving authorization to operate the new Coast Guard command and control system being installed at the District 7 Miami shore site. The system underwent several vulnerability scans and failed because it was not built in accordance with DITSCAP guidelines. Because of the unmitigated vulnerabilities, Deepwater program officials have not been able to present the system to the Coast Guard's Secret Internet Protocol Router Network (SIPRNET) Management Office and receive authorization to operate. The system must achieve a minimal, accepted level of risk before it can be approved and put online. The delay in making the new C4ISR suite operational has had a ripple effect, delaying system implementation at other shore sites and on assets.

Similarly, the Deepwater program initially experienced problems in certifying and accrediting the command and control system that the Coast Guard uses on its 123-foot patrol boats. A version of the system received authorization to operate while the contractor worked to address the minor vulnerabilities identified. However, despite creating additional system versions to try to mitigate the vulnerabilities, the contractor was not successful and therefore these other versions could not receive final authorization to operate. In April 2006, the SIPRNET Management Office informed Deepwater program managers that, unless the vulnerabilities were addressed within 45 days, access to SIPRNET would be revoked. To assist the contractor in meeting the deadline, the Coast Guard provided a "best practice" software development process that other agency units use to meet DITSCAP requirements for deploying their systems. The contractor aligned its software development approach with these best practice guidelines and, in May 2006, achieved authorization to operate a new version of the command and control system on its 123-foot patrol boats.

This command and control system installed on the 123-foot patrol boats constitutes the baseline for the core C4ISR system currently being deployed at Coast Guard shore facilities. This core C4ISR system, in turn, constitutes part of a larger C4ISR system, which will be installed on other Deepwater assets, such as the National Security Cutter. Because it has many components, successfully accomplishing certification and accreditation for the National

Security Cutter's C4ISR equipment will be especially difficult. As such, the contractor expects to apply the lessons learned in achieving certification and accreditation for the command and control system to its broader Deepwater system deployment efforts. A number of Coast Guard officials emphasized the need to successfully certify and accredit the core system to avoid the risk of losing SIPRNET capability, which is critical for all of Deepwater's 123-foot patrol boats and legacy cutters. Such secure connectivity allows Deepwater assets to coordinate missions quietly without radio chatter and sneak up on their targets without revealing their positions.

Inadequate Systems Testing

According to federal regulations, agencies are responsible for ensuring effective and efficient operation of IT equipment.[12] This entails proving that new systems function properly in a "production-like" test environment and contain needed safeguards.

While the Deepwater program has established a process for systems testing, a number of Coast Guard officials believe that this process could be improved. The contractor uses the four following methods to test Deepwater C4ISR systems:

- Analysis, to determine if the system meets performance requirements.
- Inspection, to verify with the five human senses that the system has been assembled correctly.
- Demonstration and follow-up, to ensure that the system is working correctly.
- Final testing, to verify functionality with real life data analysis.

The contractor may not use all four procedures to test each system; rather, the contractor has the authority to determine which method or combination of methods will be used. In general, the testing completed by the contractor takes place at the Maritime Domain Awareness Center in Moorestown, New Jersey and its supporting laboratories.

Our review disclosed problems with the simulation equipment that the contractor uses at the Maritime Domain Awareness Center to perform vulnerability scans on C4ISR systems during the demonstration and final testing phases. Vulnerability scans using the simulation equipment are to help ensure that the C4ISR systems they replicate are compliant with applicable security standards. However, several simulator shortcomings may hinder

[12] Office of Management and Budget Circular A-130, *Transmittal Memorandum #4, Management of Federal Information Resources*, November 28, 2000.

achievement of this objective. Specifically, Coast Guard officials told us that the simulation equipment used for the vulnerability scans has difficulty calculating how C4ISR systems work in real situations on cutters or at shore sites; the simulators therefore may produce inaccurate results. Further, because the contractor has not compared simulator performance to that of real C4ISR systems, discrepancies may result when the C4ISR systems are deployed to new assets or shore sites. Additionally, the simulation equipment has not undergone certification and accreditation to help ensure that it mimics the true C4ISR environment. Successfully certifying and accrediting the simulation equipment can increase the probability that the real C4ISR systems will function properly. While Coast Guard officials recognize the potential benefits to certifying and accrediting simulators, the contractor has resisted, asserting that to do so would require additional funding.

Further, although the Navy's Commander, Operational Test and Evaluation Force (COMOPTEVFOR) in Norfolk, Virginia is supposed to play a significant role in completing C4ISR testing, its participation in test activities to date has been limited. This is an independent group responsible for reporting to Deepwater sponsors on the operational capabilities of the C4ISR systems implemented by the contractor. Ideally, COMOPTEVFOR should have participated in the initial phases of Deepwater C4ISR development to help identify possible "faults or concerns" that could affect the operational system. Instead, the contractor provided this group access to the C4ISR systems only after they were installed on the completed 123-foot patrol boats. At that point, it completed operational testing of the systems on the 123s, but not on the legacy cutters that also had received portions of the C4ISR upgrades. The ensuing report from these operational tests noted problems with C4ISR equipment installation, training, and integration with other off-the-shelf command and control systems already installed on the 123-foot patrol boats. Also, the report indicated that, with the exception of the SIPRNET, the C4ISR systems did not operate as promised to meet Coast Guard requirements.

Recommendations

We recommend that the Commandant, U.S. Coast Guard, direct the Deepwater Program Executive Officer to:

1. Increase agency input and oversight of the requirements definition process to ensure the contractor activities meet program goals and objectives.
2. Clearly define and communicate system requirements change management processes to ensure they are consistently used to identify,

evaluate, and apply changes as appropriate, to Deepwater C4ISR requirements.

3. Ensure that, in line with federal guidelines, the contractor takes steps to mitigate security vulnerabilities that have hindered achievement of C4ISR system certification and accreditation.
4. Address shortcomings with simulation equipment and provide the access needed to support independent test and evaluation of C4ISR systems and equipment to ensure that they operate efficiently and securely.

Deepwater Systems Implementation Challenges

The Coast Guard faces a number of challenges to implementing effectively its Deepwater C4ISR systems. Due to limited oversight, a lack of clarity regarding contract requirements, and limited input into selection decisions, the agency cannot ensure that the contractor is fully meeting its Deepwater IT needs. Insufficient funding of C4ISR and engineering components has restricted achievement of integrated "system-of-systems" objectives—the linchpin of the Deepwater program. Inconsistent training, inadequate instructors, and a lack of reference materials hinder users from realizing the full potential of the C4ISR upgrades. And, ensuring effective service and support for C4ISR systems and users have been equally challenging.

Contract Management Structure Limits Oversight and Control

Although the performance-based Deepwater contract has the potential to increase contractor flexibility and reduce costs, it has several drawbacks as well. Specifically, due to a lack of funding and experience with performance-based acquisitions, the Coast Guard has not allocated sufficient resources to effectively oversee Deepwater contractor activities. Due to a lack of clarity in the contract terminology, there is some confusion about contractor responsibilities for producing the C4ISR systems, hindering timely and effective accomplishment of Deepwater program goals. The contractor has considerable autonomy in making Deepwater IT selections, which some believe are not always in the best interest of the agency, too.

Deepwater Contract Structure

The federal government requires that agencies maximize use of performance-based contracts to acquire services or products. The intent is for agencies to describe their needs in terms of what is to be achieved rather than how it is to be done, giving the contractor flexibility in the processes and proposed solutions toward meeting agency mission needs—and thereby decreasing the

total cost of program ownership. Further, interagency guidance on performance-based acquisitions states that the contracts should be structured in such a manner as to ensure meaningful agency oversight of contractor progress toward meeting requirements, milestones, and program goals.[13] Adequate federal resources must be applied effectively to carry out these oversight responsibilities. Statements of work pursuant to the performance-based contract also should be clearly written to ensure that contractor activities and products deliver intended benefits.

As previously discussed, in 2002 the Coast Guard awarded a performance-based contract to accomplish its Deepwater program. The Coast Guard awarded ICGS the role of prime contractor and overall systems integrator, with responsibility for designing, deploying, and integrating all of the air, surface, and shore assets and technologies needed for maritime domain awareness. Essentially, ICGS is a joint venture between Lockheed Martin and Northrop Grumman Ship Systems, with each company serving as first-tier subcontractors for the Deepwater program. As such, Lockheed Martin and Northrop Grumman Ship Systems can either provide Deepwater assets and systems themselves, or award this responsibility to second-tier subcontractors. Figure 4 illustrates the contractor relationships. (See Figure 4.)

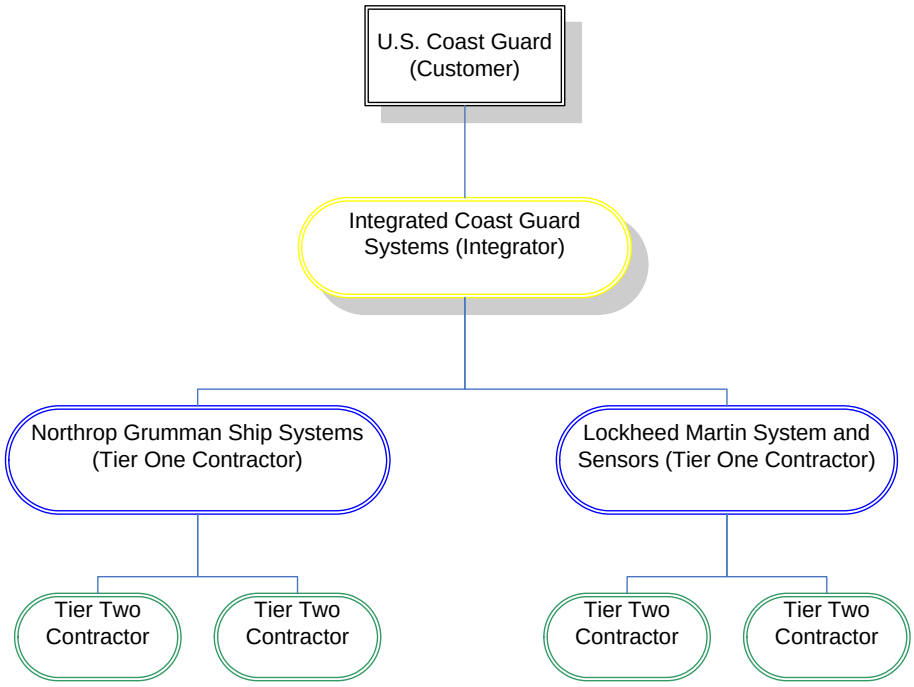

Figure 4: Deepwater Contractor Relationships

[13] *Seven Steps to Performance-Based Services Acquisition,* An Interagency-Industry Partnership in Performance.

To help execute the contract, in December 2002 the Coast Guard and ICGS signed a partnering agreement, which outlines their respective responsibilities and how they will work together to carry out the program. The agreement states that the Coast Guard is responsible for managing operational requirements; providing a uniform understanding of agency needs, perspectives, and constraints; responding to mission demand and environmental changes; ensuring contract oversight; and, operating the Integrated Deepwater System. Accordingly, the Coast Guard has an essential role to play in overseeing program management and ensuring that contractor activities are aligned with program goals and objectives. Conversely, ICGS is responsible for defining, managing, integrating, and constructing Deepwater assets and systems to comprise a single integrated system. As such, the contractor is responsible for providing Deepwater solutions and results, but in keeping with overarching Coast Guard direction. The goals of the partnering agreement include:

- Maximizing operational effectiveness and minimizing costs.
- Delivering assets and systems in accordance with prescribed cost, schedule, and technical performance objectives.
- Ensuring a collaborative work environment.
- Communicating openly and honestly to avoid mistakes and surprises.
- Managing risks by anticipating and resolving problems promptly.
- Resolving issues before they escalate.

Contract Management Staff

Due to funding limitations and a lack of experience with performance-based acquisitions, the Coast Guard has not allocated sufficient resources to effectively carry out its responsibility for overseeing the Deepwater contract. Coast Guard officials at both the Systems Integration Program Office and the Maritime Domain Awareness Center told us of the need for additional Coast Guard personnel to provide agency perspectives and oversight by attending meetings on Deepwater program management, requirements definition, and systems design issues. Also, officials said that additional Coast Guard resources are needed to review the large number of contractor plans and documents to ensure that contract requirements are being met. For example, one official estimated that the ratio of Deepwater contractors to Coast Guard program management personnel at the Maritime Domain Awareness Center—a primary contractor facility responsible for system development testing—is about 20 to 1. Based on years of experience in helping to oversee contractor activities at the center, this official said that a ratio of 10 to 1 would be more appropriate.

Staff currently assigned to Deepwater program management are overworked and pulled in many directions to provide coverage. Where staff must act in a program oversight capacity in addition to carrying out their direct responsibilities, their workloads are overwhelming. Program oversight activities include reviewing requirements, developing statements of work, overseeing systems installation, conducting training, providing technical feedback, and attending meetings at the program office in Washington, DC as well as the contractor's facility in Moorestown, New Jersey. For example, one Coast Guard official whom we interviewed serves as a liaison between the two locations. This official must travel back and forth to carry out his responsibilities for establishing systems policy and direction, promoting awareness of program progress, and communicating issues related to Deepwater requirements. A program management official questioned the impact that such thinly stretched oversight personnel are having on the Deepwater program. This official surmised that essential oversight activities are likely being overlooked, posing potential risks to successful contract accomplishment.

Further, the prime contractor is not adequately staffed to ensure that the subcontractors are fulfilling their obligations. For example, one Coast Guard official said that the system integrator has only two individuals working on program management issues for the entire C4ISR domain: A C4ISR associate program manager responsible for increment one shore assets, and a deputy associate program manager responsible for increment one surface and air assets. Together, these officials are responsible for overseeing the contractor's costs, performance, and schedule and notifying the Coast Guard if there are any problems. However, given the myriad issues related to Deepwater C4ISR, realistically they must focus on addressing the high-priority items at the expense of more minor concerns. This staffing limitation frustrates Coast Guard program management officials, who sometimes have to wait months for issues to be addressed.

Similarly, the number of subcontractors assigned to carry out specific contract activities has not always been adequate. For example, there are only three subcontractor representatives located at the Maritime Domain Awareness Center with adequate expertise to ensure systems certification and accreditation. A Coast Guard official we interviewed believes that the number of personnel should instead be between 10 and 15 to cover the wide-ranging C4ISR systems that need review and testing. Another official said that this lack of technical personnel has contributed to delays in implementing the command and control system for District 7.

Officials said that they believe the contractors are not adequately fulfilling their duties because Coast Guard personnel must fill-in and provide support.

This workload places additional strain on the already limited number of Coast Guard program management and oversight personnel. Officials told us that the Deepwater program would be adequately resourced if the prime contractor were not acting as both a systems integrator for the overall program, as well as a subcontractor with hands-on responsibilities for designing, developing, and implementing assets and systems. They said that this arrangement taxes the Coast Guard's resources needed to provide requirements review and systems testing, training, and support.

The Coast Guard has recently taken steps to try to address the lack of Deepwater contract management resources. Specifically, in FY 2005, program management requested that each program domain examine the 2002 Deepwater Human Capital Plan and determine whether additional staff was needed. Accordingly, C4ISR program managers requested an additional 28 government and contract staff resources to help with contractor oversight and other activities such as system certification and accreditation. In response, however, the C4ISR component only received five additional staff and remains challenged in its ability to adequately oversee the program.

Confusion Concerning Contractor Responsibilities

Due to a lack of clarity in the Deepwater contract and supporting documents, there is some confusion about contractor responsibilities in producing C4ISR systems. In several instances, the Coast Guard and its contractors have tended to interpret the terms of the contract differently, posing hindrances to timely and effective accomplishment of Deepwater program goals. Several Coast Guard officials stated that the contractor does not fully understand the agency's organization and mission because frequent meetings between the contractor and the Coast Guard are required to discuss the meaning of words used in the program documentation.

To illustrate: In November 2003, the Coast Guard provided a letter to the contractor stating that, contrary to the concept of operations, satellite communications plans did not include SIPRNET connectivity for Deepwater cutters operating out-of-hemisphere in ocean regions other than the Atlantic and Pacific. In its written response, the contractor disagreed with this assertion and stated that the level of connectivity it had provided was in keeping with the task order. Further, the contractor stated that the concept of operations did not specify when satellite communications for the out-of-hemisphere cutters would be needed. The contractor nonetheless agreed to identify alternative solutions for leasing additional satellite connectivity for the Coast Guard's out-of-hemisphere cutters. The contractor reiterated, however, that pursuing these alternative solutions was beyond the scope of the task order and requested reimbursement for all additional costs. The Coast

Guard ultimately agreed because it needed the satellite connectivity to communicate and coordinate mission activities with the cutters that were operating out-of-hemisphere. In response to a draft of our report, the Coast Guard noted that the above letter was written several years ago and that there has been tremendous improvement since that time.

Additionally, many of the systems testing and approval problems previously discussed can be attributed to initial difficulty that the Coast Guard had in getting the subcontractor to accept responsibility for certification and accreditation. From the Coast Guard's perspective, the Deepwater contract assigned the subcontractor responsibility for identifying and assessing C4ISR systems vulnerabilities, as well as providing software security updates. However, according to a Coast Guard official, the subcontractor believed that it was only responsible for providing a "certifiable" system that could pass certification and accreditation requirements at a later date. The subcontractor initially asserted that the Coast Guard would incur additional costs if it were to require changes to contractor procedures for developing software as a means of ensuring that the security requirements could be met. However, after a Coast Guard contracting officer provided written guidance in April 2006, the subcontractor was able to provide a certifiable system for the 123-foot patrol boats.

Finally, the Coast Guard has a responsibility to oversee the contractor's processes for accomplishing contract goals and deliverables; however, it has been difficult to get the contractor to provide such a window into its operations. For example, the contractor recently completed a C4ISR operating system scan, which identified security vulnerabilities. The contractor stated that it could not resolve the vulnerabilities without causing the system to lose functionality. When the Coast Guard asked for more details, the contractor resisted, stating that it was not required by the contract to provide such information. In May 2006, however, a Coast Guard official stated that the contractor was working to provide the requested information.

Contractor Decisions May Not Meet Agency Needs

By limiting the Coast Guard's role in determining contractor processes and solutions, the performance-based Deepwater contract is intended to promote contractor flexibility and success toward achieving program goals. However, the contract has a number of drawbacks as well. Specifically, it gives the contractor considerable autonomy in selecting the systems and equipment it believes will fulfill performance objectives outlined in the statement of work. Under ordinary circumstances, this arrangement can prove beneficial. However, officials were concerned that the two parties to the joint venture,

who serve as subcontractors for the program as well, lack the independence needed to make objective decisions in the best interest of the Coast Guard.

In purchasing its Automatic Identification System, for example, the contractor selected a vendor other than the one that the Coast Guard already uses to provide similar functions for its non-deepwater fleet. A Coast Guard official suggested that the decision was based more on the fact that the vendor was under contract than on the superior capabilities or competitive costs of its system. Similarly, the Deepwater contractor selected a brand of radios that may not be interoperable with other brands of radios used by other government agencies. In a recent survey, one Coast Guard official expressed concerns that the Deepwater contractor typically exerts little effort to ensure that the IT products it selects are aligned with the rest of the agency. Using different brands of equipment with different operating procedures and requirements can lead to increased risk that Coast Guard users will not be able to communicate effectively, in addition to causing problems in providing IT training, support, and spare parts in the long-term. Such disparities also create a divide between Deepwater and non-Deepwater assets, making it difficult for Coast Guard personnel to transition from one asset to another without having to be retrained on different equipment.

In its March 2004 report, GAO discussed issues related to the lack of competition and contractor independence in deciding on Deepwater acquisitions.[14] Specifically, it reported that the two subcontractors comprising the joint venture have sole responsibility for determining whether to hold competitions for Deepwater assets or to provide the assets themselves. GAO stated that over 40 percent of the funds obligated to the two subcontractors have remained with those companies or been awarded to their subsidiaries. Further, GAO noted that the Deepwater systems integrator uses a sourcing document developed by one of its subcontractors to guide competition decisions made by the subcontractors. However, this guidance is a philosophy—not a formal process involving specific actions—which encourages competition, but does not require it. GAO concluded that the lack of transparency into significant make or buy decisions, and the government's lack of a mechanism to hold the contractor accountable, raise questions about whether the Coast Guard will be able to control costs. GAO found that as of September 30, 2003, Lockheed Martin planned to retain 42 percent of its obligated dollars and to award 58 percent to second-tier subcontractors. In response to our draft report, the Coast Guard stated that it had hired a contractor to assess the extent of second-tier competition conducted by the prime contractor, as a means of addressing the GAO recommendations. The

[14] GAO-04-380, March 2004.

contractor provided nine suggestions for addressing the GAO recommendations, of which the Coast Guard has implemented eight.

C4ISR and System Engineering Funding

Office of Management and Budget Circular A-130 directs federal agencies to develop information systems that facilitate interoperability across networks of heterogeneous hardware, software, and telecommunications platforms. IT planning to achieve these objectives should be linked to expected program and mission needs, reflect budget constraints, and form the basis for budget requests.

As previously discussed, the Deepwater "system-of-systems" approach is intended to deliver a package of C4ISR systems across all of the program's new or upgraded sea, air, and shore assets. The approach involves enhanced command and control systems as well as a streamlined logistics structure to support a layered defense of major cutters, patrol boats, helicopters, unmanned aerial vehicles, and maritime patrol aircraft—all connected using a single command and control architecture. The C4ISR capabilities comprise a fundamental building block toward providing the interoperability, situational awareness, and communications needed to detect, intercept, and interdict potential threats in the maritime domain. This integrated "mix of forces" solution, including minimal development of assets and, wherever possible, procurement of state-of the-art products and technologies, is a departure from traditional one-for-one asset acquisition programs. Engineering support for all design, test, and production activities is key to ensuring a fully integrated Deepwater system. Engineering teams are responsible for performing the necessary analysis and tradeoffs, recognizing when interface impacts might occur, and taking early action to avoid integration problems.

However, insufficient funding for C4ISR and systems engineering and integration components of the Deepwater program has restricted achievement of the intended "system-of-systems" approach. While Deepwater is an essential acquisition, it faces the same budget realities as other federal agency programs. Specifically, each year the Office of Management and Budget requires that the Coast Guard include full funding for the Deepwater program in its agency-wide capital plan. However, whereas the President's budget request for the C4ISR program in FY 2006 was about $74 million, the Coast Guard only received approximately $44 million—about $30 million less than the amount that the Coast Guard said it needed to achieve its FY 2006 C4ISR objectives.

Due to the reduced level of funding in FY 2006, the Coast Guard has been hindered in accomplishing some C4ISR initiatives as scheduled. For example,

detailed design and development activities for C4ISR increment two have been delayed by at least three months. This, in turn, has resulted in a delay in implementing enhanced maritime domain awareness capabilities across all Deepwater assets by approximately one year. The President has requested approximately $61 million for Deepwater C4ISR in FY 2007.

In conjunction with these C4ISR funding reductions, the systems engineering and integration component responsible for supporting accomplishment of Deepwater "system-of-systems" objectives has been under-funded, too. According to the International Council on Systems Engineering, such expenditures should constitute about 10 to 15 percent of a program's budget. However, Deepwater systems engineering and integration funding has declined each year since the program's inception, from a high of 20 percent of the overall budget in FY 2002 to four percent in FY 2006. Without adequate funds for engineering to support C4ISR systems integration, the risk is increased that newly acquired air and surface assets may not provide the interoperability across assets or the other capabilities that the Coast Guard needs to perform its mission. Further, where adequate resources are provided for Deepwater systems engineering and integration activities, there is greater potential for increased product quality, reduced costs, and shorter program schedules.

Inadequate User Training

Office of Management and Budget Circular A-130 requires that users of federal information resources have the skills, knowledge, and training they need to manage information resources, enabling the federal government to serve the public through automated means. Similarly, the *Clinger-Cohen Act of 1996* states that agencies are responsible for ensuring that IT users receive the training that they need to effectively perform their jobs.[15] The Deepwater challenge to train personnel to operate effectively the new and upgraded C4ISR equipment in line with these requirements has been considerable. However, given inconsistent and untimely training, a lack of knowledgeable instructors, and inadequate reference materials, the program has not effectively met this challenge. Unless the Coast Guard addresses these training deficiencies, users may not be able to maximize the potential of the C4ISR equipment provided through the Deepwater program.

Training Not Timely

The Deepwater program has not fully ensured that users receive timely instruction on operating new or upgraded C4ISR equipment. The primary

[15] Division E of Public Law 104-106.

strategy has been to offer "just-in-time" training, which entails providing informal, hands-on instruction to users shortly after systems are implemented on the various surface and shore assets. Because of a lack of funding, the program has not established "pipeline" training—a series of required courses and continuing education—to instruct new or incoming crewmembers on how to utilize C4ISR systems. In response to our draft report, the Coast Guard agreed that funding constraints have limited training, but the contractor is meeting funded contractual requirements nonetheless.

According to a number of Coast Guard crews, this lack of pipeline training is a problem particularly for staff transitioning from one assignment to the next. There is a general expectation that incoming staff will quickly learn to operate the C4ISR equipment, even though they do not receive any formal training. Whereas learning C4ISR user skills "on-the-fly" may be easy for technically savvy crewmembers, it is more difficult for those that are not accustomed to operating sophisticated IT equipment. Users who receive "just-in-time" C4ISR training usually are expected to ease the transition for incoming crewmembers by informally training them to use the upgraded IT equipment; however, this is not always effective. Deepwater program officials typically do not revisit assets to train crewmembers that were not present at the time of initial "just-in-time" training.

The combined "just-in-time" and "train the trainer" strategy has several additional limitations. For example, there is no helpdesk number to call for follow-on assistance with the equipment after the "just-in-time" training has been completed. Further, as the Deepwater program has evolved, there have been fewer upgraded assets and therefore fewer people trained who have the potential to provide informal instruction for incoming staff. According to an April 2005 report by COMOPTEVFOR, not enough Coast Guard personnel received "just-in-time" C4ISR training to serve as instructors for new crewmembers who arrived on 123-foot patrol boats later in the year.[16] The review indicated that, as a result, it would be difficult for boat crews to sustain institutional knowledge and pass that knowledge on to relief personnel over the long-term.

Additionally, because the "just-in-time" approach involves providing training in a piecemeal fashion, users can either forget what they learned about component parts from earlier training, or not fully understand how the C4ISR equipment works together as a whole. District 7 Command Center personnel are required to receive 16 hours of training on Deepwater upgrades. However, as of April 2006, they had received only eight hours because all C4ISR

[16] *Update of the 123-foot Patrol Boat Operational Assessment Analysis Report of September 29, 2004,* Department of the Navy, Commander, Operational Test and Evaluation Force, April 27, 2005.

training cannot be completed until the entire system becomes fully operational. Unless the system goes online soon, it may be difficult for District 7 users to link prior training to any future instruction that they receive on the completed system.

Unlike the Deepwater program, the Command and Control Engineering Center—a Coast Guard center of excellence—offers pipeline training. Such training is centered on one Deepwater C4ISR component—the Command Display and Control Integrated Navigation System—to help ensure that users fully understand the upgrade. This training includes four days of formal instruction on a laptop computer, one day of shipboard training, and two or three days of training while at sea. Center officials are available for additional training, as crewmembers need it. A number of Coast Guard officials believe that Deepwater would benefit from adopting a similar approach to training.

Inadequate Contract Trainers

A number of Coast Guard officials told us that the contractors hired to provide "just-in-time" training are not well versed on the Deepwater C4ISR systems. The officials said that the training that the contractors provide is minimal in comparison with what the Coast Guard might provide on similar upgrades: for example, it might consist of the contractor briefly reviewing features of the equipment but without providing hands-on instruction. They said the contractors tend to focus on technical and operational aspects of the systems but do not address how to apply the technology to the Coast Guard mission effectively. Additionally, they said that the training provided by the contractor could be clearer and more understandable.

Further, Coast Guard officials expressed concern that the contract trainers have little concept of how the various C4ISR upgrades link together. Officials said that the contractors provide training on the individual component systems in a piecemeal fashion and seem unsure of how the C4ISR package is supposed to function as a whole. For example, one Coast Guard official mentioned that training on a tactical component of the overall C4ISR system was covered very quickly and only addressed basic concepts. This official said that contract trainers provided no explanation as to how this component fits within the overall C4ISR design. Because they received no hands-on or operational training, crewmembers had to make do and read the instruction manual to learn to use the system on their own time, taking them away from their regularly assigned duties. The Coast Guard official suggested that, without adequate operational training, crewmembers might not be able to utilize the equipment effectively to meet their C4ISR needs.

Because contractor trainers are not always knowledgeable or available to provide C4ISR guidance to crewmembers, Coast Guard officials sometimes must assume these responsibilities. One Coast Guard official has been assigned informally to provide hands-on C4ISR training on the 123-foot patrol boats as well as carry out his primary duties, which include program management, contract oversight, and system testing. Trainees also regularly call this individual directly to ask follow-on questions, instead of contacting Deepwater trainers. Trainees have found this individual to be more helpful than some contractors in providing guidance on how to apply C4ISR technology to Coast Guard missions and scenarios.

Figure 5: USCGC MATAGORDA, 123-Foot Patrol Boat

Lack of Training Guidance

The Deepwater program offers limited reference materials to support C4ISR users. Various training guides, which include systems operating instructions, diagrams, troubleshooting advice, and references, have been published but are not available on all cutters, especially some of the 123-foot patrol boats. (See Figure 5 for a photograph of one such boat.) Crewmembers on one cutter used the training guides at one point and found them very helpful. Other documentation, such as Logistics Information Management System (LIMS) and C4ISR operating manuals, also are available, however a Coast Guard official described the latter as "pretty bad." This official indicated that the descriptions, terminology, and layouts of the manual differed from typical Coast Guard guidance, making it difficult to use. Similarly, other users said that the reference materials are very basic and do not address many of the issues that they encounter in using the software. At times, users have to call a

Deepwater site representative, who phones the help desk, which in turn contacts a contractor technician, for support. The contractor is supposed to return the user's call within a few hours, but officials said that this rarely happens so obtaining assistance can be a time consuming process.

One Coast Guard official said that although some parts of the agency often prepare quick reference cards for users on how equipment operates, the Deepwater program has not done so. A crewmember on one cutter is using his spare time to prepare such cards to help his colleagues address issues that they encounter when operating the upgraded C4ISR equipment.

Users Do Not Maximize Capabilities of C4ISR Equipment

Given the weaknesses in its training approach, the Coast Guard may not be able to maximize all of the potential uses of the C4ISR equipment provided through the Deepwater program. Personnel whom we interviewed generally provided positive feedback on the upgraded systems, but expressed concerns about not receiving adequate training or guidance. They indicated that the combined "just-in-time" and "train the trainer" method—whereby some users receive instruction directly from contract trainers, some get this information second-hand, and others are self-taught—has resulted in inconsistent user knowledge and ability to operate the C4ISR equipment. Where crewmembers have to figure out on their own how to use the new software, it can be very time consuming. For example, it sometimes takes Coast Guard personnel up to 15 minutes to connect to and utilize the SIPRNET capability provided to Deepwater assets. This is too long, especially when they are at sea, tracking illegal "go-fast" boats, which could possibly land on U.S. soil before network connections are established.

Further, many users are unaware of or unable to fully utilize C4ISR capabilities because they have not been trained on all of the component systems. For example, a crewmember on one cutter that we toured was overwhelmed with the number of C4ISR upgrades and was never able fully to learn to operate the security cameras; he could focus only on operations gear instead. Further, this official said that given the lack of training, he has not learned to use SIPRNET or the common operating picture and therefore cannot maximize their capabilities. Unless the Coast Guard takes steps to address these training deficiencies as it deploys additional assets, the problems with untrained C4ISR users and unused capabilities may only worsen.

The Coast Guard recognizes that it has a long way to go to provide adequate training. For example, crewmember training on using C4ISR equipment and LIMS was one of the critical issues that COMOPTEVFOR addressed in its review of 123-foot patrol boat operations. In its April 2005 report,

COMOPTEVFOR stated that systems training was inadequate; there were many areas where crewmembers received no training at all. Also, COMOPTEVFOR found a lack of formal on-board training programs, lesson plans, training handouts, and standards to certify personnel on use of the equipment. COMOPTEVFOR indicated that while "just-in-time" training might prove adequate for current crews, the lack of pipeline training for incoming crews and support personnel was a problem. Based on these findings, COMOPTEVFOR identified 123-foot patrol boat training as a high-risk area that, if not mitigated, could adversely affect the effectiveness and safety of onboard operations.

The Deepwater program has recently issued a broad industry-wide announcement seeking innovative training technology to better support program operations. It has requested information on best practices, new products and techniques, and distance learning initiatives and services that can help reduce costs and enhance the Deepwater training approach. In addition, the program is constructing a facility in Petaluma, California that will offer training on C4ISR equipment. This training facility, due to be completed in 2006, is expected to provide C4ISR training for crewmembers of the soon-to-be deployed National Security Cutter.

Inadequate IT Support

Office of Management and Budget Circular A-130 requires that agencies provide mechanisms to support IT equipment and keep it operational after implementation. The Deepwater prime contractor's approach to upkeep of the new and upgraded C4ISR equipment has been ineffective. In addition to providing technical and engineering services during system testing, integration, and installation, the contractor is responsible for correcting hardware and software deficiencies, systems documentation, and continuously updating the configuration baseline. To this end, the contractor has instituted an Integrated Logistics System, which constitutes its management approach to supporting, maintaining, and ensuring a supply chain for surface and shore assets. An Integrated Logistics Support team helps ensure that all Deepwater assets have adequate parts, training, manuals, and maintenance procedures in place to support the Coast Guard mission.

The Integrated Logistics Support team uses LIMS (a web-based tool) to track requests and exchange information regarding system repairs and replacement parts. C4ISR users can call a toll-free number or log directly into LIMS to make their requests for technical support, though it sometimes can take 3-4 days to receive a response. Via LIMS, users can obtain information about assets that might be able to provide the spare parts they need, too. For example, if the executive officer on one cutter needs a part that is not in stock,

this official might access LIMS to see if another vessel has that part available. Currently, only crewmembers on the 123-foot patrol boats can access LIMS, although there are plans to extend access to other units across the Coast Guard.

The contractor's Integrated Logistics Support approach, although helpful, has not been adequate. A number of officials told us that the Deepwater contractor does not provide a level of assistance comparable to the high-level service they are accustomed to receiving from Coast Guard IT support personnel. Generally, officials said that they need better service, on site technical support, and quicker repairs and parts replacement. They said that, prior to Deepwater, cutters received support from Electronic Support Units and other Coast Guard teams, which were located on Coast Guard installations and therefore were more responsive. The Deepwater contract, however, prevents these Coast Guard units from servicing C4ISR upgrades on surface and shore assets. Officials in the Electronic Support Units also lack knowledge and training on how much of the installed C4ISR equipment operates. Coast Guard personnel must rely on the Deepwater approach, which generally has been slower and less efficient than the Electronic Support Units in providing C4ISR service.

Specifically, the Deepwater program's "just-in-time" approach of generally waiting to accumulate multiple requests from a given location before providing C4ISR support or replacement parts has not been effective. The delays until contractor support arrives on site can impede operational efficiency and mission accomplishment. For example, on one patrol boat, the Coast Guard command and control system has not been operational in over a year because the contractor has not come out to repair it. Further, crewmembers on a different patrol boat told us that their C4ISR equipment kept shutting down unexpectedly, requiring that they restart the entire system every 10-15 minutes to keep it up and running until contractor representatives could arrive to fix the problem. This was especially difficult at night when, for stealth reasons, the cutter conducted maritime security patrols without lights. Crewmembers often found themselves in the precarious position of losing their night vision when returning to the darkened bridge from the brightly lit rooms below deck where the C4ISR equipment was located.

Further, contractor difficulty in locating spare parts adds to delays in providing C4ISR service. This is especially problematic for certain types of assets. Although replacement parts for the new national security cutter are generally available, spares for the legacy 123-foot patrol boats are logistically harder to obtain. Parts are required not only for the 123-foot patrol boat, but also for the short range prosecutors that they transport and use to intercept and

board suspect vessels. Figure 6 provides a picture of a short range prosecutor. (See Figure 6.)

According to one captain, cutters spend an extensive amount of time in repair status. For example, although 123-foot patrol boats are supposed to be in operational status at least 2,500 hours each year, the boats generally spend about half the year undergoing repairs and therefore are unable to meet this expectation. Also, it is time-consuming for crews to remove parts from assets and mail them to the contractor facility for repair. Crewmembers stated that it might take several months to get the equipment back from the contractor. Without the full complement of C4ISR equipment while repairs are ongoing, crews find it difficult to operate the system as a whole. Officials at one operations center responsible for coordinating asset deployment often receive complaints about contractor delays in providing C4ISR support and repairs, but are powerless to help.

Figure 6: USCG Short Range Prosecutor

A lack of contractor personnel on site to provide Deepwater C4ISR support compounds this situation. Due to limited funding, there is generally only one contractor representative available on site at District 7 to respond to problems. This representative is not sufficient to service all the assets in the Miami, Florida; Key West, Florida; and Savannah, Georgia area. This individual functions more as a liaison than a technician with specialized C4ISR training. Overworked, this individual may take a week, or one to two months, to respond to a LIMS repair request. Crewmembers on one cutter have never received a maintenance visit by merely submitting a work order through LIMS. At one point, the crewmembers had to reboot their C4ISR systems every half hour while at sea to sustain communications. Although Deepwater contractors were well aware of the problem, they still had no technicians available to resolve it once the cutter returned to port. In commenting on a draft of this report, the Coast Guard informed us it has made additional support technicians available to respond to crewmember requests. Some crewmembers have suggested that cutter support teams, staffed with shore-side relief personnel, also would be helpful so that C4ISR technicians over-

taxed from keeping the systems operational can take leave once they return from sea.

As a result, instead of working through the established logistics support process, Coast Guard personnel sometimes informally contact officials at the Maritime Domain Awareness Center or District 7 for assistance even though these officials are not responsible for providing Deepwater support. Such ad hoc methods of obtaining C4ISR support have led to confusion as to who is responsible. The Deepwater program recently outlined plans to assign a C4ISR technician to each Deepwater vessel. The strategy is to exchange an engineer billet on each ship for an IT specialist billet. The IT specialist billet is to serve as a liaison between the cutter and the Deepwater contractor to help ensure timely maintenance and support. A drawback to this strategy is the fact that the crew will lose an engine maintenance technician—a critically needed skill to sustain operations of the aging Coast Guard fleet.

Additionally, the LIMS system used to coordinate and track maintenance requests has been difficult to use. First, as previously discussed, requests for assistance submitted through the system are not addressed in a timely manner. Users must follow-up repeatedly to determine the status of their maintenance or parts requests. Second, users said that although the system has much potential, the database is much bigger than what the Coast Guard will ever need, making it unwieldy to use to locate needed equipment. For example, one crewmember stated that it takes him an average of 90 minutes to locate a replacement part in LIMS. Third, LIMS is housed on the communications server so that if the server goes down—which it sometimes does due to overload—the system becomes inaccessible. When this happens, assets at sea become limited in their ability to report maintenance calls. This can affect mission readiness if critical equipment fails: at one point the navigation system on a cutter shut down, requiring that crewmembers manually chart their course in order to dock safely.

Last, often replacement parts are not entered into the LIMS database in a timely manner so that users can readily locate the supplies they need. For example, one crewmember needed a laptop battery but neither the laptop nor the battery was listed in the system. It took the contractor over a month to locate a battery and send it to the crewmember. Crewmembers on this same cutter requested a printer and waited two months for a response in LIMS. During the delay, their options were to buy a new printer with the ship's funds, borrow one from a nearby cutter, or do without. The crew ultimately borrowed a printer from another cutter. Users said that the ability to deal with LIMS deficiencies is the result of tremendous effort by the Deepwater on site representative and other Coast Guard district maintenance organizations. The

COMOPTEVFOR recommended addressing the LIMS deficiencies before system access is provided to other Coast Guard locations.

Because LIMS has not ensured timely IT support, the Coast Guard continues to rely on the long-standing practice of issuing casualty reports to communicate and coordinate C4ISR maintenance requests. Casualty reports are requests issued Coast Guard-wide to call attention to the need for mission-essential repairs or maintenance. There are three levels of casualty reports, corresponding to the criticality of the needed repair: while category 2 casualty reports might be used for minor repairs, category 4 casualty reports are used to secure parts or support fundamental to executing maritime missions (such as, a cutter cannot sail until a technical problem is fixed). To ensure that C4ISR repairs and support are paid for using Deepwater program funds and not general agency operating funds, C4ISR users are not supposed to issue casualty reports. However, when LIMS fails them, C4ISR users often resort to the reports as a means of elevating and ensuring faster response to their maintenance requests.

Recommendations

We recommend that the Commandant, U.S. Coast Guard, direct the Deepwater Program Executive Officer to:

5. Assess Deepwater staffing needs and apply adequate program management resources to effectively oversee and support program activities.
6. Review the Deepwater contract and supporting documents and agreements and make modifications as appropriate to ensure that contractor responsibilities are clearly defined, communicated, and accepted.
7. Establish C4ISR spending priorities to help ensure that "system-of-systems" objectives are achieved in line with budget realities.
8. Review and revise the Deepwater training approach to ensure that sufficient training, adequate instructors, and reference materials are available to support C4ISR systems users.
9. Ensure that the contractor provides adequate and timely support for C4ISR systems and their users.

Management Comments and OIG Evaluation

We obtained written comments on a draft of this report from the Chief of Staff, U.S. Coast Guard. We have included a copy of the comments in their entirety at Appendix B.

In the comments, the Coast Guard generally concurred with all of the findings and recommendations in our report and expressed appreciation for our efforts to document areas for improvement regarding Deepwater's IT systems. The Coast Guard said that it is in the process of implementing corrective actions in line with the high-level report recommendations, but emphasized that funding will be key to accomplishing improvement objectives. Specifically, the Chief of Staff said that funding constraints have delayed the Coast Guard's ability to accomplish certain Deepwater IT objectives as scheduled, requiring the agency to re-plan programmed work and that this may continue to pose challenges for the future. The Chief of Staff went on to provide clarification regarding the findings and corresponding recommendations in our report and summarize progress the Coast Guard has made to address them. While we recognize the efforts that the Coast Guard has ongoing, we look forward to receiving periodic updates on implementation progress as well as additional improvement initiatives.

Specifically, the Coast Guard concurred with Recommendation 1 concerning the need for increased agency input and oversight of the requirements definition process to ensure that contractor activities meet program goals and objectives. The Chief of Staff said that our report accurately discusses the partnership between the Coast Guard and the prime contractor, ICGS, under the terms of the performance-based contract. That is, the contractor is responsible for defining and implementing a plan to achieve overall systems integration objectives, but the Coast Guard decides whether these requirements are being met within available funding. However, the Chief of Staff attributed the OIG's perception of limited Coast Guard influence over contractor effectiveness in meeting requirements to its examination of C4ISR development activities during an early phase of the program. The Chief of Staff inferred that since then, the Coast Guard has put processes in place to oversee contractor activities and reduce the need for changes as the contract progresses. Further, since 2005, the Coast Guard has taken additional steps to improve the requirements definition process and has increased stakeholder representation on the integrated product teams involved in technical reviews hosted by the contractor. We acknowledge the efforts made to improve the requirements definition process during the course of our review and encourage continued enhancements to ensure that the contractor fulfills Coast Guard expectations.

Similarly, the Coast Guard concurred with Recommendation 2 concerning defining and communicating system requirements change management processes. The Chief of Staff stated that the Deepwater Program Office and the prime contractor have implemented engineering and broader change-management processes approved by the Joint Integrated Deepwater System Configuration Control Board. The configuration control board has begun

taking steps to help ensure coordination and oversight of program changes and avoid changes that may previously have gone unreported. In addition, this official said that the requirements management plan is being revised and is due for completion in FY 2006. We are encouraged by such advancements in the requirements change management process and look forward to reviewing the requirements management plan once it is completed.

The Coast Guard concurred with Recommendation 3 regarding steps needed to ensure that the contractor mitigates Deepwater IT security vulnerabilities. The Chief of Staff said that the Deepwater Program Office is working closely with the Coast Guard's Command, Control, Communications, Computers, and Information Technology Directorate to ensure that proper steps are taken in this regard. For example, this official noted that the Coast Guard has addressed security vulnerabilities and received authority to operate the C4ISR systems used on its 123-foot patrol boats. However, the Coast Guard did not address our concerns about continued delays in completing and installing a new Coast Guard command and control system at the District 7 Miami shore site. We would appreciate clarification on the status of this effort as it will affect not only other shore sites that are scheduled to receive the command and control system, but also the National Security Cutter which is due to be completed in 2007.

Although the Coast Guard concurred with Recommendation 4 regarding the shortcomings of the simulation equipment, the Chief of Staff said that independent verification, validation, and accreditation of the simulator is not included in the scope of the contract and is not being pursued at this time. The Chief of Staff contended that the simulator's level of accuracy is sufficient to verify interfaces within the C4ISR system, even though some elements of the Coast Guard have expressed a desire for independent verification, validation, and accreditation of the simulator to help ensure that the actual systems will function properly when deployed to the assets. Further, the Coast Guard did not address part of our recommendation about providing the Navy's Commander, Operational Test and Evaluation Force with the access needed for independent test and evaluation of C4ISR systems and equipment. In line with our report recommendation, we strongly encourage the Coast Guard to plan and complete the verification, validation, and accreditation of the simulator to ensure that the testing environment matches potential real-life situations. In addition, we request that the Coast Guard provide details on its plans for supporting independent C4ISR test and evaluation to ensure that the system will operate efficiently and securely after implementation.

The Coast Guard concurred with Recommendation 5 concerning Deepwater staffing and program management resource needs. In the response, the Chief

of Staff discussed the Commandant's commitment to evaluating and improving the Coast Guard acquisition structure, process, and workforce, but cautioned that finding qualified individuals to fill the vacancies has been a barrier to providing the program oversight and efficiencies needed. This official stated that the Commandant has chartered a panel of experts to formulate recommendations on how to improve Coast Guard acquisitions, with a particular focus on bolstering in-house subject matter expertise. We recognize the difficulties the Coast Guard has had in obtaining qualified personnel, and appreciate continued efforts to overcome this challenge. Ensuring adequate Deepwater program oversight will be key to ensuring that the Coast Guard's mission objectives are successfully met.

The Coast Guard concurred with Recommendation 6 and described efforts to address and review the Deepwater contract and its supporting documents, agreements, and modifications to ensure that contractor responsibilities are clearly defined, communicated, and accepted. Specifically, the Chief of Staff stated that when contracting officers are asked to interpret the contract, there has been no confusion about contractor responsibilities in producing C4ISR systems. Further, this official stated that the contracting officers, contracting officer technical representatives, and program managers are aligned and ICGS is given clear guidance on the contractual requirements. Nonetheless, the Chief of Staff stated that for the next contract award term, government and contractor responsibilities are being further refined and negotiated. In the meantime, activities and processes that can be accomplished within the terms of the existing contract will continue. We are encouraged by the Coast Guard's plan to address ambiguities in the contract for the next award term and look forward to seeing how the government and contractor responsibilities will be clarified and communicated.

The Coast Guard concurred with Recommendation 7 regarding establishing C4ISR spending priorities to achieve "system of systems" objectives. The Chief of Staff said that the Coast Guard currently establishes C4ISR spending priorities each year, but conceded that enacted funding levels have caused certain objectives to be deferred until funding becomes available. Addressing priorities within the funding provided may be a challenge, but will be key to ensuring that assets are equipped with the C4ISR systems they need to operate effectively.

The Coast Guard concurred with Recommendation 8 concerning C4ISR user training and stated that the Coast Guard and contractor have under taken a number of actions to address the various training and logistics system issues described in our report. Such actions include ensuring pipeline training for the National Security Cutter C4ISR suite, as well as providing computer based LIMS training.

However, the Coast Guard's response did not address the need to improve training for the 123-foot patrol boat and shore site C4ISR operators. Specifically, the Chief of Staff responded that most of these issues identified in our report have already been brought to Coast Guard management's attention and have already been incorporated into subsequent training plans. The Chief of Staff stated also that timely and consistent use of the C4ISR systems has improved the contract instructors' knowledge of the systems and that ICGS is meeting funded contractual requirements. We look forward to learning more about the improved training plans and approaches to ensure that C4ISR operators that will use the system at shore facilities and on other Deepwater assets will receive the instruction they need to function effectively.

Lastly, the Coast Guard concurred with Recommendation 9 regarding adequate and timely support for C4ISR systems and their users. Specifically, the Chief of Staff stated that while the contractor is meeting current requirements, the Coast Guard and contractor are evaluating how to provide more effective user support within funding limitations. We look forward to learning more about the plans developed for improvements in this area.

To establish criteria for this review, we researched U.S. laws, regulations, and other federal guidance applicable to the Coast Guard. Documentation, such as media articles and press releases obtained through Internet searches, provided background information about the Deepwater program. Additionally, we reviewed earlier reports and congressional testimony by the Government Accountability Office and industry organizations to learn more about their findings and recommendations related to Deepwater.

To accomplish our review objectives, we met with representatives at Coast Guard headquarters in the Washington, DC area to learn about their roles, responsibilities, and activities related to the Deepwater program. Senior Coast Guard officials provided initial briefings on the program, and more specifically on its C4ISR components. The C4ISR program manager and deputy program manager discussed with us the system requirements definition process as well as their incremental approach to implementing IT and plans to upgrade assets to meet these requirements. These officials, along with other staff at the Systems Integration Program office, told us about testing of newly developed systems, plans for ensuring interoperability of the systems, and user training. They discussed program budgeting, funding, and personnel management. Additionally, these officials provided information on Deepwater contract requirements, performance measurement, and logistics management.

Personnel at Coast Guard headquarters assisted us in identifying other locations where we might visit to learn about new C4ISR components. During the course of our review, we visited the Maritime Domain Awareness Center, a state-of-the art contractor facility in Moorestown, NJ. This center is responsible for developing, testing, and integrating systems and assets related to Deepwater as well as other homeland security programs. In addition to leading us on a tour of the facility, center officials provided several briefings on the Deepwater program structure and plans for providing improved command and control. Center officials discussed Deepwater requirements definition, change management processes, and integrated product and process development. They offered their perspectives on Deepwater program management, communications, and training. Also, they outlined plans for C4ISR system testing, certification, and accreditation. A contractor at the Space and Naval Warfare Systems Command in Charleston, SC discussed system testing and evaluation activities, too.

We visited several Coast Guard vessels and shore sites to understand and observe C4ISR upgrades implemented through the Deepwater program.

Specifically, we toured the following United States Coast Guard Cutters (USCGCs) at locations in Portsmouth, VA, and Key West, FL:

- USCGC NORTHLAND
- USCGC RESOLUTE
- USCGC MATAGORDA
- USCGC NUNIVAK
- USCGC MANITOU
- USCGC METOMPKIN

We visited the Communications Area Master Station Atlantic in Chesapeake, VA (responsible for supporting communications among all Coast Guard assets on the eastern seaboard of the United States) and the Communications Center in Miami, Florida (responsible for supporting Coast Guard District 7 operations). At the various ship and shore locations, we inspected C4ISR upgrades and talked to users about their experiences with the new equipment as well as the training and support they had received. At the District 7 Communications Center, a contractor provided a demonstration of the new command and control system under development. Coast Guard officials, contractors, and users at District 7 told us about their input into C4ISR requirements, system design and security, testing and evaluation of the C4ISR domain, and implementation of the C4ISR components.

Last, we visited two of the Coast Guard's three centers of excellence in communications and IT: The Telecommunications and Information Systems Command in Alexandria, Virginia and the Command and Control Engineering Center in Portsmouth, Virginia. Although not officially part of the Deepwater program, these centers of excellence receive funding to support program activities and help ensure that the systems under development will interface with existing Coast Guard systems.

We limited our audit to C4ISR requirements definition and implementation of systems upgrades. We did not observe systems testing or address classified aspects of the Deepwater program.

We conducted our audit from December 2005 through April 2006. We performed our work according to generally accepted government audit standards. The principal OIG points of contact for this audit are Frank Deffer, Assistant Inspector General, Information Technology Audits and Sondra McCauley, Director, Information Management Division. Other major contributors are listed at Appendix C.

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

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-823
Phone: (202) 267-2294
Fax: (202) 267-4850
Email: mark.kulwicki@uscg.dhs.gov

7501

MEMORANDUM

12 JUL 2006

From: Robert J. Papp, Jr., VADM
Chief of Staff, U.S. Coast Guard

Reply to Attn of: CG-823
Mark Kulwicki
202-267-2294

To: Assistant Inspector General for Information Technology,
Department of Homeland Security

Subj: Improvements Needed in the U.S. Coast Guard's Acquisition and Implementation of Deepwater Information Technology Systems

Ref: (a) Draft Report dated May 2006

1. This letter transmits our comments to the Department of Homeland Security Inspector General draft report findings and recommendations contained in reference (a).

2. We have reviewed the draft report and generally concur with the findings and recommendations. We have provided some technical comments and clarifications for your consideration.

3. The Coast Guard appreciates the opportunity to comment on this report and will continue its work to improve the Information Technology systems in the Deepwater Program. If you have any questions, please contact Mark Kulwicki at (202)-267-2294.

#

Enclosure: U.S. Coast Guard Comments on Draft Report

UNITED STATES COAST GUARD
STATEMENT ON INSPECTOR GENERAL REPORT

TITLE: "Improvements Needed in the U.S. Coast Guard's Acquisition and Implementation of Deepwater Information Technology Systems" (Draft Report dated May 2006)

The Coast Guard concurs with the principal findings of this report and appreciates the efforts of the Office of Inspector General, Department of Homeland Security in documenting areas for improvement within Deepwater's information technology systems.

The Coast Guard also agrees with the high-level recommended actions and is in the process of implementing corrective measures. Key to this is what can be accomplished with the enacted funds.

Information technology systems are extremely sensitive to deliverable deferrals, as the products provided during one segment are interrelated with later work. Funding constraints have caused certain objectives to be postponed until additional funding becomes available, requiring the Coast Guard to re-plan the programmed work.

The following comments are provided in response to the findings of the report.

1 - Recommendation: Increase agency input and oversight of the requirements definition process to ensure the contractor activities meet program goals and objectives.

Concur with these additional clarifications of the finding. The requirements definition process in a performance-based contract involves the Government setting broad-based objectives with the contractor experts defining and implementing a plan to achieve the requirements necessary to meet those objectives within budget. As a result, the Government is the decision maker on whether the contractor is meeting its requirements within available funding. The current arrangement discussed in this report is in accordance with the USCG and the Integrated Coast Guard Systems (ICGS) partnership wherein ICGS has the responsibility for overall systems integration under a performance-based contract.

Perceived "limited influence in how those requirements are met" is explained by the fact that Increment 1 is post-Critical Design Review (CDR). There are processes already in place for input, influence, and review during the Systems Readiness Review (SRR), Preliminary Design Review (PDR) and CDR events. The intent is to control and reduce changes as we progress through these events, and look to introduce further changes either in later increments or via Engineering Change Proposals (ECP).

Since 2005, the Coast Guard has taken additional steps to improve the requirements definition process and now has more stakeholder representation on all Integrated Product Teams (IPTs) who participate in the Technical Solutions Reviews (TSRs) hosted by the contractor.

2 - Recommendation: Clearly define and communicate system requirements change management processes to ensure they are consistently used to identify, evaluate, and apply changes as appropriate, to Deepwater C4ISR requirements.

Concur with these additional clarifications of the finding. The Deepwater Program Office along with our industry partners, ICGS, has implemented an engineering change process—as well as a broader change-management process—culminating in approval by the Joint Integrated Deepwater System Configuration Control Board (JIDS CCB). In addition, the requirements management plan is being revised and will be completed in FY06. The JIDS CCB has begun taking steps to help ensure coordination and oversight of program changes and avoid changes which may previously have gone unreported. These steps include audits, special change reviews, cross-domain specification alignment reviews, process training, and corrective actions.

3 - Recommendation: Ensure that, in line with federal guidelines, the contractor takes steps to mitigate security vulnerabilities that have hindered achievement of C4ISR system certification and accreditation.

Concur with these additional clarifications of the finding. The Deepwater Program Office is working closely with the USCG's Command, Control, Communications, Computers, and Information Technology Directorate (CG-6) to ensure we are taking the proper steps to mitigate security vulnerabilities on future installations of the C4ISR systems in accordance with Department of Defense Information Technology Security Certification & Accreditation Process (DITSCAP) for Secret Internet Protocol Router Network (SIPRNET) based systems and DHS mandated Federal Information Security Management Act (FISMA) standards for Sensitive but Unclassified (SBU) systems.

Currently, the WPB-123 system has been revised to the latest security standards, including the revised system build process, and received a class-wide Authority to Operate (ATO) in mid 2006. The new system is installed on seven operational hulls with the eighth hull scheduled to be completed this fiscal year.

4 - Recommendation: Address shortcomings with simulation equipment and provide the access needed to support independent test and evaluation of C4ISR systems and equipment to ensure that they operate efficiently and securely.

Concur with these additional clarifications of the finding. In the Maritime Domain Awareness Center (MDAC), where the simulation equipment resides, eEYE Retina, Defense Information Systems Agency (DISA) Gold disks, and Systems Requirement Review (SRR) scripts are used for Certification & Accreditation (C&A) purposes. These scripts are supplied as Government Furnished Equipment (GFE) to the contractor and are utilized as a risk reduction tool for C&A scanning purposes in the lab prior to asset deployment. For a different purpose at the MDAC, the Integrated Deepwater System Information Systems (IDSIS) interface simulator is utilized in functional and requirements testing processes. This interface simulator has been developed over many years and has been utilized successfully on other development programs. Its level of fidelity is sufficient to verify interfaces within the C4ISR system that are unavailable with equipment in the lab, and to verify the associated C4ISR system functionality as well. While some elements of the USCG have expressed a desire for an independent Verification,

Validation & Accreditation (VV&A) of the IDSIS simulator, it is not included in the scope of the C4ISR Increment 1 development CLIN. Therefore, VV&A of IDSIS is not being pursued at this time.

5 - Recommendation: Assess Deepwater staffing needs and apply adequate program management resources to effectively oversee and support program activities.

Concur with these additional clarifications of the finding. Deepwater personnel and staffing issues are symptomatic of larger issues facing the Coast Guard and the government acquisition community. Finding qualified individuals to apply for vacancies has been a barrier in providing sufficient oversight and efficiencies within Deepwater.

One of ADM Allen's first priorities articulated shortly after becoming the 23rd Commandant of the Coast Guard is to evaluate and improve the Service's acquisition structure, processes, and workforce. Currently, a panel of experts chartered by ADM Allen is formulating recommendations that will be vetted through USCG leadership. The intention is to improve the Service's execution of acquisition, with a particular focus on bolstering in-house subject matter expertise through a cadre of acquisition professionals. As the largest acquisition in Coast Guard history, Deepwater will be essential in the formulation of these recommendations, and stands to be a primary beneficiary of their implementation.

6 - Recommendation: Review the Deepwater contract and supporting documents and agreements and make modifications as appropriate to ensure that contractor responsibilities are clearly defined, communicated, and accepted.

Concur with these additional clarifications of the finding. When Contracting Officers (KOs) are asked to interpret the contract, there is no confusion about contractor responsibilities in producing C4ISR systems. The KOs, Contracting Officer Technical Representatives (COTRs) and Program Managers (PMs) are aligned and ICGS is provided clear guidance on the contractual requirements.

Additionally, the current award term terminates in June 2007. Consequently, government and contractor responsibilities are being further refined and negotiated as part of the new award term contract. In the meantime, activities and processes that address this issue and that can be accomplished within the existing contract will continue.

7 - Recommendation: Establish C4ISR spending priorities to help ensure that "system of systems" objectives are achieved in line with budget realities.

Concur with these additional clarifications of the finding. We currently establish C4ISR spending priorities each year. The enacted funding levels have caused certain objectives to be deferred until funding becomes available.

8 - Recommendation: Review and revise the Deepwater training approach to ensure that sufficient training, adequate instructors, and reference materials are available to support C4ISR systems users.

Concur with these additional clarifications of the finding. The USCG along with ICGS has already taken many actions to address the ILS and training issues described in this report. These actions include installation of a NSC C4ISR suite at USCG Training Center (TRACEN) Petaluma for pipeline training of NSC personnel and the USCG Reserve and Training Directorate's (CG-13's) efforts to provide Logistics Information Management System (LIMS) training via computer based training (CBT). Most of the data in this report appears to have been captured from WPB-123 crews, and based on the initial training conducted. Many of the issues and comments included in this report were previously captured as part of four Coast Guard led after training "hot wash" activities, and already incorporated into subsequent training evolutions. Time and consistent use of the C4ISR systems have improved the C4ISR contract instructors' knowledge of systems.

The contractor is meeting the *funded* contractual requirements.

9 - Recommendation: Ensure that the contractor provides adequate and timely support for C4ISR systems and their users.

Concur with these additional clarifications of the finding. While the contractor is meeting the funded requirements, with regard to support for the C4ISR systems and their users, the Coast Guard and ICGS are evaluating how to provide more effective user support within available funding.

Information Management Division

Sondra McCauley, Director
John Shiffer, Audit Manager
Meghan Sanborn, Auditor
Shannon Frenyea, Auditor
Lane Melton, Technical Support
Chiu-Tong Tsang, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
Executive Secretariat
General Counsel
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
DHS Legislative and Intergovernmental Affairs
DHS GAO OIG Audit Liaison

United States Coast Guard

Chief of Staff
Deepwater Program Executive Officer
Deepwater C4ISR Program Manager
Audit 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, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, 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 the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations–Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.