United States Government Accountability Office

Testimony

Before the Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, House of Representatives

For Release on Delivery
Expected at 10 a.m. EDT
July 31, 2013

COAST GUARD

Observations on Progress Made and Challenges Faced in Developing and Implementing a Common Operational Picture

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice Issues

July 31, 2013

COAST GUARD

Observations on Progress Made and Challenges Faced in Developing and Implementing a Common Operational Picture

GAO Highlights

Highlights of GAO-13-784T, a testimony before the Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, House of Representatives

Why GAO Did This Study

To facilitate its mission effectiveness through greater maritime situational awareness, the Coast Guard developed its COP—a map-based information system shared among its commands. The COP displays vessels, information about those vessels, and the environment surrounding them on interactive digital maps. COP information is shared via computer networks throughout the Coast Guard to assist with operational decisions. COP-related systems include systems that can be used to access, or provide information to, the COP.

This statement summarizes GAO's work on (1) the Coast Guard's progress in increasing the availability of data sources and COP information to users and (2) the challenges the Coast Guard has experienced in developing and implementing COP-related systems. This statement is based on GAO's prior work issued from July 2011 through April 2013 on various Coast Guard acquisition and implementation efforts related to the COP, along with selected updates conducted in July 2013. To conduct the selected updates, GAO obtained documentation on the Coast Guard's reported status in developing COP-related acquisition planning documents.

What GAO Recommends

GAO has made recommendations in prior work to enhance the Coast Guard's development and implementation of its COP-related systems. DHS generally concurred with the recommendations and has reported actions under way to address them.

View GAO-13-784T. For more information, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

What GAO Found

The Coast Guard, a component of the Department of Homeland Security (DHS), has made progress in developing its Common Operational Picture (COP) by increasing the information in the COP and increasing user access to this information. The Coast Guard has made progress by adding internal and external data sources that allow for better understanding of anything associated with the global maritime domain that could affect the United States. The COP has made information from these sources available to more COP users and decision makers throughout the Coast Guard. For example, in 2006, the ability to track the location of Coast Guard assets, including small boats and cutters, was added to the COP. This capability—also known as blue force tracking—allows COP users to locate Coast Guard vessels in real time and establish which vessels are in the best position to respond to mission needs. In addition to adding information to the COP, the Coast Guard has also made the information contained in the COP available on more computers and on more systems, which, in turn, has increased the number of users with access to the COP.

The Coast Guard has also experienced challenges in developing and implementing COP-related systems and meeting the COP's goals for implementing systems to display and share COP information. These challenges have affected the Coast Guard's deployment of recent COP technology acquisitions and are related to such things as the inability to share information as intended and systems not meeting intended objectives. For example, in July 2011, GAO reported that the Coast Guard had not met its goal of building a single, fully interoperable Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance program (C4ISR) system—a $2.5 billion project intended to enable the sharing of COP and other data among its offshore vessels and aircraft. Specifically, GAO noted that the Coast Guard: (1) repeatedly changed its strategy for achieving the goal of the C4ISR system and (2) that not all vessels and aircraft were operating the same C4ISR system, or even at the same classification level and hence could not directly exchange data with one another as intended. GAO found similar challenges with other Coast Guard COP-related systems not meeting intended objectives. For example, in February 2012, GAO reported that the intended information-sharing capabilities of the Coast Guard's WatchKeeper software—a major part of the $74 million Interagency Operations Center project designed to gather data to help port partner agencies collaborate in the conduct of operations and share information, among other things—met few port agency partner needs, in part because the agency failed to determine these needs when developing the system. Further, in April 2013, GAO reported that, among other things, the Coast Guard experienced challenges when it deployed its Enterprise Geographic Information System (EGIS), a tool for viewing COP information that did not meet user needs. The challenges Coast Guard personnel experienced with EGIS included system slowness and displays of inaccurate information.

Chairman Hunter, Ranking Member Garamendi, and Members of the Subcommittee:

Thank you for the opportunity to discuss the status of the Coast Guard's progress in developing a Common Operational Picture (COP), and the challenges the agency has faced in managing this effort. As you know, maritime domain awareness (MDA)—which involves the effective understanding of anything in the maritime environment that could impact the security, safety, economy or environment of the United States—is critical to the Coast Guard's mission efforts. According to the Coast Guard, MDA played a key role in 2011 as it interdicted over 100 tons of narcotics, intercepted over 2,400 alien migrants, detained over 190 suspected smugglers, boarded over 100 foreign vessels to suppress illegal fishing, and rescued over 3,800 persons.

To enhance its situational awareness, the Coast Guard operates within a complex information-sharing network with its maritime partners. Specifically, as the lead agency in the Department of Homeland Security (DHS) for maintaining and improving MDA efforts, the Coast Guard works with its partners to facilitate the sharing and dissemination of a wide array of information and intelligence to secure the nation's maritime transportation system against potential threats. The level of information sharing among these partners is largely dependent on the information source and classification level. For example, the Coast Guard works directly with the Navy as a major part of its defense readiness mission. However, since the Navy's command and control system operates at the classified level, the Coast Guard must also be able to share information at the classified level. Similarly, because many of its mission-related interagency activities are with other federal, state, and local government agencies, as well as the private sector, the Coast Guard must also be able to communicate and share information at the unclassified level. As a result, the Coast Guard operates in both the classified and unclassified environment.[1]

To facilitate this information sharing for mission effectiveness and situational awareness with all of its partners, in 1998 the Coast Guard

[1] While the Department of Defense-managed classified COP provides important information for Coast Guard maritime operations, over the last 10 years, the Coast Guard has been building its unclassified COP for its personnel, other federal agencies, and non-federal partners.

began developing its COP—an interactive map-based information system that can be shared among Coast Guard commands—that displays vessels and information about those vessels and the environment surrounding them. In general, the Coast Guard's COP can be described as an information display that provides the position and additional information on vessel and aircraft contacts (called tracks) to the Coast Guard and other decision makers. The Coast Guard's concept for the COP includes a complex interplay of data, assets, technology, and multiple organizations at multiple security levels helping to populate and share information within the COP. The COP can be a stand-alone presentation or part of mission-oriented Geographic Information System (GIS) displays that are linked to information sources.[2] COP-related systems include systems that can be used to access, or provide information, to the COP.

My statement today is based on our prior work issued from July 2011 through April 2013 on the Coast Guard's implementation of COP-related systems, and the challenges the Coast Guard has encountered in acquiring and implementing these systems, including selected updates conducted in July 2013 related to the Coast Guard's acquisition strategy of COP-related systems. This statement discusses (1) the Coast Guard's progress in increasing data sources and the availability of COP information to users and (2) the challenges the Coast Guard has experienced in developing and implementing COP-related systems. For our previous reports we analyzed Coast Guard documentation, such as pertinent provisions of the Coast Guard's Common Operational Picture Concept of Operations, and interviewed Coast Guard officials, including headquarters officials responsible for managing the COP's development and requirements and field personnel who use the COP. More detailed information on our scope and methodology appears in our published work. [3] For the selected updates, we obtained documentation on the

[2] Specifically, a GIS is an integrated collection of computer software and data used to view and manage information about geographic places, analyze spatial relationships, and model spatial processes, in order to share information related to the people, vessels, and facilities in a mapped display.

[3] See GAO, Coast Guard: *Clarifying the Application of Guidance for Common Operational Picture Development Would Strengthen Program*. GAO-13-321 (Washington, D.C.: April 25, 2013); GAO, Maritime Security: *Coast Guard Needs to Improve Use and Management of Interagency Operations Centers*. GAO-12-202 (Washington, D.C: February 13, 2012); and GAO, Coast Guard: Action Needed As Approved Deepwater Program Remains Unachievable. GAO-11-743 (Washington, D.C.: July 28, 2011).

Coast Guard's reported status in developing acquisition planning and technical documents for COP-related systems. All of our work was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

According to the Coast Guard, the COP became operational in 2003 and is comprised of four elements:

- **Track data feeds:** The primary information included in the Coast Guard's COP is vessel and aircraft position information—or tracks—and descriptive information about the vessels, their cargo, and crew. Track information may be obtained from a variety of sources depending on the type of track. For example, the COP includes track information or position reports of Coast Guard and port partner vessels.

- **Information data sources:** The information data sources provide supplementary information on the vessel tracks to help COP users and operational commanders determine why a track might be important. The COP includes data from multiple information sources that originate from the Coast Guard as well as from other government agencies and civilian sources.[4]

[4] Internal sources include intelligence inputs and Coast Guard databases such as the Marine Information for Safety and Law Enforcement (MISLE) and the Ship Arrival Notification System (SANS), among others. MISLE collects, stores, and disseminates data on vessels, cargo facilities, waterways, and parties (both individuals and organizations), as well as Coast Guard activities involving all of these entities. MISLE activities include law enforcement boardings, vessel sightings, marine inspections, marine safety investigations, response actions, search and rescue operations, operational controls, and enforcement actions. The SANS is a Coast Guard database populated with Notice of Arrival information that vessels are required to submit 96 hours prior to entering U.S. territorial waters. Coast Guard command centers can access this database to gather vessel, crew, cargo, and company information concerning ships entering their area of responsibility. External sources include the Department of Defense and the National Oceanic and Atmospheric Administration.

- **Command and control systems:** These systems collect, fuse, disseminate, and store information for the COP. Since the COP became operational in 2003, the Coast Guard has provided COP users with various systems that have allowed them to view, manipulate and enhance their use of the COP. These systems have included the Global Command and Control System (GCCS), Command and Control Personal Computer (C2PC), and Hawkeye.[5] In addition to the technology needed to view the COP, the Coast Guard has also developed technology to further enhance the information within the COP and its use to improve mission effectiveness. This has occurred in part through its former Deepwater[6] Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) program system improvements.[7]

- **COP management procedures:** These procedures address the development and the use of the COP. This would include, for example, the Concept of Operations document, which identifies the basic components, use, and exchange of information included in the COP and the requirements document, which identifies the essential capabilities and associated requirements needed to make the COP

[5] C2PC is a Microsoft Windows-based system implemented in 2004 that displays the COP from a GCCS-based server that allows users to view near real-time situational awareness. Hawkeye is a system implemented in 2005 that monitors and tracks commercial vessels on the coast and in port areas using radar, cameras, and Automatic Identification System (AIS) sensors. AIS equipment transmits information such as the name of the vessel, its position, speed, course, and destination to receivers within range of its broadcast, allowing these vessels to be tracked. GCCS is a system developed in 2003 that provides commanders a single, integrated, scalable command and control system that fuses, correlates, filters, maintains and displays location and attribute information on friendly, hostile and neutral forces. It integrates this data with available intelligence and environmental information in support of command decision making.

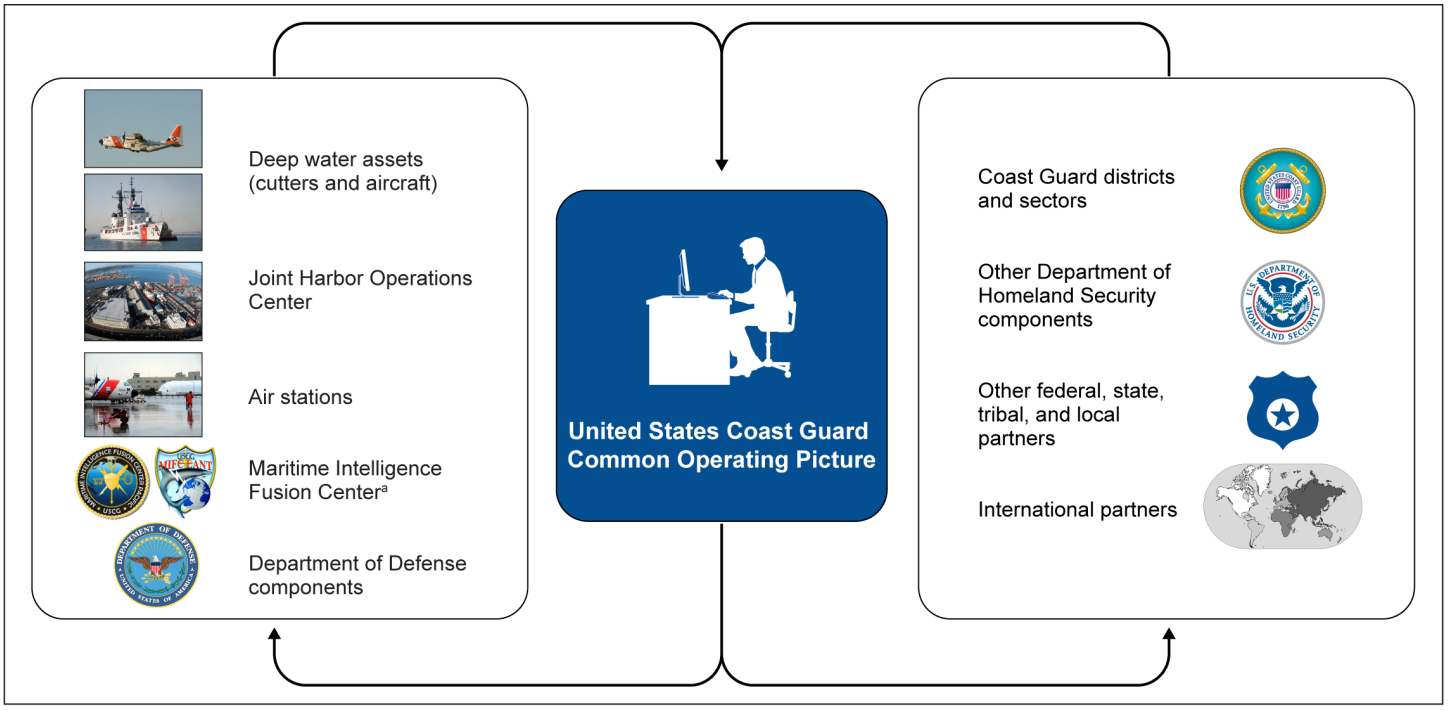
[6] The Coast Guard's acquisition program aimed at recapitalizing its surface, air, and, information technology capacity (formerly known as Deepwater) is an integrated effort to replace or modernize the agency's aging vessels and aircraft assets that are used for missions beyond 50 miles from shore.

[7] C4ISR is the systems, procedures, and techniques used to collect and disseminate information. This includes intelligence collection and dissemination networks, command and control networks, and systems that provide the common operational/tactical picture. C4ISR also includes information assurance products and services, as well as communications standards that support the secure exchange of information by C4ISR systems (digital, voice, and video data to appropriate levels of command). This technology acquisition was intended to create an interoperable network of sensors, computer systems, and hardware to improve MDA.

function. These procedures also include other documents such as standard operating procedures on how the Coast Guard uses the COP, agreements with others using the COP on how information is to be shared or exchanged, and rules for how data are correlated and how vessels are flagged as threats or friends.

Figure 1 depicts the Coast Guard's vision of the COP with Coast Guard internal and external users.

Figure 1: The Coast Guard's Vision of the Common Operational Picture



Source: Coast Guard (photos and logo); DHS (logo); DOD (logo); Map Resources (map); Art Explosion (clip art).

[a]The Coast Guard's two Maritime Intelligence Fusion Centers serve as the central hubs for fusion, analysis, and dissemination of maritime intelligence and information at the operational and tactical level.

The Coast Guard Has Made Progress in Adding Data Sources and the Availability of COP Information to Users

In April 2013, we reported that since the COP became operational in 2003, the Coast Guard has made progress in adding useful data sources and in increasing the number of users with access to the COP.[8] In general, the COP has added internal and external data sources and types of vessel-tracking information that enhance COP users' knowledge of the maritime domain. Vessel tracking information had been available previously to Coast Guard field units located in ports through a Vessel Tracking Service—that is, a service that provides active monitoring and navigational advice for vessels in confined and busy waterways to help facilitate maritime safety.[9] However, adding it to the COP provided a broader base of situational awareness for Coast Guard operational commanders. For example, before automatic identification system (AIS)[10] vessel-tracking information was added to the COP, only Coast Guard units specifically responsible for vessel-tracking, were able to easily track large commercial vessels' positions, speeds, courses, and destinations. According to Coast Guard personnel, after AIS data were added to the COP in 2003, any Coast Guard unit could access such information to improve strategic and tactical decision making. In 2006, the ability to track the location of Coast Guard assets, including small boats and cutters, was also added to the COP. This capability—also known as blue force tracking—allows COP users to locate Coast Guard vessels in real time and establish which vessels are in the best position to respond to mission needs. Similarly, blue force tracking allows the Coast Guard to differentiate its own vessels from commercial or unfriendly vessels.

Another enhancement to the information available in the COP was provided through the updating of certain equipment on Coast Guard assets that enabled them to collect and transmit data. Specifically, the Coast Guard made some data collection and sharing improvements, including the installation of commercial satellite communications

[8] GAO-13-321.

[9] Vessel Tracking Services provide active monitoring and navigational advice for vessels in confined and busy waterways to help facilitate maritime safety.

[10] The Maritime Transportation Security Act of 2002 mandates that most large commercial vessels operate an AIS while in U.S. waters. 46 U.S.C. § 70114. On board vessels, AIS equipment transmits information such as the name of the vessel, its position, speed, course, and destination to receivers within range of its broadcast, allowing these vessels to be tracked when they are operating in coastal areas, on inland waterways, and in ports. Receivers may be installed on other vessels, land stations, or other locations. Coast Guard personnel monitor screens transmitting information on the tracked vessels.

equipment and AIS receivers, onboard its older cutters. This added capability made the COP information more robust by allowing Coast Guard vessels at sea to receive, through AIS receivers, position reports from large commercial vessels and then transmit this information to land units where it would be entered into the COP. This equipment upgrade on older Coast Guard cutters added information into the COP that is generally not available through other means.

According to Coast Guard officials, in addition to adding information to the COP, the Coast Guard has also made the information contained in the COP available on more computers and on more systems, which, in turn, has increased the number of users with access to the COP. One of the key steps toward increasing the number of users with COP access occurred in 2004 with the implementation of C2PC, which made both the classified and unclassified COP available to additional Coast Guard personnel. According to Coast Guard officials, the advent of C2PC allowed access to the COP from any Coast Guard computer connected to the Coast Guard data network. Prior to C2PC, Coast Guard personnel had access to the COP through Coast Guard GCCS workstations.

The Coast Guard Has Experienced Challenges in Developing and Implementing COP-related Systems

We previously reported that the Coast Guard has experienced challenges with COP-related technology acquisitions that resulted from the Coast Guard not following its own information technology acquisition guidance and processes. These challenges included poor usability and the inability to share information as intended, and ultimately resulted in the Coast Guard not meeting its goals for multiple COP-related systems. For example, four COP-related systems have been affected by the Coast Guard not closely following its acquisition processes.

C4ISR project. The C4ISR project was designed to allow the Coast Guard's acquired offshore vessels and aircraft to both add information to the COP using their own sensors as well as view information contained within the COP, thereby allowing these assets to become both producers and consumers of COP information.[11] However, in July 2011, we reported that the Coast Guard had not met its goal of building the $2.5 billion

[11] In July 2011, we reported that the Coast Guard was developing C4ISR infrastructure that it expected to collect, correlate, and present information into a single COP to facilitate mission execution. See GAO-11-743.

C4ISR system.[12] Specifically, we reported that the Coast Guard had repeatedly changed its strategy for achieving C4ISR's goal of building a single fully interoperable command, control, intelligence, surveillance, and reconnaissance system across the Coast Guard's vessels and aircraft. Further, we found that not all aircraft and vessels were operating the same C4ISR system, or even at the same classification level, and hence could not directly exchange data with each other. For example, an aircraft operating with a classified system had difficulty sharing information with others operating on unclassified systems during the Deepwater Horizon oil spill incident. In addition, we reported at that time that the Coast Guard may shift away from a full data-sharing capability and instead use a system where shore-based command centers serve as conduits between assets while also entering data from assets into the COP. This approach could increase the time it takes for COP information, for example, gathered by a vessel operating with a classified system to be shared with an aircraft operating with an unclassified system. Because aircraft and vessels are important contributors to and users of COP information, a limited capability to quickly and fully share COP data could affect their mission effectiveness. We concluded that given these uncertainties, the Coast Guard did not have a clear vision of the C4ISR required to meet its missions.

We also reported in July 2011 that the Coast Guard was managing the C4ISR program without key acquisition documents. At that time, the Coast Guard lacked an acquisition program baseline that reflected the planned program, a credible life-cycle cost estimate, and an operational requirements document for the entire C4ISR acquisition project. According to Coast Guard information technology officials, the abundance of software baselines could increase the overall instability of the C4ISR system and complexity of the data sharing among assets. We recommended, and the Coast Guard concurred, that it should determine whether the system-of-systems concept[13] for C4ISR is still the planned vision for the program, and if not, ensure that the new vision is comprehensively detailed in the project documentation. In response to our recommendation, the Coast Guard reported in 2012 that it was still supporting the system-of-systems approach, and was developing needed

[12] GAO-11-743.

[13] A system-of-systems is a set or arrangement of assets that results when independent assets are integrated into a larger system that delivers unique capabilities.

documentation. We will continue to assess the C4ISR program through our ongoing work on Coast Guard recapitalization efforts.

Development of WatchKeeper. Another mechanism that was expected to increase access to COP information was the DHS Interagency Operations Center (IOC) program, which was delegated to the Coast Guard for development.[14] This $74 million program began providing COP information to Coast Guard agency partners in 2010 using WatchKeeper software. The IOCs were originally designed to gather data from sensors and port partner sources to provide situational awareness to Coast Guard sector[15] personnel and to Coast Guard partners in state and local law enforcement and port operations, among others. Specifically, WatchKeeper was designed to provide Coast Guard personnel and port partners with access to the same unclassified GIS data, thereby improving collaboration between them and leveraging their respective capabilities in responding to cases. For example, in responding to a distress call, access to WatchKeeper information would allow both the Coast Guard unit and its local port partners to know the location of all possible response vessels, so they could allocate resources and develop search patterns that made the best use of each responding vessel.

In February 2012, we reported that the Coast Guard had increased access to its WatchKeeper software by allowing access to the system for Coast Guard port partners.[16] However, the Coast Guard had limited success in improving information sharing between the Coast Guard and

[14] IOCs are facilities and systems designed to help port agencies collaborate in the conduct of operations; collaborate and jointly plan operations; share targeting, intelligence and scheduling information; developing real-time awareness, evaluate threats, and deploy resources; and minimize the economic impact from any disruption. In July 2007, the DHS Assistant Secretary for Legislative Affairs reported to Congress that the Coast Guard's acquisition project Command 21—later named the Interagency Operations Centers (IOC) project—would meet the Safety and Accountability For Every Port Act of 2006 (SAFE Port Act) provision that requires the establishment of IOCs. The SAFE Port Act requires IOCs to be incorporated in the implementation and administration of, among other things, maritime intelligence activities, information sharing, and short and long-range vessel tracking. Pub. L. No. 109-347, 120 Stat. 1884, 1892-93 (2006).

[15] Coast Guard sectors run all Coast Guard missions at the local and port level, such as search and rescue, port security, environmental protection, and law enforcement in ports and surrounding waters, and oversee a number of smaller Coast Guard units, including small cutters, small boat stations, and Aids to Navigation teams.

[16] GAO-12-202.

local port partners and did not follow its established guidance during the development of WatchKeeper—a major component of the $74 million Interagency Operations Center acquisition project. By not following its guidance, the Coast Guard failed to determine the needs of its users, define acquisition requirements, or determine cost and schedule information. Specifically, prior to the initial deployment of WatchKeeper, the Coast Guard had made limited efforts to determine port partner needs for the system. For example, we found that Coast Guard officials had some high level discussions, primarily with other DHS partners, but that port partner involvement in the development of WatchKeeper requirements was primarily limited to Customs and Border Protection because WatchKeeper had grown out of a system designed for screening commercial vessel arrivals—a Customs and Border Protection mission. However, according to the *Interagency Operations Process Report: Mapping Process to Requirements for Interagency Operations Centers*, the Coast Guard identified many port partners as critical to IOCs, including other federal agencies (e.g., the Federal Bureau of Investigation) and state and local agencies.

We also determined that because few port partners' needs were met with WatchKeeper, use of the system by port partners was limited. Specifically, of the 233 port partners who had access to WatchKeeper for any part of September 2011 (the most recent month for which data were available at the time of our report), about 18 percent had ever logged onto the system and about 3 percent had logged on more than five times. Additionally, we reported that without implementing a documented process to obtain and incorporate port partner feedback into the development of future WatchKeeper requirements, the Coast Guard was at risk of deploying a system that lacked needed capabilities, which would continue to limit the ability of port partners to share information and coordinate in the maritime environment. We concluded, in part, that the weak management of the IOC acquisition project increased the program's exposure to risk. In particular, fundamental requirements-development and management practices had not been employed; costs were unclear; and the project's schedule, which was to guide program execution and promote accountability, had not been reliably derived. Moreover, we reported that with stronger program management, the Coast Guard could reduce the risk that it would have a system that did not meet Coast Guard and port partner user needs and expectations. As a result, we recommended, and the Coast Guard concurred, that it collect data to determine the extent to which (1) sectors are providing port partners with WatchKeeper access and (2) port partners are using WatchKeeper; then develop, document, and implement a process to obtain and incorporate

port-partner input into the development of future WatchKeeper requirements; and define, document, and prioritize WatchKeeper requirements. As of April 2013, we had not received any reports of progress on these recommendations from the Coast Guard.

Coast Guard Enterprise Geographic Information System (EGIS). In April 2013, we also reported that Coast Guard personnel we interviewed who use EGIS--an important component, along with its associated viewer, for accessing COP information—stated that they had experienced numerous challenges with the system after it was implemented in 2009.[17] Our site visits to area, district, and sector command centers in six Coast Guard field locations, and discussions with headquarters personnel, identified numerous examples of user concerns about EGIS.[18] Specifically, the Coast Guard personnel we interviewed who used EGIS stated that it was slow, did not always display accurate and timely information, or degraded the performance of their computer workstations—making EGIS's performance generally unsatisfactory to them. For example, personnel from one district we visited reported losing critical time when attempting to determine a boater's position on a map display because of EGIS's slow performance. Similarly, personnel at three of the five districts we visited described how EGIS sometimes displayed inaccurate or delayed vessel location information, including, for example, displaying a vessel track indicating a 25-foot Coast Guard boat was located off the coast of Greenland—a location where no such vessel had ever been. Personnel we met with in two districts did not use EGIS at all to display COP information because doing so caused other applications to crash.

In addition to user-identified challenges, we reported in April 2013 that Coast Guard information technology (IT) officials told us they had experienced challenges largely related to insufficient computational power

[17] EGIS is a Coast Guard geographic information system used to view and manage information about geographic places, analyze spatial relationships, and model spatial processes. Much of the unclassified information contained in the COP is available through EGIS. EGIS can display this information on multiple viewers. See GAO-13-321.

[18] Command Centers perform three primary functions: command and control, situational awareness, and information management for their area of responsibility. They coordinate activities between operational commanders and assets performing the missions. The specific differences among command centers depend on the primary missions performed by their command.

on some Coast Guard work stations, a lack of training for users and system installers, and inadequate testing of EGIS software before installation. For example, according to Coast Guard IT officials, Coast Guard computers are replaced on a regular schedule, but not all at once, and EGIS's viewer places a high demand on the graphics capabilities of computers. They added that this demand was beyond the capability of the older Coast Guard computers used in some locations. Moreover, Coast Guard IT management made EGIS available to all potential users without performing the tests needed to determine if capability challenges would ensue. In regard to training, Coast Guard officials told us that they had developed online internal training for EGIS, and classroom training was also available from the software supplier. However, Coast Guard IT officials stated that they did not inform users that this training was available. This left the users with learning how to use EGIS on the job. Similarly, the installers of EGIS software were not trained properly, and many cases of incomplete installation were later discovered. These incomplete installations significantly degraded the capabilities of EGIS. Finally, the Coast Guard did not pre-test the demands of EGIS on Coast Guard systems in real world conditions, according to Coast Guard officials. Tests conducted later, after users commented on their problems using EGIS, demonstrated the limitations of the Coast Guard network in handling EGIS. According to Coast Guard officials, some of these challenges may have been avoided if they had followed established acquisition processes for IT development. If these problems had been averted, users may have had greater satisfaction and the system may have been better utilized for Coast Guard mission needs.

Poor communication by, and among, Coast Guard IT officials led to additional management challenges during efforts to implement a simplified EGIS technology called EGIS Silverlight. According to Coast Guard officials, the Coast Guard implemented EGIS Silverlight to give users access to EGIS data without the analysis tools that had been tied to technical challenges with the existing EGIS software. Coast Guard personnel from the Office of the Chief Information Officer (CIO) stated that EGIS Silverlight was available to users in 2010; however, none of the Coast Guard personnel we spoke with at the field units we visited mentioned awareness of or use of this alternative EGIS option when asked about what systems they used to access the COP. According to CIO personnel, it was the responsibility of the system sponsor's office to notify users about the availability of EGIS Silverlight. However, personnel from the sponsor's office stated that they were unaware that EGIS Silverlight had been deployed and thus had not taken steps to notify field personnel of this new application that could have helped to address EGIS

performance problems. These Coast Guard officials were unable to explain how this communication breakdown had occurred.

Coast Guard One View (CG1V). In April 2013, we reported that the Coast Guard had not followed its own information technology development guidance when developing its new COP viewer, known as Coast Guard One View, or CG1V.[19] The Coast Guard reported that it began development of CG1V in April 2010 to provide users with a single interface for viewing GIS information, including the COP, and to align the Coast Guard's viewer with DHS's new GIS viewer.[20] However, in 2012, during its initial development of CG1V, the agency did not follow its System Development Life Cycle (SDLC) guidance which requires documents to be completed during specific phases of product development.[21] Specifically, 9 months after CG1V had entered into the SDLC the Coast Guard either had not created certain required documents or had created them outside of the sequence prescribed by the SDLC. For example, the SDLC-required tailoring plan is supposed to provide a clear and concise listing of SDLC process requirements throughout the entire system lifecycle, and facilitate the documentation of calculated deviations from standard SDLC activities, products, roles, and responsibilities from the outset of the project. Though the SDLC clearly states that the tailoring plan is a key first step in the SDLC, for CG1V it was not written until after documents required in the second phase were completed. Coast Guard officials stated that this late completion of the tailoring plan occurred because the Coast Guard's Chief Information Officer had allowed the project to start in the second phase of the SDLC because they believed CG1V was a proven concept. However, without

[19] GAO-13-321. CG1V is a viewer under development that can be used to display information contained within the COP. It can also be used to receive, correlate, and analyze a variety of information from multiple sources to provide situational awareness. Specifically, these viewers interface with the COP and other systems to visually display data, on a map, to decision makers.

[20] Coast Guard officials stated that CG1V development began in 2010 but was delayed for 2 years because of the Coast Guard's response to the Deepwater Horizon oil spill and other unforeseen events that diverted Coast Guard resources.

[21] In 2004, the Coast Guard implemented the SDLC process for non-major IT acquisitions—those with less than $300 million dollars in life cycle costs—to help ensure IT projects are managed effectively and meet user needs. The SDLC process has seven major phases: (1) conceptual planning, (2) planning and requirements, (3) design, (4) development and testing, (5) implementation, (6) operations and maintenance activities, and (7) disposition.

key phase one documents, the Coast Guard may have prematurely selected CG1V as a solution without reviewing other viable alternatives to meet its vision, and may have dedicated resources to CG1V without knowing project costs. In October 2012, Coast Guard officials acknowledged the importance of following the SDLC process and stated their intent to complete the SDLC-required documents. Clarifying the application of the SDLC to new technology development would better position the Coast Guard to maximize the usefulness of the COP. In our April 2013 report, we recommended that the Commandant of the Coast Guard direct the Coast Guard Chief Information Officer to issue guidance clarifying the application of the SDLC for the development of future projects. The Coast Guard concurred with the recommendation and reported that it planned to mitigate the risks of potential implementation challenges of future technology developments for the COP by issuing proper guidance and clarifying procedures regarding the applicability of the SDLC. The Coast Guard estimated that it would implement this recommendation by the end of fiscal year 2013.

Chairman Hunter, Ranking Member Garamendi, and Members of the Subcommittee, this completes my prepared statement. I would be happy to respond to any questions.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Dawn Hoff (Assistant Director), Jonathan Bachman, Jason Berman, Laurier Fish, Bintou Njie, Jessica Orr, Lerone Reid, and Katherine Trimble.