United States Government Accountability Office

GAO

Report to Congressional Requesters

April 2013

# COAST GUARD

# Clarifying the Application of Guidance for Common Operational Picture Development Would Strengthen Program

GAO
Accountability * Integrity * Reliability

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-13-321, a report to congressional requesters

April 2013

# COAST GUARD

## Clarifying the Application of Guidance for Common Operational Picture Development Would Strengthen Program

## Why GAO Did This Study

To facilitate its mission effectiveness and share 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.

GAO was requested to evaluate the Coast Guard's development of COP-related systems. GAO assessed the extent to which the Coast Guard (1) has made progress in making information included in the COP available to users and any challenges it has encountered in implementing COP-related systems, and (2) followed its approved information technology development guidance when developing new technology.

GAO conducted site visits to six Coast Guard sector commands and five district command centers, based on geography to engage a broad range of COP users, analyzed Coast Guard policies and documents, and interviewed Coast Guard headquarters officials managing the COP's development and implementation.

## What GAO Recommends

GAO recommends that the Coast Guard clarify the application of the SDLC for the development of future technology projects. DHS concurred with our recommendation.

View GAO-13-321. For more information, contact Stephen L.Caldwell at (202) 512-9610 or caldwells@gao.gov.

## What GAO Found

The U.S. Coast Guard, a component of the Department of Homeland Security, has made progress in developing its Common Operational Picture (COP) by increasing the information in the COP and increasing user access to this information, but the Coast Guard has also faced challenges in developing COP-related systems. The Coast Guard has made progress by adding internal and external data sources that allow for better maritime domain awareness—the effective understanding of anything associated with the global maritime domain that could affect the United States. In addition, the COP has made information from these sources available to more COP users and decision makers throughout the Coast Guard. However, the Coast Guard has also experienced challenges in meeting the COP's goals and implementing systems to display and share COP information. For example, it experienced challenges when it deployed its Enterprise Geographic Information System (EGIS), a tool that did not meet user needs. The challenges Coast Guard personnel experienced with EGIS included system slowness and displays of inaccurate information. Our prior work 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, did not meet port partners' needs, in part, because the agency failed to determine these needs.

The Coast Guard has not followed its own information technology development guidance when developing new technology. A recent example occurred in 2012 when the agency did not follow its System Development Life Cycle (SDLC) guidance during its initial development of Coast Guard One View (CG1V), its new planned COP viewer. The SDLC requires documents to be completed during specific phases of product development. The Coast Guard, however, did not follow this process during the early development of CG1V. Specifically, we found in February 2013, 9 months after CG1V had entered into the SDLC that 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 to provide a clear and concise listing of SDLC process requirements throughout the entire system lifecycle, and facilitates 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 it was a proven concept. Without key phase one documents, the Coast Guard may have dedicated resources 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.

# Contents

Figures

## Abbreviations

| | |
|---|---|
| AIS | Automatic Identification System |
| C2PC | Command and Control Personal Computer |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance |
| CG1V | Coast Guard One View |
| COP | Common Operational Picture |
| DHS | Department of Homeland Security |
| EGIS | Enterprise Geographic Information System |
| GCCS | Global Command and Control System |
| GIS | Geographic Information System |
| IT | Information Technology |
| MDA | maritime domain awareness |
| MISLE | Marine Information for Safety and Law Enforcement |
| SDLC | System Development Life Cycle |

G A O

Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

April 25, 2013

The Honorable Bill Shuster
Chairman
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Duncan Hunter
Chairman
Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Don Young
House of Representatives

In 2011, the U.S. Coast Guard (Coast Guard) 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. According to the Coast Guard, these accomplishments required the agency to have maritime domain awareness (MDA)—the effective understanding of anything in the maritime environment that could impact the security, safety, economy or environment of the United States. In a 2009 testimony before the Subcommittee on Coast Guard & Maritime Transportation of the Committee on Transportation and Infrastructure, U.S. House of Representatives, Coast Guard Admiral Brian Salerno stated that awareness is essential to everything the Coast Guard does. In his words, "We cannot hold polluters accountable unless we can match them to their spills; we cannot keep vessels from colliding if we don't know where they are; we can't rescue survivors unless we find them; and we cannot intercept those who would do us harm if they are able to blend in with the millions of recreational boaters who lawfully enjoy our ports and coastal waters."[1]

[1] Hearing before the Subcommittee on Coast Guard & Maritime Transportation, Committee on Transportation and Infrastructure, House of Representatives, 111th Congress (2009) (statement of Rear Admiral Brian M. Salerno, Assistant Commandant for Marine Safety, Security and Stewardship, U.S. Coast Guard).

To enhance its situational awareness, the Coast Guard operates within a complex information sharing network with its maritime partners. As the lead agency in the Department of Homeland Security (DHS) for maintaining and improving MDA efforts, the Coast Guard works with its maritime 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 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 have the means to share information at the classified level as well. Similarly, because many of its mission-related interagency activities are with other federal, state, and local government agencies, and 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.

To facilitate this information sharing for mission effectiveness and situational awareness with all of its partners, in 1998 the Coast Guard began developing its Common Operational Picture (COP)—a map-based information system that can be shared among Coast Guard commands—that displays vessels, information about those vessels and the environment surrounding them. According to the Coast Guard, the COP became operational in 2003 and has continued to evolve as more information has been added to it. More fully, the COP is "common" because the same information is shared across computer networks and is available for display in all Coast Guard command centers and on many mobile assets. It is "operational" because the information displayed is relevant to Coast Guard operations and is used to facilitate command and control and decision making. [2] The COP is a "picture" because the information is presented on an interactive digital map. The COP can be a standalone presentation or part of mission-oriented Geographic Information System (GIS) displays that are linked to information sources.[3]

[2] Command and control is the exercise of authority and direction by a commander over assigned and attached forces to accomplish a mission.

[3] 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.

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. Our focus in this report is on the unclassified COP.

You expressed an interest in the impact on mission effectiveness of the Coast Guard's efforts to integrate various data collection technologies into systems displaying the COP. You also expressed interest in the overall management of the Coast Guard's COP technology implementation. This report addresses the following:

- To what extent has the Coast Guard made progress in making information included in the COP available to users and what challenges, if any, has the agency encountered in implementing COP-related systems?
- To what extent is the Coast Guard following its approved information technology development guidance when developing new COP technology?

To address the first objective, we analyzed pertinent provisions of the Coast Guard's Common Operational Picture Concept of Operations and the unsigned Operational Requirements Document for the COP. [4] We also reviewed a Coast Guard-wide message regarding the Coast Guard Enterprise Geographic Information System (EGIS), and memos and e-mails written from 2008 through 2013 by Coast Guard information technology (IT) systems development leadership about the COP, EGIS, and Coast Guard One View (CG1V), the Coast Guard's ongoing GIS viewer development effort.[5] Additionally, because the COP is dependent upon underlying systems being developed and deployed by the Coast

[4] Although the Operational Requirements Document is unsigned we reviewed the document to better understand the Coast Guard's early vision for the COP.

[5] 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. 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.

Guard, we analyzed pertinent sections of prior GAO reports[6] on the Deepwater acquisition program[7] to determine the original information sharing expectations for the Deepwater Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) system and the system's actual capabilities.[8] Similarly, we reviewed our previously published report[9] on Interagency Operations Centers (IOC)[10] to determine the planned information sharing capabilities for the WatchKeeper software toolset, the capabilities of the system as deployed, and the extent to which maritime security stakeholders outside the Coast Guard were using the system.[11]

We obtained information on user experiences with the Coast Guard COP and GIS systems by interviewing Coast Guard personnel at 6 of the 35

[6] GAO, *Coast Guard: Action Needed as Approved Deepwater Program Remains Unachievable*, GAO-11-743 (Washington, D.C.: July 28, 2011). GAO, *Observations on the Coast Guard's and the Department of Homeland Security's Fleet Studies*, GAO-12-751R (Washington, D.C.: May 31, 2012).

[7] The Coast Guard's Deepwater acquisition program (known as Deepwater) was 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.

[8] 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).

[9] GAO, *Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers*, GAO-12-202 (Washington, D.C.: Feb. 13, 2012).

[10] 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; develop real-time awareness, evaluate threats, and deploy resources; and minimize the economic impact from any disruption.

[11] WatchKeeper software was designed to gather data from sensors and port partner sources to provide situational awareness to certain Coast Guard field personnel and to Coast Guard partners in state and local law enforcement and port operations, among others. WatchKeeper was also designed to provide Coast Guard personnel and port partners with access to the same unclassified GIS data; thereby improving collaboration between them.

Coast Guard Sector[12] command centers[13] (Boston, Massachusetts; Hampton Roads, Virginia; Key West and Miami, Florida; Puget Sound, Washington; and San Francisco, California), five of the nine Coast Guard district command centers (Boston, Massachusetts; Portsmouth, Virginia; Miami, Florida; Alameda, California; and Seattle, Washington), and the two Coast Guard area command centers (Portsmouth, Virginia and Alameda, California). We also met with system users at Coast Guard air stations in Elizabeth City, North Carolina; Miami, Florida; and Sacramento, California; on board various Coast Guard Cutters including *Bear*, *Bernard C. Webber*, *Midgett*, and *Waesche*; and at Maritime Intelligence Fusion Centers Atlantic and Pacific.[14] We also interviewed Coast Guard headquarters personnel representing the offices responsible for developing requirements for the COP and GIS, and for developing the IT systems expected to fulfill those requirements. Each location was selected to provide access to a broad range of COP users from different shore-based units, vessels, and aircraft within a concentrated geographic area. While information we obtained at these locations may not be generalized across all Coast Guard units, because we selected these locations based on the diversity of their geographic locations and the various uses of the COP by personnel in these locations, the units we visited provided us with an overview and users' perspectives on the general progress and challenges of implementing the COP. To determine the nature and prevalence of user identified challenges with COP-related systems, we reviewed EGIS system test results and trouble tickets sent by system users seeking assistance in troubleshooting EGIS problems, or in determining the capabilities and usability of EGIS.

[12] 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.

[13] 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.

[14] The Coast Guard's two Maritime Intelligence Fusion Centers serve as the central hub for fusion, analysis, and dissemination of maritime intelligence and information at the operational and tactical level. They provide tactical intelligence support to the District and Sector Intelligence Staffs, and to Command Intelligence Officers in their area.

To address the second objective we reviewed pertinent sections of the Coast Guard's System Development Life Cycle (SDLC) Practice Manual to assess the Coast Guard approach for developing IT systems against its own requirements.[15] We then compared the SDLC manual to industry standard guidance for IT development to ensure it met industry standards. To determine the extent to which the SDLC requirements were met, we reviewed a Coast Guard-wide message regarding EGIS, and memos written from 2009 through 2012 from Coast Guard IT systems development leadership related to the COP, EGIS, and CG1V. We also met with representatives from the Coast Guard CIO's staff and current and former representatives of the Office of C4 & Sensors Capabilities under the Assistant Commandant for Capability to discuss the process used, and the extent to which it followed Coast Guard guidance in the development of COP systems.

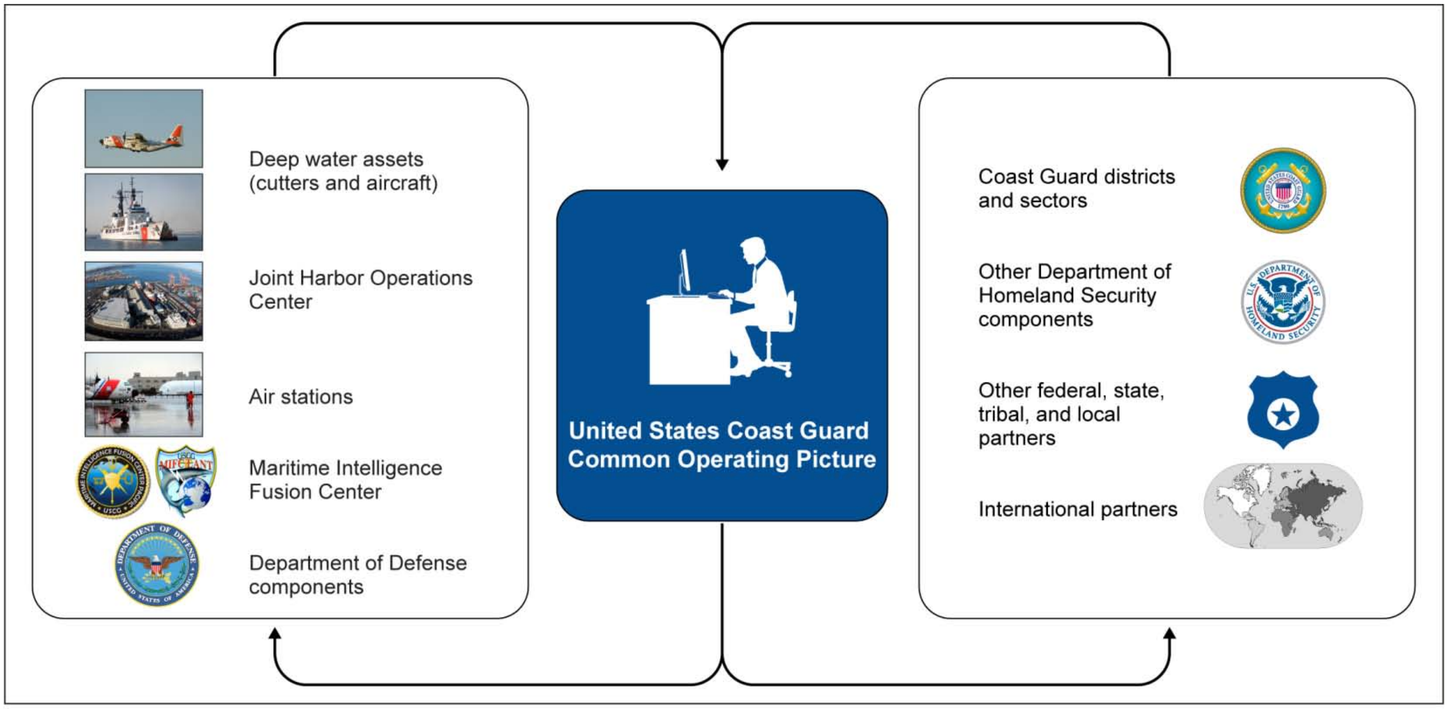
We conducted this performance audit from April 2012 to April 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Background

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. As shown in figure 1, entities outside of the Coast Guard are also integral parts of the COP.

[15] According to the Coast Guard's SDLC manual, the SDLC is a comprehensive lifecycle management framework that applies to all C4&IT systems. A C4&IT system is any combination of related people, methods or processes, hardware, software, data, and telecommunications components utilized to accomplish mission or business needs.

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



Deep water assets (cutters and aircraft)
Joint Harbor Operations Center
Air stations
Maritime Intelligence Fusion Center
Department of Defense components
United States Coast Guard Common Operating Picture
Coast Guard districts and sectors
Other Department of Homeland Security components
Other federal, state, tribal, and local partners
International partners

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

## Elements of the Coast Guard’s COP

According to the Coast Guard, the COP comprises four elements: (1) track data feeds, (2) information data sources, (3) command and control systems, and (4) COP management procedures.

- 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 automatic identification system (AIS) tracks,[16] as well as fishing vessel tracks from the National Oceanic and Atmospheric Administration's[17] Vessel Monitoring System.[18] The COP also includes track information or position reports of Coast Guard and port partner vessels. The Coast Guard receives aircraft location information from Customs and Border Protection's Air and Marine Operations Center.[19] In addition to vessel-related information, the COP also includes information and data that can be geographically referenced, such as the boundary lines of Coast Guard units' areas of responsibility or U.S. territorial waters, and weather information, among other things. See figure 2 for an example of vessel tracks on a COP display.

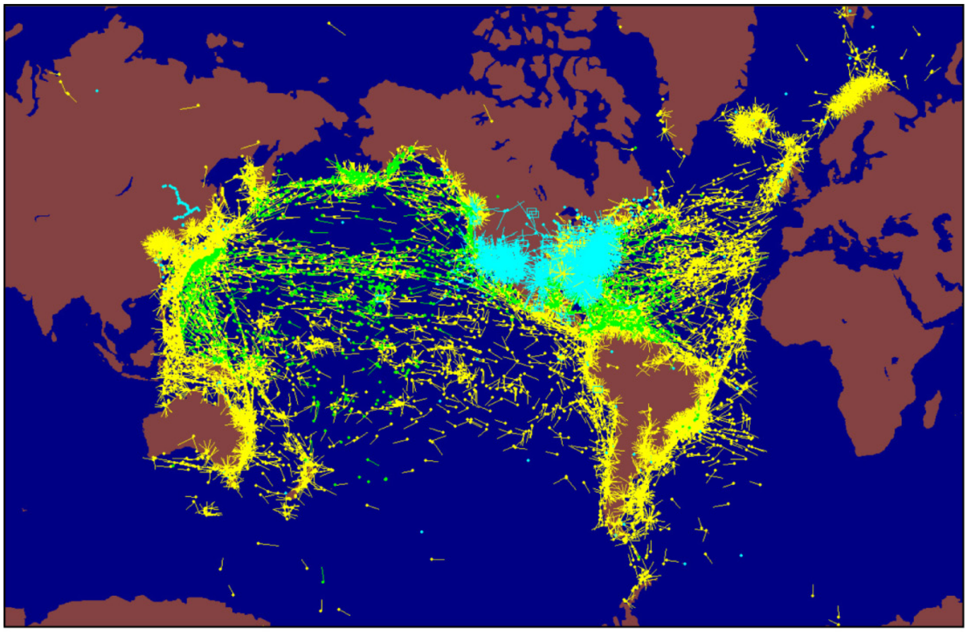
[16] The Maritime Transportation Security Act of 2002 mandates that most large commercial vessels operate an AIS while in U.S. waters. 46 U.S.C. § 70114. On board vessels, AIS equipment transmits information such as the name of the vessel, its position, speed, course, and destination to receivers within 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.

[17] The National Oceanic and Atmospheric Administration is an agency within the Department of Commerce whose missions include management of U.S. marine fisheries.

[18] The Coast Guard defines the Vessel Monitoring System as a tracking system to monitor commercial fishing boats to ensure they are operating only in authorized areas during specified fishing seasons.

[19] The Air and Marine Operations Center is Customs and Boarder Protection's Office of Air and Marine's 24-hour operations center. It provides domain awareness through multiple data feeds and detects, sorts, and monitors suspect air and marine traffic.

Figure 2: Vessel and Aircraft Tracks Displayed on the Common Operational Picture



Source: Coast Guard.

- 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. Internal sources include intelligence inputs and Coast Guard databases such as the Marine Information for Safety and Law Enforcement (MISLE)[20] and the Ship Arrival Notification System,[21] among others. External information sources

[20] 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.

[21] The Ship Arrival Notification System is a Coast Guard database populated with Notice of Arrival information required to be provided by vessels 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.

include the Department of Defense, Joint Interagency Task Force South, and the National Oceanic and Atmospheric Administration.[22] All of these information sources are fused with, or overlaid on, the track information to provide more complete information to COP users about the nature of the identified tracks.

- Command and control systems. These are the systems used to 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. Among these systems have been the Global Command and Control System (GCCS), Command and Control Personal Computer (C2PC), and Hawkeye. See appendix I for additional information on the various systems and applications that COP users identified as providing access to COP information.

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 Program C4ISR system improvements. This technology acquisition was intended to create an interoperable network of sensors, computer systems, and hardware to improve MDA. Specifically, C4ISR was designed to allow the Coast Guard's new vessels and aircraft, acquired under the Deepwater program, 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. 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.[23] Similarly, as we reported in February 2012, the WatchKeeper software that was developed as part of the DHS Interagency Operations Center program was intended to increase the information available to the COP by having port partners add information from their data bases while increasing the port partners' access to Coast Guard information. Coast Guard

[22] Joint Interagency Task Force South is a joint military service and civilian agency task force whose mission is to detect and interdict illegal trafficking.

[23] GAO-11-743.

Sectors were expected to give their port partners access to the software, which was to act as a two way conduit for information sharing. At that time we reported that the Coast Guard had been installing the software in all 35 of its Sector locations.[24]

- 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 that are included in the COP. It would also include the requirements document, which identifies the essential capabilities and associated requirements needed to make the COP function. It also includes other documents such as standard operating procedures on how the Coast Guard uses the COP, agreements with others using the Coast Guard COP on how information is to be shared or exchanged, and the rules for how data are correlated and also how vessels are flagged as threats or friends.[25]

## Advances in Coast Guard COP Technology

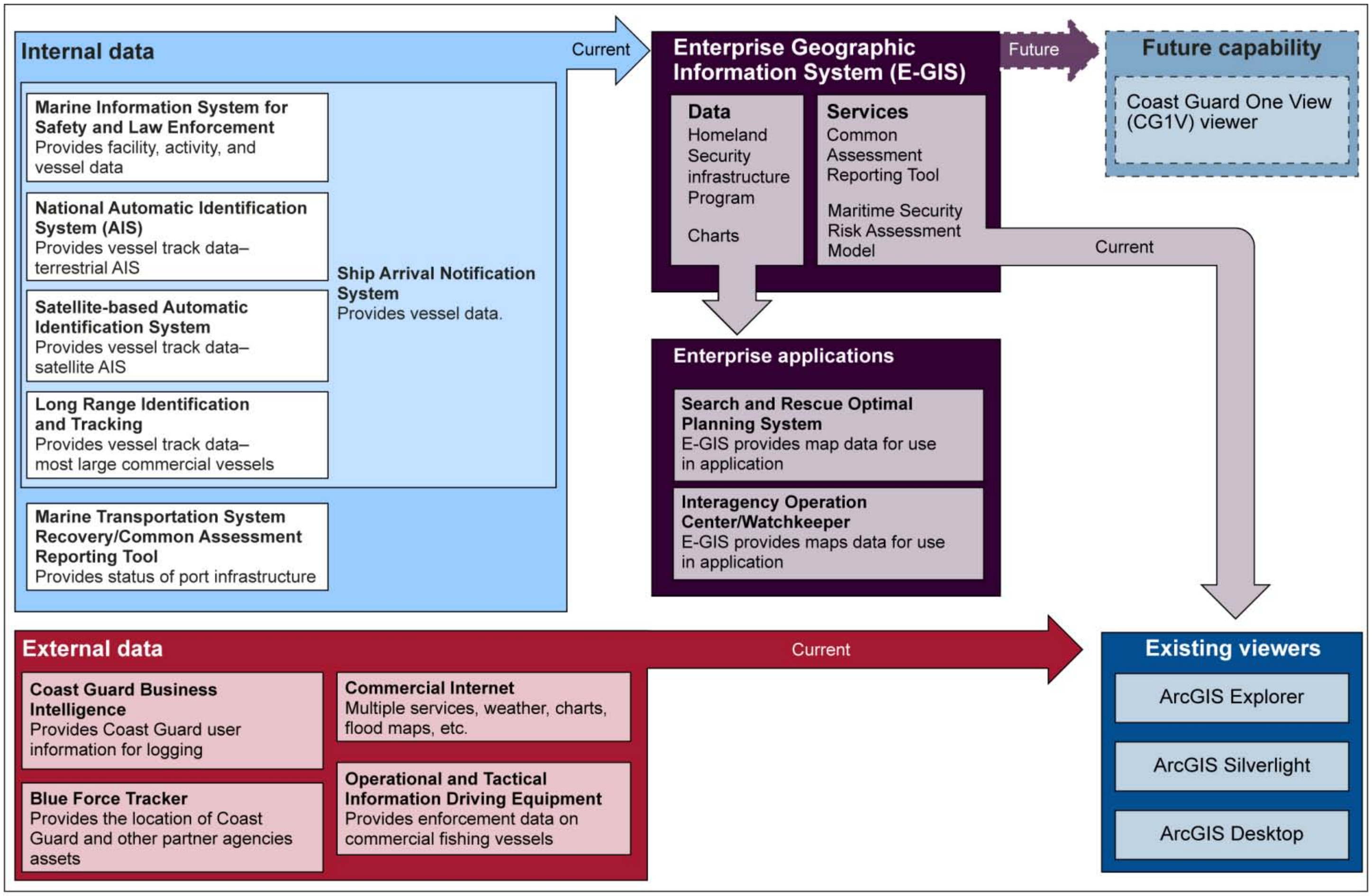
The Coast Guard relies on GIS, which is an integrated collection of computer software and data used to view and manage information about geographic places, analyze spatial relationships, and model spatial processes, in order to share information related to the people, vessels, and facilities in a mapped display. GIS allows Coast Guard personnel the ability to easily see the different aspects of ongoing events on a map, and, if necessary, deploy Coast Guard assets to address the issue. As a result, Coast Guard-wide GIS is an important capability for enabling Coast Guard personnel to view and analyze COP information. The Coast Guard's first agency-wide GIS vehicle was to add a GIS viewer to the existing MISLE database. This later evolved into what the Coast Guard refers to as Enterprise GIS, or EGIS. These GIS-based applications with their incorporated viewers are not limited to viewing the COP, but can

[24] GAO-12-202.

[25] Coast Guard vessels are expected to report their locations to the COP. Positions of other U.S. military and civilian governmental agency vessels are received through information feeds from their home services and agencies and are included in the COP. These vessels are identified in blue on COP displays. Information feeds from Coast Guard Intelligence, and other intelligence sources supply location information on vessels considered as threats. These vessels are identified in red. The locations of neutral vessels, typically maritime traffic, are gathered through systems such as the AIS, and these vessels are identified in white.

also be used to receive, correlate, and analyze a variety of information from multiple sources to provide situational awareness. For example, CG1V is being developed to allow Coast Guard personnel to have a single viewer to interface with COP information and other Coast Guard GIS databases, as seen in figure 3.

**Figure 3: Coast Guard Vision of Coast Guard One View**

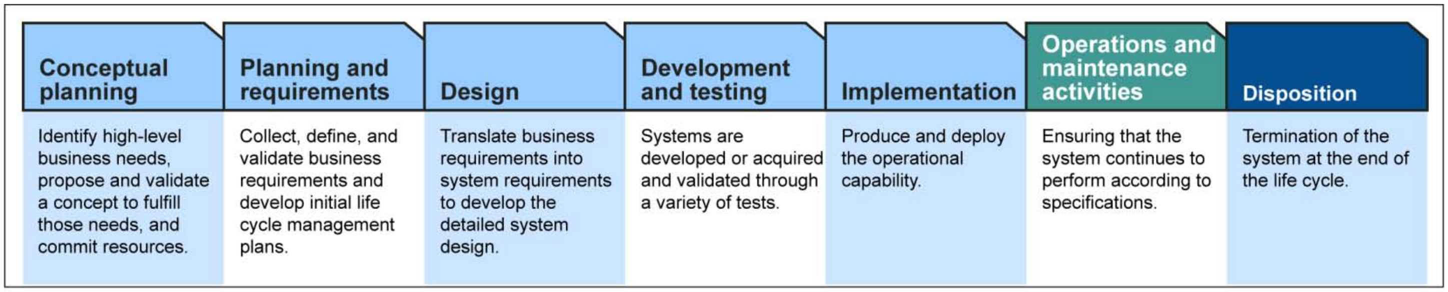

Internal data
Marine Information System for Safety and Law Enforcement
Provides facility, activity, and vessel data
National Automatic Identification System (AIS)
Provides vessel track data–terrestrial AIS
Satellite-based Automatic Identification System
Provides vessel track data–satellite AIS
Long Range Identification and Tracking
Provides vessel track data–most large commercial vessels
Ship Arrival Notification System
Provides vessel data.
Marine Transportation System Recovery/Common Assessment Reporting Tool
Provides status of port infrastructure
Current
Enterprise Geographic Information System (E-GIS)
Data
Homeland Security infrastructure Program
Charts
Services
Common Assessment Reporting Tool
Maritime Security Risk Assessment Model
Future
Future capability
Coast Guard One View (CG1V) viewer
Current
Enterprise applications
Search and Rescue Optimal Planning System
E-GIS provides map data for use in application
Interagency Operation Center/Watchkeeper
E-GIS provides maps data for use in application
External data
Coast Guard Business Intelligence
Provides Coast Guard user information for logging
Blue Force Tracker
Provides the location of Coast Guard and other partner agencies assets
Commercial Internet
Multiple services, weather, charts, flood maps, etc.
Operational and Tactical Information Driving Equipment
Provides enforcement data on commercial fishing vessels
Current
Existing viewers
ArcGIS Explorer
ArcGIS Silverlight
ArcGIS Desktop

Source: GAO and Coast Guard.

## Information Technology Acquisition Process

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[26]—to help ensure IT projects are managed effectively and meet user needs. The Coast Guard's SDLC process is documented in the U.S. Coast Guard SDLC Practice Manual. According to the Practice Manual, the SDLC process provides consistent framework for IT project management and risk evaluation to help ensure systems are developed and maintained on time and within budget, and that they deliver the capabilities necessary to meet user requirements. In addition, the SDLC process provides guidance describing the actions necessary, including event sequences, to ensure compliance with Coast Guard-wide polices, the Office of Management and Budget Circular No. A-130, Management of Federal Information Resources,[27] and DHS Acquisition Directive 102-01 (AD 102-01).[28] The SDLC has seven major phases, beginning with the Conceptual Planning phase and ending with the Disposition phase, as seen in figure 4.

**Figure 4: Illustration of the Seven System Development Life Cycle Phases**



| Conceptual planning | Planning and requirements | Design | Development and testing | Implementation | Operations and maintenance activities | Disposition |
|---|---|---|---|---|---|---|
| Identify high-level business needs, propose and validate a concept to fulfill those needs, and commit resources. | Collect, define, and validate business requirements and develop initial life cycle management plans. | Translate business requirements into system requirements to develop the detailed system design. | Systems are developed or acquired and validated through a variety of tests. | Produce and deploy the operational capability. | Ensuring that the system continues to perform according to specifications. | Termination of the system at the end of the life cycle. |

Source: GAO analysis of Coast Guard System Development Life Cycle Practice Manual.

[26] For major IT acquisitions, those with a life cycle cost of $300 million and above, Coast Guard developed the Major Systems Acquisition Manual to establish policies and procedures, and provide guidance for the implementation of an acquisition management and review process as defined by DHS Acquisition Directive 102-01.

[27] Office of Management and Budget. Circular A-130. http://www.whitehouse.gov/omb/circulars_a130_a130trans4

[28] Department of Homeland Security, DHS Directives System, *Acquisition Management Directive*, Directive Number 102-01 Revision Number 01 (Washington, DC: Jan. 26, 2010).

Figure 4 summarizes the activities that must be completed within each phase. According to the SDLC manual, to proceed from one SDLC phase to the subsequent phase, activities and products from each phase must be completed, reviewed, and approved by the designated authority. Each project is managed by an Integrated Project Team that includes representatives from the CIO's office and representatives of the Coast Guard headquarters directorate responsible for the mission. The project team works with customers, users, and stakeholders to deliver successful and supportable IT systems. The CIO is responsible for designating projects into the SDLC and the Asset Manager within the CIO's office is tasked with guiding, overseeing, and monitoring the execution of SDLC for the assigned system to ensure alignment and compliance with the SDLC process. Another role under the SDLC is the sponsor, who defines and validates functional requirements and accepts capability needed to support Coast Guard mission or business performance.

## Our Prior Work on COP-Related Systems

We have previously reported on challenges the Coast Guard has experienced in meeting goals of COP-related systems, such as C4ISR and WatchKeeper. Some of the shortcomings with these technology systems have included the inability to share information as intended.

### The C4ISR Project

In July 2011, we reported that the Coast Guard had not met its goal of building a single C4ISR system—intended to enable the sharing of COP and other data among its offshore vessels and aircraft.[29] Specifically, we noted that the Coast Guard repeatedly changed its strategy for achieving the goal of its $2.5 billion C4ISR project, which was to build a single fully interoperable command, control, intelligence, surveillance, and reconnaissance system across the Coast Guard's Deepwater vessels and aircraft. 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, sharing information gathered by an aircraft operating with a classified system was difficult during the Deepwater Horizon oil spill incident. In addition, we reported that the Coast Guard may shift away from a full data-sharing capability, and instead, use a system where shore-based command centers could be a conduit between assets while also entering data from assets into the COP. This could increase the time it takes for COP

[29] GAO-11-743.

information 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 may 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 the following key documents: 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 between assets. We recommended, and the Coast Guard concurred, that it should determine whether the system-of-systems concept 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.[30] 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 documentation. The agency also reported that it planned to install a communication system on air and vessel assets to provide for interoperability and direct communication.

### Coast Guard Development of WatchKeeper

One mechanism expected to increase access to COP information was the DHS Interagency Operations Center program, which was delegated to the Coast Guard for development. This program began providing COP information to Coast Guard agency partners in 2010. Using WatchKeeper software, IOCs were originally designed to gather data from sensors and port partner sources to provide situational awareness to Coast Guard sector personnel and to Coast Guard partners in state and local law enforcement and port operations, among others. WatchKeeper was designed to provide Coast Guard personnel and port partners with access to the same unclassified GIS data, thereby improving collaboration between them. Making this information available to port partners has also

[30] 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.

allowed the Coast Guard to leverage the capabilities of its partners in responding to cases. For example, in responding to a distress call, if both the Coast Guard unit and its local port partners know the location of all possible response vessels, they can allocate resources and develop search patterns that make 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; however, the Coast Guard had limited success in improving information sharing between the Coast Guard and local port partners.[31] We found that the Coast Guard did not follow established guidance during the development of WatchKeeper—a major component of the $74 million Interagency Operations Center acquisition project—by, in part, failing to determine the needs of its users, define acquisition requirements, or determine cost and schedule information. Prior to the initial deployment of WatchKeeper, the Coast Guard made only limited efforts to determine port partner needs for the system. We found that Coast Guard officials had some high level discussions, primarily with other DHS partners. Port partner involvement in the development of WatchKeeper requirements was primarily limited to Customs and Border Protection because WatchKeeper grew 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.[32]

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

[31] GAO-12-202.

[32] This document is not available to the public.

at risk of deploying a system that lacked needed capabilities, and that 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 $74 million 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 should 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 have not received any reports of progress on these recommendations from the Coast Guard.

## The Coast Guard Has Made Some Progress in Increasing the Availability of COP Information to Users, but Has Experienced Challenges in Implementing COP-Related Systems

The Coast Guard has made some progress in increasing the amount and type of information included in the COP, and has increased the number of users with access to that information. However, it has faced challenges in implementing some COP-related systems.

## The Coast Guard Has Made Progress in Adding Information to the COP and Making That Information Available to More Users

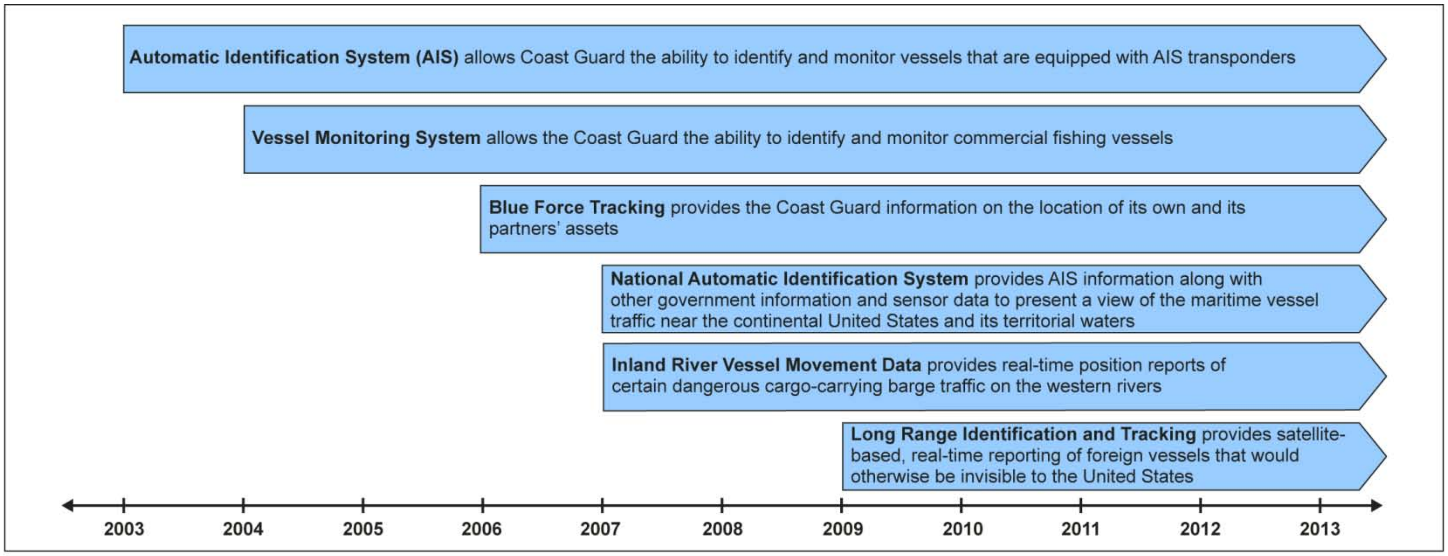
Since the COP became operational in 2003, the Coast Guard has made progress in adding useful data sources and in increasing the number of users with access to the COP. In general, the COP has added multiple sources and types of vessel-tracking information that enhance COP users' knowledge of the maritime domain. While vessel tracking information had been available previously to Coast Guard field units located in ports with a Vessel Tracking Service, adding it to the COP provided a broader base of situational awareness for Coast Guard operational commanders.[33] For example, before AIS 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. Figure 5 shows examples of data sources added to the COP since 2003.[34]

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

[34] According to Coast Guard officials, since the foundation of the COP is based on GCCS, the COP Web Services System is used to translate data sources such as AIS, Vessel Monitoring System, and Long Range Identification and Tracking—a system for tracking vessels at sea—into a format the GCCS can read in order to populate the COP.

Figure 5: Examples of Data Sources Added to the Common Operational Picture since 2003



Source: GAO analysis of Coast Guard data.

Another enhancement to the information available in the COP was provided through the updating of certain equipment on Coast Guard assets to enable them to collect and transmit data. Specifically, the Coast Guard made some data collection and sharing improvements, including the installation of commercial satellite communications 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 both within and outside the agency. 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 Encountered Challenges in Meeting its Goals for Multiple COP-Related Systems

The Coast Guard has experienced multiple challenges in meeting its goals for multiple COP-related systems. Some of these challenges were identified by users and some were identified by Coast Guard IT management. The challenges related to such things as poor usability, degradation of computer performance, and the inability to share information as intended, and they have affected the Coast Guard's deployment of recent technology acquisitions.

### Coast Guard User Identified Challenges

Coast Guard personnel we interviewed who use EGIS stated they experienced numerous challenges with EGIS—an important component with its associated viewer for accessing COP information—after it was implemented in 2009. 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. Specifically, the Coast Guard EGIS users we interviewed stated that EGIS was slow, did not always display accurate and timely information, or degraded the performance of their computer workstations—making EGIS's performance generally unsatisfactory for 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. The problems that we witnessed firsthand or that were described to us by Coast Guard personnel were validated by data from the Coast Guard's EGIS-related help desk tickets which summarize problems with EGIS, among other things, for Coast Guard IT staff.[35] For

[35] Help desk tickets are created when Coast Guard personnel contact the Command, Control, and Communications Engineering Center representatives for technical assistance with any Coast Guard information system. As a result of the call, a ticket is prepared by a representative that includes the issue problem, user name, user location, and issue disposition.

example, our examination of the fiscal year 2011 help desk tickets indicated that users reported several types of problems with EGIS including problems related to performance, loss of capabilities, and data error notification, among other issues. In one District, limitations users encountered with EGIS caused that District to request permission from Coast Guard headquarters to use an alternative system because EGIS's poor performance affected the ability of district personnel to monitor blue force tracking. However, personnel responsible for managing EGIS development at Coast Guard headquarters told us that EGIS was never intended to be able to display blue force tracking—which is likely why users were experiencing difficulty using it for this purpose. They also recognized that the lack of user training on EGIS's capabilities likely contributed to this misunderstanding about its capabilities.

### Coast Guard Management Identified Challenges

Coast Guard IT officials told us they experienced challenges largely related to insufficient computational power on some Coast Guard work stations, a lack of training for users and system installers, and inadequate testing of EGIS software before installation. 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. When EGIS was installed on these older computers performance suffered. In regard to training, Coast Guard officials told us that they had developed on-line internal training for EGIS and classroom training was also available from the software supplier. Coast Guard IT officials said, however, 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 test the demands of EGIS on Coast Guard systems in real world conditions, according to Coast Guard officials. Only later, after users commented on their problems using EGIS, did the Coast Guard perform the tests that 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 the SDLC process for IT development. Specifically, they said that if they had completed three required planning documents—an implementation plan, a training plan, and a Test and Evaluation Master Plan, and conducted the associated activities outlined by these types of planning documents—the agency could have avoided these management challenges that it experienced after EGIS's deployment.[36] 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 CIO office personnel 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 Coast Guard CIO office personnel, it was the responsibility of the 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.

[36] The implementation plan describes how the system will be deployed in the operational environment. The training plan includes a training curriculum, schedule, outline, descriptions, training materials, resources and facility requirements, and identification of the target audience for the system. The Test and Evaluation Master Plan includes the tasks and activities performed to ensure that the system has been adequately tested to assure successful implementation.

## The Coast Guard Has Not Adhered to its Information Technology Development Guidance for Most Recent COP Technology

Although the SDLC process has been in place since 2004, the Coast Guard has not adhered to this guidance for the development of more recent COP-related technology—Coast Guard One View, or CG1V.

The Coast Guard reported that it began development of a new GIS viewer—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. However, the Coast Guard diverged from the SDLC process at the outset when in April 2012 the Coast Guard CIO placed CG1V into the second, rather than first, phase of the SDLC through a designation letter—the action that places an IT acquisition into the Coast Guard's technology development process.[37] The designation letter states that CG1V shall enter the SDLC in its second phase, planning and requirements, rather than its first phase, conceptual planning—without any explanation as to why the system was being placed into the second rather than first phase. As a result, the Coast Guard began developing requirements for CG1V before it had defined how it planned to manage the development of CG1V or had defined the deliverables for each phase of the project.

Coast Guard officials from the program sponsor's office stated that they had skipped the initial phase of the SDLC process because the CIO had allowed them to do so. They stated that this approval was based on the CIO's office agreeing with the program sponsor that CG1V was a proven and validated concept, and that there was value in developing a platform that was compatible with both the DHS and Department of Defense's IT systems. Thus, CG1V program officials stated that they believed that they could enter the SDLC process at planning and requirements rather than at conceptual planning—the phase that is used to determine the need for a system, assess its costs and risks, and define project planning approaches. However, the SDLC manual only allows for "legacy systems"—rather than new systems, such as CG1V—to be placed into the SDLC out of sequence.[38] In addition, the manual explicitly states that the SDLC begins with the conceptual planning phase and as such,

[37] Coast Guard officials stated that CG1V development began in 2010 but was delayed for 2 years due to the Coast Guard's response to the Deepwater Horizon Oil Spill and other unforeseen events that diverted Coast Guard resources.

[38] "Legacy Systems" are systems that have already been developed or reached a stage of maturity but have not completed the necessary products for the SDLC or were developed prior to implementation of the SDLC.

CG1V's designation into the planning and requirements phase did not, from the outset, follow the process outlined in the SDLC guidance.

Although officials stated in October 2012 that efforts were underway to complete phase one documents for CG1V, as of February 2013, almost a year after CG1V's April 2012 designation into the second phase of the SDLC, the Coast Guard has not completed two of the five key documents needed to exit the first phase. For example, the business case—an SDLC-required document that presents the problem to be solved, the solution being proposed, and the expected value of the project—has not been completed by the Coast Guard. This document is also used by management to determine if staff or other resources are to be devoted to defining and evaluating alternative ways to respond to the identified need or opportunity. In addition to not having the business case completed, the acquisition strategy had also not been completed as of February 2013. The acquisition strategy lays out the funding source for the project and the anticipated costs of completing the planning and requirements phase. It also includes a review of the business case to ensure the efficient utilization of Coast Guard resources. As we have previously reported, when managing the C4ISR program, the Coast Guard had inadequate or incomplete acquisition documentation. Specifically, we reported in July 2011, that the Coast Guard's C4ISR project lacked the technical planning documents necessary to both articulate the vision of a common C4ISR baseline—a key goal of the C4ISR project—and to guide the development of the C4ISR system in such a way that the system on each asset remains true to the vision.[39] With respect to our ongoing review of CG1V, by not completing the business case and acquisition strategy, the Coast Guard may have prematurely selected CG1V as a solution without reviewing other viable alternatives to meets its vision, and may also have dedicated resources to CG1V without knowing the project costs.

In addition to not completing two key phase one documents, the Coast Guard has also developed other SDLC documents for CG1V out of sequence. Specifically, the SDLC manual states that the tailoring plan is to be developed in conceptual planning before other documents, such as

[39] GAO-11-743.

the Functional Requirements Document, are created.[40] The tailoring plan is to provide a clear and concise listing of SDLC process requirements throughout the entire system lifecycle, and facilitates the documentation of calculated deviations from standard SDLC activities, products, roles, and responsibilities from the outset of the project.[41] Though the SDLC manual clearly states that the tailoring plan is a key first step in the SDLC, CG1V's tailoring plan was not approved until February 2013, almost a year after CG1V was designated into the SDLC. Coast Guard officials stated that they were completing some documents retroactively because projects cannot exit any phase of the SDLC process without completing the documents required in each of the preceding phases. For example, to exit the conceptual planning phase and enter into the planning and requirements phase, projects must complete all of the exit criteria—which includes several key documents—from the conceptual planning phase. Similarly, the Functional Requirements Document—a phase two document—was also drafted out of sequence in March 2012, but in this case it was drafted early—a full month before CG1V was even designated into the SDLC. By completing these documents out of sequence, the Coast Guard did not follow the disciplined activities and product outputs of the SDLC to ensure that appropriate information is gathered and monitored to support investment decisions.

In December 2012, another key phase one action occurred out of sequence with the review of CG1V by the Coast Guard's Enterprise Architecture Board.[42] The Enterprise Architecture Board, met to determine, among other things, if CG1V aligned with the Coast Guard's

[40] According to the SDLC manual, the Functional Requirements Document defines the functions and requirements of the system being developed or implemented. To define these requirements, the sponsor is required to coordinate with all user, stakeholder, and customer groups during the development of requirements. The different perspectives, inputs, outputs, and services provided by or required for each representative group help strengthen the identification of requirements, necessary functionality, and required integration of the developing system with other systems and the environment in which it will be operating.

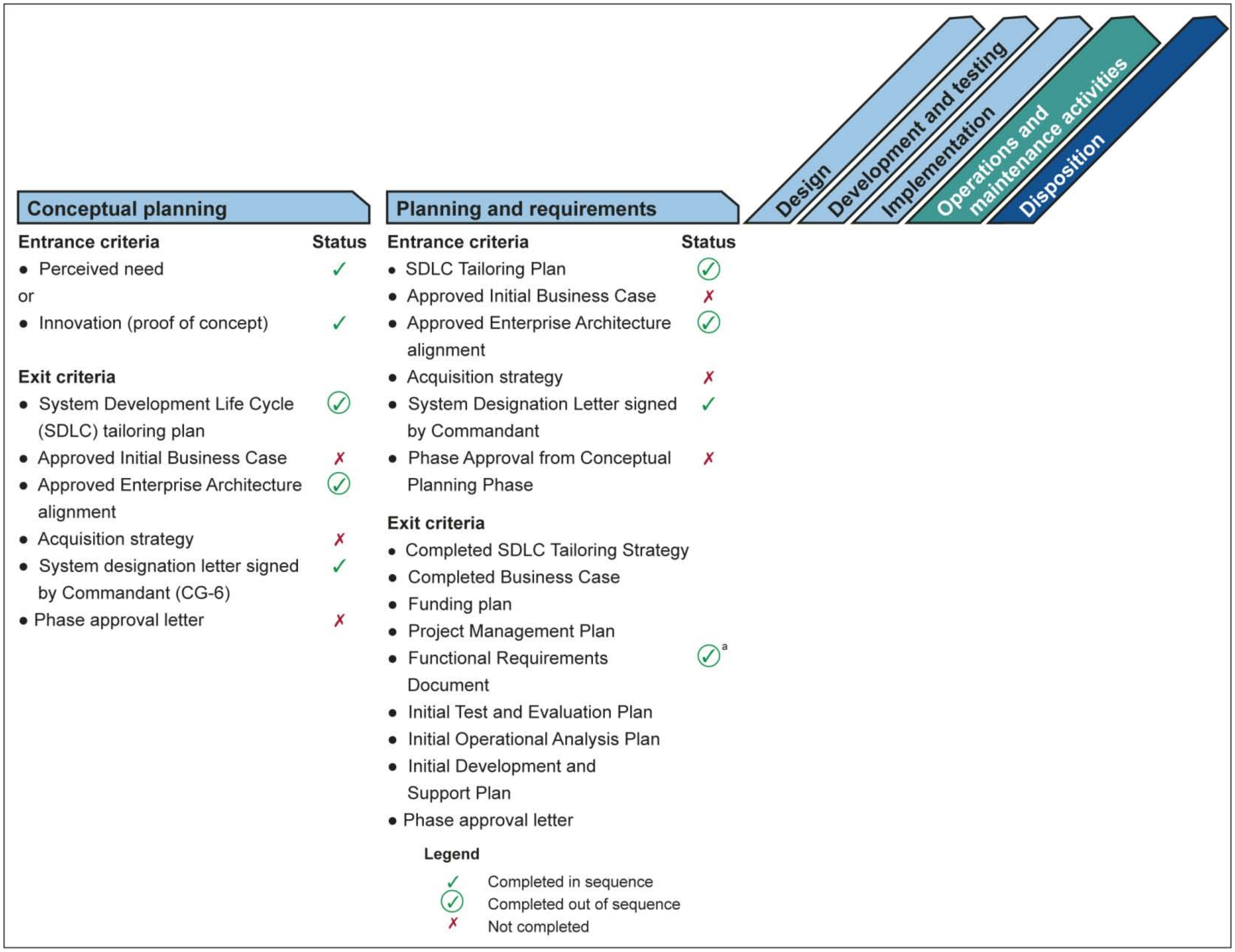
[41] A key feature of the SDLC is the tailoring plan. The SDCL tailoring plan allows for flexibility in the SDLC process. Documented in the tailoring plan, the SDLC requirements may be modified to fit unique project characteristics.

[42] The Enterprise Architecture Board provides guidance through reviews of Coast Guard information technology investments. The Enterprise Architecture Board is required to review all Coast Guard C4&IT acquisitions to make sure the project is aligned with its enterprise architecture.

enterprise architecture and whether an equivalent capability already existed in the enterprise architecture.[43] Although its review was conducted later in the process than might be expected under the SDLC, according to Coast Guard officials, the Enterprise Architecture Board confirmed that CG1V was in alignment with the Coast Guard's enterprise architecture. However, the Enterprise Architecture Board also placed conditions on CG1V's development—including a requirement that CG1V program officials continue working to complete SDLC requirements for this program. As figure 6 shows, most SDLC documents for phase one have either been completed out of sequence or have not been completed at all. If the Coast Guard does not adhere to the SDLC as prescribed, the agency runs the risk of missing early opportunities to identify and address problems if CG1V's development falls behind schedule, runs over its budget, or does not meet user needs when it is deployed.

[43] According to Coast Guard's Enterprise Architecture Handbook, the Coast Guard's enterprise architecture is the blueprint for modernizing and transforming legacy systems to meet future mission capabilities and requirements. Enterprise Architecture brings together key business and technical information across the organization to support better decision making for C4&IT systems. This is done by capturing, organizing, and communicating information about Coast Guard performance measures, business processes, information requirements, applications, systems, and technologies through the Enterprise Architecture Board.

**Figure 6: Coast Guard System Development Life Cycle (SDLC) Documentation for Coast Guard One View as of February 2013**



**Conceptual planning**

| Entrance criteria | Status |
|---|---|
| • Perceived need | ✓ |
| or | |
| • Innovation (proof of concept) | ✓ |
| **Exit criteria** | |
| • System Development Life Cycle (SDLC) tailoring plan | ✓⃝ |
| • Approved Initial Business Case | ✗ |
| • Approved Enterprise Architecture alignment | ✓⃝ |
| • Acquisition strategy | ✗ |
| • System designation letter signed by Commandant (CG-6) | ✓ |
| • Phase approval letter | ✗ |

**Planning and requirements**

| Entrance criteria | Status |
|---|---|
| • SDLC Tailoring Plan | ✓⃝ |
| • Approved Initial Business Case | ✗ |
| • Approved Enterprise Architecture alignment | ✓⃝ |
| • Acquisition strategy | ✗ |
| • System Designation Letter signed by Commandant | ✓ |
| • Phase Approval from Conceptual Planning Phase | ✗ |
| **Exit criteria** | |
| • Completed SDLC Tailoring Strategy | |
| • Completed Business Case | |
| • Funding plan | |
| • Project Management Plan | |
| • Functional Requirements Document | ✓⃝[a] |
| • Initial Test and Evaluation Plan | |
| • Initial Operational Analysis Plan | |
| • Initial Development and Support Plan | |
| • Phase approval letter | |

**Legend**

| | |
|---|---|
| ✓ | Completed in sequence |
| ✓⃝ | Completed out of sequence |
| ✗ | Not completed |

Source: GAO analysis of Coast Guard data.

[a] Since CG1V has not exited out of the planning and requirements phase of the SDLC, it is not required to have met the exit criteria. However, the FRD, an exit requirement, has been completed.

Officials from the CIO's office stated the importance of the phase one documentation to the integrity of the SDLC and stated that they intended to have the required documents from phase one completed and approved. They also stated that in following the SDLC for CG1V they would be encouraging other Coast Guard program offices to follow the

SDLC for their projects. Moreover, a key official from the CIO's office stated in January 2013 that while the SDLC has been around for almost 9 years, the process was slow to ramp up in the Coast Guard and there still remains a lack of awareness around the process. For example, he said that sometimes SDLC-required documents get drafted but the project sponsors do not see them as important and thus do not review them in a timely manner. He also noted that sometimes officials do not follow the process because they are working to meet a deadline. He added, however, that following the SDLC is important because it can help the Coast Guard achieve more successful implementation of new systems.

## Conclusions

The Coast Guard has increased the amount of information included in the COP and the number of users with access to COP information. However, the Coast Guard has encountered and continues to encounter many challenges in implementing its COP goals. These challenges are exemplified by the difficulty the Coast Guard has had with implementing C4ISR systems and COP tools such as WatchKeeper. We have documented these challenges individually in several prior reports but recognize here the broader impact of the challenges with these systems on the Coast Guard's COP. For example, in 2011, we reported that the Coast Guard's C4ISR project had not met its intended goals, and we see now in 2013 that its benefit to the COP has been more limited than originally planned. In 2012, we reported that the Coast Guard's effort to implement WatchKeeper as a COP tool had made some progress, but the lack of port partners utilizing WatchKeeper and its inability to add information from local sensors jeopardized its purpose of improving information sharing and enhancing MDA across federal, state, and local port partners. These limitations have had another impact as well—as they have also affected the robustness and utility of information contained in the COP. In this review we again found IT implementation challenges—in this case related to the Coast Guard's implementation of EGIS. These challenges, which Coast Guard officials acknowledged, resulted in numerous technical shortcomings and unsatisfied users. Coast Guard officials stated that some of EGIS's implementation challenges could have been avoided if they had followed the SDLC process when developing EGIS.

The Coast Guard is now developing a new COP-related technology, CG1V, and early efforts—such as not completing certain documentation and completing other documentation out of sequence—demonstrate that the Coast Guard was again not adhering to its own guidance. Although the Coast Guard has subsequently completed one of the documents required in the conceptual design phase and IT officials have expressed the intent to adhere to the SDLC process during the course of our review, there appears to still be some lack of awareness surrounding the SDLC process. Given the current budget environment and the resource-intensive nature of developing IT systems, the Coast Guard must be especially prudent in expending resources that help it accomplish its missions. Clarifying the applicability of the SDLC process mitigates risks of implementation challenges and maximizes the potential contribution of future technology development for the COP.

## Recommendation for Executive Action

To better ensure that the Coast Guard follows the SDLC as required, we recommend 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.

## Agency Comments

We provided a draft of this report to the Department of Homeland Security for comment. In its written comments, reprinted in appendix II, DHS concurred with our recommendation. In addition, DHS provided technical comments, which we incorporated as appropriate.

With regard to our recommendation, that the Coast Guard issue guidance clarifying the application of the SDLC for the development of future projects, DHS stated that the Coast Guard will review, clarify, and issue guidance related to the applicability of the SDLC process to mitigate risks of implementation challenges and maximize the potential contribution of future technology development for the COP.

As arranged with your office, unless you publicly announce its contents earlier, we plan on no further distribution of this report until 30 days after its issue date. At that time we will send copies of this report to the Secretary of Homeland Security, the Commandant of the Coast Guard, and interested congressional committees as appropriate. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me 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 report. Staff who made key contributions to this report are listed in appendix III.

Steve Caldwell

Stephen L. Caldwell Director,
Homeland Security and Justice Issues

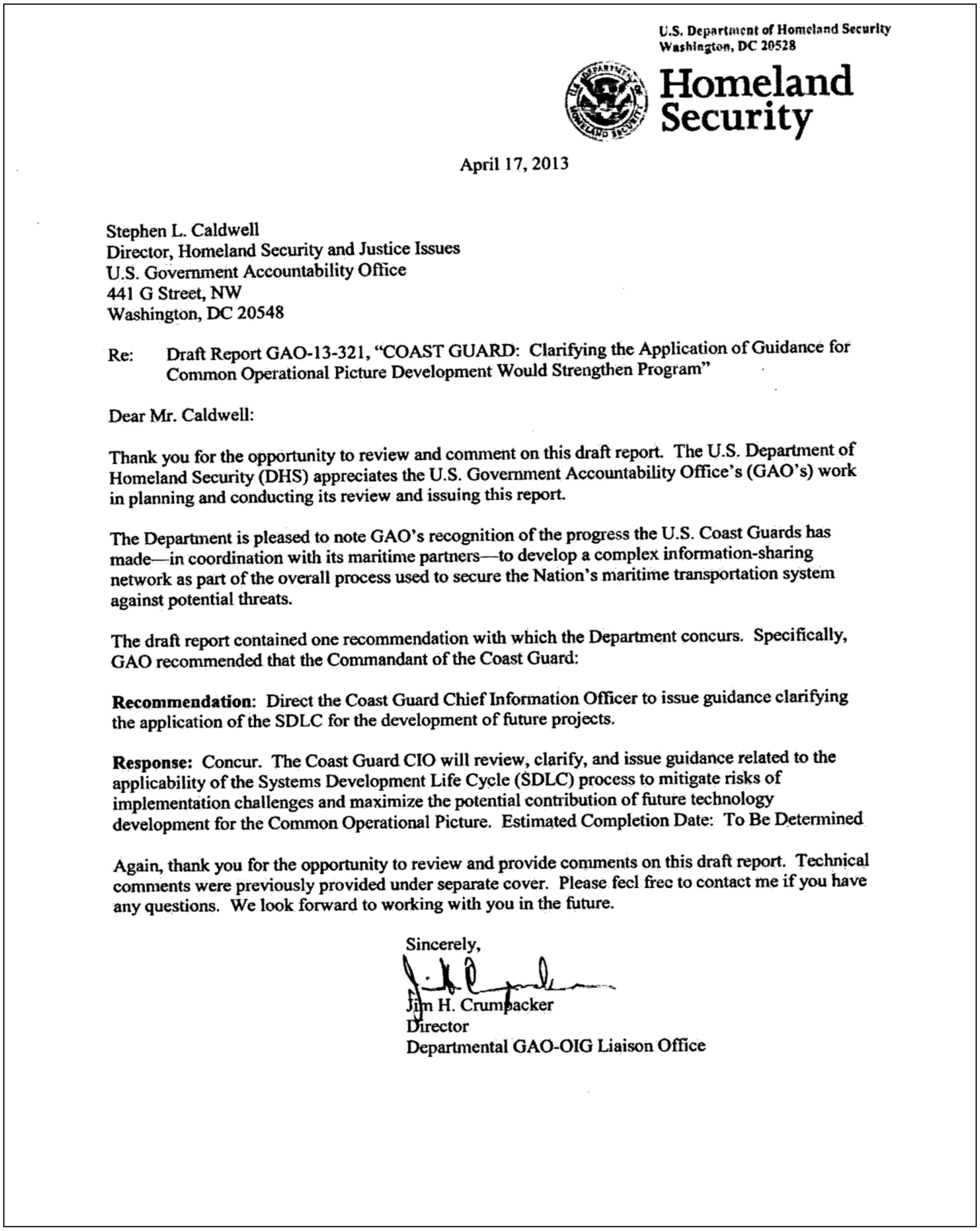
# Appendix I: User Identified Systems and Applications Used to Access Common Operational Picture Information

| System Name | Year Implemented | System Description |
|---|---|---|
| Global Command and Control System (GCCS) | 2003 | A system 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. |
| Marine Information for Safety and Law Enforcement Geographic Information System (MISLE GIS) | 2004 | An application that displays base maps and charts, Coast Guard-specific information on facilities and waterways, as well as dynamic data relating to Coast Guard cases and activities. |
| Command and Control Personal Computer (C2PC) | 2004 | A Microsoft Windows-based system that displays the COP from a GCCS-based server that allows users to view near real-time situational awareness. C2PC enables users to view and edit the COP, apply overlays, display imagery, as well as send and receive tactical messages. |
| Search and Rescue Optimal Planning System | 2004 | A software system the Coast Guard uses for maritime search and rescue planning. It has the ability, among other things, to:<br>• handle multiple rescue scenarios,<br>• model pre-distress motion and hazards,<br>• account for the effects of previous searches,<br>• make requests and receive real-time data from an environmental data server,<br>• manually input wind and current information via a sketch tool using objective analysis techniques, and<br>• use the latest drift algorithms to project the drift of the survivors and craft. |
| Hawkeye[a] | 2005 | A system that monitors and tracks commercial vessels on the coast and in port areas using radar, cameras, and Automatic Identification System (AIS) sensors. |
| WebCOP | 2008 | WebCOP is an Internet browser-based viewer of the COP that features vessel profiling and access to unclassified databases including MISLE and the Ship Arrival Notification System. It also includes access to real-time video feeds, voice communications, and collaborative tools (chat). |
| Enterprise Geographic Information System (EGIS) | 2010 | The Coast Guard’s geographic information system used to view and manage information about geographic places, analyze spatial relationships, and model spatial processes. EGIS can display this information on multiple viewers. |
| WatchKeeper | 2010 | As part of the Interagency Operations Center acquisition project, WatchKeeper is a Coast Guard system originally designed to gather data from sensors and port partner sources to provide situational awareness to Coast Guard personnel and port partners. Through WatchKeeper, Coast Guard personnel and port partners have access to the same data. |

Source: GAO analysis of Coast Guard and Navy information.

[a] The Coast Guard is currently in the process of disposing of the Hawkeye system.

# Appendix II: Comments from the Department of Homeland Security



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

Homeland
Security

April 17, 2013

Stephen L. Caldwell
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-13-321, "COAST GUARD: Clarifying the Application of Guidance for Common Operational Picture Development Would Strengthen Program"

Dear Mr. Caldwell:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the progress the U.S. Coast Guards has made—in coordination with its maritime partners—to develop a complex information-sharing network as part of the overall process used to secure the Nation's maritime transportation system against potential threats.

The draft report contained one recommendation with which the Department concurs. Specifically, GAO recommended that the Commandant of the Coast Guard:

**Recommendation:** Direct the Coast Guard Chief Information Officer to issue guidance clarifying the application of the SDLC for the development of future projects.

**Response:** Concur. The Coast Guard CIO will review, clarify, and issue guidance related to the applicability of the Systems Development Life Cycle (SDLC) process to mitigate risks of implementation challenges and maximize the potential contribution of future technology development for the Common Operational Picture. Estimated Completion Date: To Be Determined

Again, thank you for the opportunity to review and provide comments on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

# Appendix III: GAO Contact and Staff Acknowledgments

## GAO Contact

Stephen L. Caldwell, (202) 512-9610 or caldwells@gao.gov.

## Staff Acknowledgments

In addition to the contact named above, Dawn Hoff, Assistant Director; Jonathan Bachman; Bintou Njie; and Julian King made significant contributions to this report. In addition, William Carrigg and Karl Seifert provided technical assistance with information-technology issues; Michele Fejfar assisted with design and methodology; Tracey King provided legal support; Jessica Orr and Anthony Pordes provided assistance in report preparation; and Eric Hauswirth developed the report's graphics.

(441075)

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

### Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

## Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.