GAO

United States Government Accountability Office

Report to Congressional Requesters

September 2004

MARITIME SECURITY

Better Planning Needed to Help Ensure an Effective Port Security Assessment Program

G A O

Accountability ★ Integrity ★ Reliability

MARITIME SECURITY

Better Planning Needed to Help Ensure an Effective Port Security Assessment Program

Why GAO Did This Study

Created in the wake of the September 11, 2001, terrorist attacks, the Port Security Assessment Program was designed to evaluate security at the nation's 55 most economically and militarily strategic ports. Implemented by the U.S. Coast Guard, an agency of the Department of Homeland Security, the program focuses on identifying vulnerabilities, suggesting approaches to minimize them, and making the information available to those responsible for developing and implementing portwide security plans. The program has been under way for more than 2 years and has undergone several sets of changes, including the addition of a geographic information system (GIS). GAO was asked to discuss why and how the program changed and assess the Coast Guard's approach for implementing the program in its current form.

What GAO Recommends

To enhance the program's effectiveness as a tool for improving port security, GAO recommends that the Coast Guard define performance requirements for the GIS and develop a more comprehensive plan for implementing both the GIS and the Port Security Assessment Program as a whole. In commenting on a draft of this report, the Coast Guard agreed to take steps to define the functional requirements of the GIS and to more fully develop a plan for the long-term implementation of the program.

www.gao.gov/cgi-bin/getrpt?GAO-04-1062.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Margaret Wrightson at (415) 904-2200 or wrightsonm@gao.gov.

What GAO Found

Changes in the Port Security Assessment Program reflect attempts to deal with two main developments since the program's inception: evolving assessment needs at the ports and missteps in how the initial assessments were carried out. The program was designed as a comprehensive assessment of each port and its critical assets, such as passenger terminals, factories, cargo facilities, and bridges. However, the need for comprehensive assessments was diminished when many owners and operators of these critical assets began conducting their own assessments to comply with new regulatory requirements or apply for security grants. The program's assessments also proved more expensive than expected, and a GAO review conducted at the time found shortcomings in their quality and usefulness. The current program's assessments are more targeted in scope and nature, including the opportunity for local Coast Guard officials to request reviews of specific assets they do not know enough about. To help local authorities with security planning and response, the Coast Guard decided to incorporate a GIS. A GIS is a computer mapping system designed to have many information "layers" that can be easily updated and retrieved. The Coast Guard expects to complete the assessments at the 55 ports by February 2005, but no timeline exists for making the GIS component operational.

Although the revised program holds promise, the implementation approach is at increased risk because the Coast Guard is not taking sufficient steps in the planning process. Contrary to best practices for technology systems development, the GIS is being developed without sufficient up-front work to identify how the system will be expected to perform. Both the GIS component and the program as a whole also lack a project plan detailing tasks, schedules, and costs. In other federal agencies, GAO has identified similar projects that failed when such steps were not followed. The initial response of local Coast Guard officials to the new, targeted assessments is generally positive. However, the assessments could be of greater benefit if functional requirements for the GIS were more clearly defined, so the Coast Guard could use the assessments to address gaps in security knowledge.

A terrorist attack on port assets could result in human casualties, economic disruption, and environmental destruction. Assessments of assets such as bridges are to identify methods to protect them from such an attack.

Source: Port of Long Beach.

United States Government Accountability Office

Contents

Abbreviations

BLM	Bureau of Land Management
DHS	Department of Homeland Security
DTRA	Defense Threat Reduction Agency
GIS	geographic information system
MTSA	Maritime Transportation Security Act
NVIC	Navigation and Vessel Inspection Circular

United States Government Accountability Office
Washington, DC 20548

September 30, 2004

The Honorable Don Young
Chairman
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Frank A. LoBiondo
Chairman
Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
House of Representatives

Three years after the terrorist attacks of September 11, 2001, securing the nation's ports continues to be a major concern. Ports and associated waterways are particularly vulnerable because of their size, accessibility, and the many sites and facilities that could be targeted. Gathering information about these vulnerabilities is an essential step for developing deterrents and responding effectively if an incident occurs. One such effort is the Port Security Assessment Program, which is designed to assess port vulnerabilities and security measures in the nation's 55 most economically and militarily strategic ports.[1] Since November 2001, nearly $70 million in appropriated funds has been and continues to be spent on this project, which is administered by the United States Coast Guard, an agency of the Department of Homeland Security (DHS).

This program has changed considerably since its inception in the days immediately following the September 11 attacks. Among these changes, the Coast Guard has added a new feature—a geographic information system (GIS). A GIS is a computer mapping system with many information "layers" that can be quickly retrieved and displayed and easily updated. If, for example, a port received notice of potential threats to chemical plants in the area, a well-designed GIS could identify locations of these plants, provide a variety of information about them, and pinpoint available surveillance and response resources for Coast Guard personnel and others involved in port security. This tool is intended to provide up-to-date, readily accessible information to help develop security plans and respond

---

[1]There are a total of 361 ports in the United States.

GAO-04-1062 Maritime Security

to specific threats or incidents. However, the experience of other federal agencies has shown that developing an information technology system, such as a GIS, that clearly meets users' needs can be difficult.

Given the role the program is expected to play in enhancing the Coast Guard's ability to provide security at our nation's ports, this report (1) discusses why and how the program has changed over time and (2) assesses the Coast Guard's approach for implementing the program as it is currently configured.

To address the first objective, we reviewed Coast Guard documents and spoke with officials at Coast Guard headquarters responsible for implementing the program. We also visited ports that had been assessed. At the ports, we interviewed local Coast Guard personnel as well as numerous stakeholders to determine how the assessment process was carried out. For part of the history of the program, we also relied on our previous work.[2] To address our second objective, we interviewed Coast Guard officials, including the GIS Program Manager to assess progress on the GIS development effort. We also reviewed Coast Guard documents, including its systems acquisition guidance, and documentation of the Coast Guard's efforts to modify its port security GIS. Finally, we reviewed information and documentation related to GIS applications and identified standards and best practices for information systems acquisition and development to determine best practices for managing such a project. Our work, which was conducted from June 2003 through August 2004, was done in accordance with generally accepted government auditing standards.

Results in Brief

The changes in the Port Security Assessment Program reflect attempts to deal with two main developments since the program's inception: evolving assessment needs at the ports and missteps in how the program's initial assessments were carried out. As originally designed, the program involved hiring an outside contractor to conduct a vulnerability assessment encompassing a wide range of port activities and installations, including docks, warehouses, shipping facilities, bridges, factories and power stations, and other facilities and infrastructure. By the time these assessments began in August 2002, however, various port stakeholders,

---

[2]GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*, GAO-03-1155T (Washington, D.C.: Sept. 9, 2003).

including port authorities, and owners and operators of boats, factories, and other facilities, had begun or completed their own assessments in order to identify security vulnerabilities of their assets or apply for federal security grants. More security information subsequently became available as new regulatory requirements went into effect in 2003 requiring owners or operators of specific facilities and vessels in the nation's ports to conduct security assessments of those assets. The increased information from these stakeholders, combined with higher-than-expected costs for the contractor's first 8 assessments, led the Coast Guard to begin changing the scope of the contractor's assessments. When our examination of the contractor's efforts found shortcomings in the quality and usefulness of the assessments, the Coast Guard temporarily stopped conducting assessments in order to make further revisions to the program. By this time, the Coast Guard had also decided that a GIS would be useful for assembling and using the extensive amount of security information becoming available, leading to its adoption as part of the program. The program now includes four components—GIS and three specific types of assessments: a compilation and synopsis of other assessments already conducted in the port, an assessment of the port's maritime vulnerabilities by former Navy Special Operations Forces, and the option for specific assessments of critical infrastructure or operations as requested by the local Coast Guard Captain of the Port. These assessments are more tailored to specific needs than the previous assessments were. The Coast Guard plans to complete these assessments so that all 55 of the most strategic ports will have received an assessment using either the previous approaches or the current approach. Coast Guard officials have not yet determined when the GIS will be completed and made available.

The revised program holds promise, but the Coast Guard's implementation approach is putting that promise at increased risk, particularly for the GIS component. Developing a GIS that can meet the varying security requirements of 55 ports is a complex undertaking, and the Coast Guard has increased the risk by not using project management principles called for by the information technology industry's best practices. Specifically,

- The Coast Guard has not yet identified the functional requirements for the GIS or taken the steps needed to ensure that Coast Guard personnel modifying the system and Coast Guard and other personnel who will actually use it have a clear and mutual understanding of these requirements. Industry practices call for carefully identifying these requirements and documenting how they will be developed. In previous work that we have done on other agencies' development of information

technology systems, we have found systems that had to be abandoned when these steps were not followed.

- The Coast Guard is proceeding without first developing a plan that clearly indicates how the GIS will be managed, what it is expected to cost, or when the various work steps should be completed.

As the Coast Guard is facing these problems for the GIS component, it is proceeding to carry out the other three assessment components at individual ports. As of early August 2004, these assessment components had been performed at twelve ports. Local Coast Guard officials responsible for security at those ports indicated that the individual components generally appeared to be of value in security planning activities. However, because specific functional requirements in the GIS have not been defined, Coast Guard officials are not in a position to fully use these assessments to help address gaps in the information they need for security planning and response. Finally, beyond the GIS component, the program as a whole lacks a fully developed plan detailing costs, schedule, and overall management strategy. The lack of such a plan may negatively affect the usefulness of the assessment program in the long term.

To help ensure that the Port Security Assessment Program is operated effectively, we are recommending that the Coast Guard define and document GIS requirements and develop a plan for implementing both the GIS and the program as a whole. In commenting on a draft of this report, Coast Guard officials generally agreed with the facts and concurred with our recommendations. The Coast Guard also provided technical comments which we have incorporated into this report as appropriate.

Background

Creating effective security in the nation's ports in the post-September 11 world is a challenging task. Ports present attractive targets for terrorists: they are sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks. Besides terminals where goods bound for import or export are unloaded or loaded onto vessels, ports also contain other facilities critical to the nation's economy, such as refineries, factories, and power plants. These many facilities, along with the ships and barges that ply port waterways, can be vulnerable on many fronts. For example, container terminals, where containers are transferred between ships and railroad cars or trucks, need ways to screen vehicles and routinely check cargo for evidence of tampering. At factories and other facilities where hazardous

materials are present, safeguards must be in place to prevent unauthorized persons from gaining access. Similarly, vessels ranging from oil tankers to tugboats need effective access control over critical operating areas, such as engine and control rooms.

The framework for the nation's collective response to this challenge is now found in the Maritime Transportation Security Act (MTSA), passed by the Congress in November 2002. MTSA's implementing regulations require owners and operators of facilities and vessels to conduct assessments that will identify their security vulnerabilities and to develop security plans to mitigate these vulnerabilities. Under these regulations, these plans are to include such items as measures for access control, responses to security threats, and drills and exercises to train staff and test the plan. MTSA was enacted after the Coast Guard initially began developing the Port Security Assessment Program in the wake of the September 11 attacks.

Some basic information about geographic information systems, or GIS, may be helpful in understanding this component of the Port Security Assessment Program. A GIS can be thought of as a sort of electronic map, but with many more capabilities than traditional paper mapping. For example, paper maps can provide only a static snapshot of selected entities and their locations and cannot be easily updated or changed. By contrast, information in a GIS can be easily and continually updated. In addition, because a GIS stores information on separate "layers" related to such things as roads or buildings, users can combine data layers at will, providing the capability to quickly create and view maps for specific purposes any time they are needed. Data layers in a GIS can be extremely varied. Typical types include the following:

- Layers describing location, ownership, and other information about real property (called cadastral data).

- Layers that have the characteristics of a map and image qualities of a photograph (called digital orthoimagery).

- Layers describing water features such as lakes, ponds, streams and rivers, canals, oceans, and coastlines (called hydrographical data).

For the Coast Guard, potential GIS layers could include transportation—describing anchorages, bridges, and roadways; utilities—including power plants, power lines, and substations; and emergency response—including police and fire stations, and hospitals. Figure 1 illustrates, in a simplified way, this concept of layers and how they can be integrated.

Figure 1: Examples of Layers in a Geographic Information System
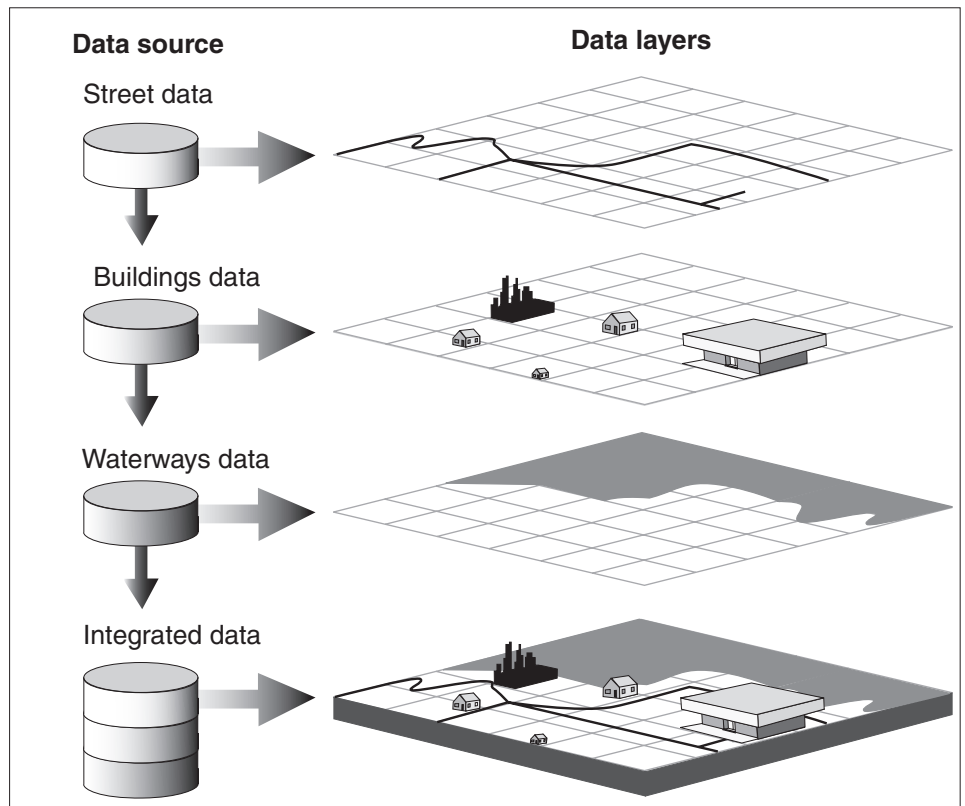

Source: GAO.

The database capabilities of a GIS allow many other kinds of information to be embedded on these data layers as well, so that the information is easily available. For example, a GIS allows the user to know not only the location of a building relative to other buildings or roads, but can also provide information such as the building's owner, when the building was built, the building's contents, and its dimensions and height. This ability to create maps on demand for specific purposes, with additional information at the ready, surpasses what can be done with traditional mapping approaches.

One illustration of a GIS's usefulness came in connection with efforts to recover debris from the space shuttle *Columbia* when it was lost in re-entering the earth's atmosphere on February 1, 2003. Debris from the shuttle was spread over at least 41 counties in Texas and Louisiana. In Texas, a state-operated GIS provided authorities with precise maps and

search grids to guide reconnaissance and collection crews in the field. Officials in charge of the effort used maps of debris fields, combined with GIS data about the physical terrain, to carefully track the pieces of debris found. Figure 2 is a map, created from debris data entered into the GIS, showing the general west-to-east track of debris data across several east Texas counties and the outer boundaries of the area in which debris was found.

Figure 2: Sample GIS Map of Debris Path from Space Shuttle *Columbia*
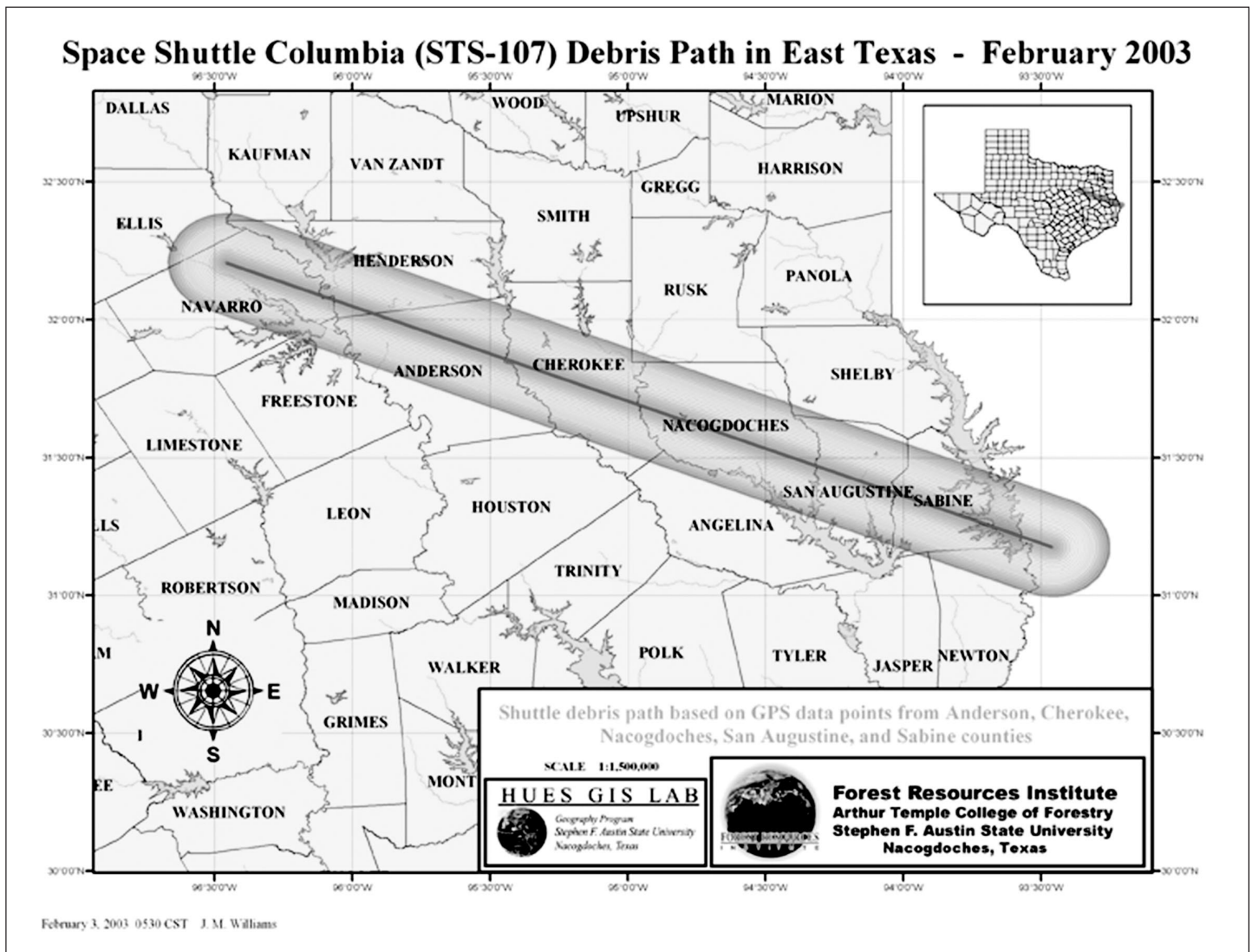
Source: Forest Resources Institute, Arthur Temple College of Forestry, Stephen F. Austin State University.

Assessment Program Has Been Extensively Revised

The Coast Guard has made significant revisions to adapt the Port Security Assessment Program to the increasing amount of security evaluations performed by port stakeholders and to address shortcomings in the program's initial implementation. The Coast Guard initially set out to use the program as an assessment of security conditions at 55 ports. The Coast

Guard and the contractor it hired to develop the assessment approach and conduct the assessments started the first assessments in August 2002, when other assessment efforts were also under way. Port stakeholders around the country had begun or already completed their own assessments of their facilities or vessels in order to identify security vulnerabilities of their assets or obtain federal assistance in strengthening their security. Even more security information was to become available as new regulatory requirements were implemented in 2003 requiring security assessments to be performed by the owners or operators of facilities and vessels operating in the nation's ports. This changing security environment and higher-than-expected costs to complete the contractor's initial assessments prompted the Coast Guard to revise the scope of the contractor's assessments. Our examination of the contractor's initial assessments identified additional shortcomings in the quality of the work and the assessment approach. In response, the Coast Guard temporarily postponed all assessment work to make further revisions, both to take advantage of the other sources of assessment information and make the assessments more useful in port security planning efforts. The revised program (1) added a GIS as a new feature and (2) tailored security assessments for particular purposes, such as synthesizing existing assessments or assessing certain infrastructure at the direction of local Coast Guard personnel. The assessments are to be completed by February 2005—but the Coast Guard is still developing its GIS and is uncertain as to when the GIS will be ready for use.

Program Initially Focused on Assessing Post-9/11 Vulnerabilities at Key Ports

The Coast Guard began the Port Security Assessment Program to assess the vulnerabilities of the nation's most strategic commercial and military ports in the aftermath of the September 11, 2001, terrorist attacks. (See fig. 3 for a timeline of the program.) To identify which ports were most strategic, the Coast Guard considered such factors as cargo volume, import/export cargo value, volume of passenger traffic on ferries or cruise ships, population density around the port, the presence of critical infrastructure or key assets, the presence of military forces or bases, and whether the port was designated to support major military deployments. From this analysis, 55 ports out of 361 ports were chosen to be the first to receive port security assessments.

Figure 3: Timeline of Key Events in the Development of Port Security Assessment Program
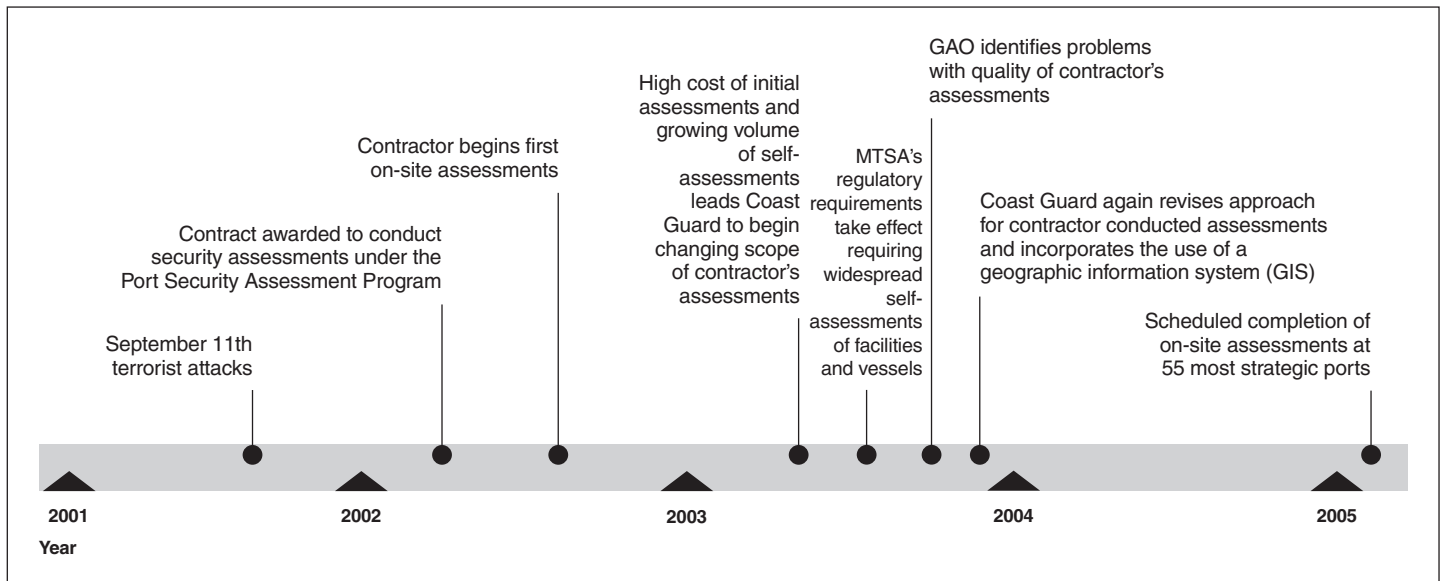
Source: GAO analysis.

In April 2002, the Coast Guard selected a contractor to perform the assessments. Under this arrangement, the contractor was responsible for developing an approach (which the Coast Guard calls "Version 1") to assess vulnerabilities of port assets and systems such as cargo facilities, manufacturing facilities, passenger terminals, power generation and fuelling facilities, as well as other infrastructure such as public access areas and bridges. The assessment was to identify the relationships between selected assets to port systems, identify the vulnerabilities of those assets to terrorist attacks, and recommend actions to mitigate the vulnerabilities.[3] With oversight from the Coast Guard, the contractor had primary responsibility for conducting key activities of each assessment, such as identifying which assets should be assessed, collecting data from stakeholders, making on-site visits, and analyzing the data collected. The final product was to be a comprehensive written report of the findings identified during the assessment. Primary customers for this work were

---

[3]In addition to conducting port vulnerability assessments of the ports identified as strategic commercial and military seaports, the contractor was to develop model port security guidelines and a port vulnerability self-assessment tool for ports that did not receive a port vulnerability assessment. We did not examine the development of these components of the Coast Guard's program.

the local Coast Guard Captain of the Port and port stakeholders serving on Area Maritime Security Committees, who could use it in such security planning efforts as the development of an Area Maritime Security Plan.[4]

The first assessments began in August 2002; the Coast Guard's goal was to complete them at all 55 ports by the end of 2004.[5] To further refine the approach before assessing "megaports" such as New York/New Jersey or Los Angeles/Long Beach, as well as to give the program a chance to build additional assessment teams to perform the work, the Coast Guard decided to try out the approach at medium-sized ports first such as San Diego and Boston. Under the time frame the Coast Guard adopted, officials expected to conduct assessments of 8 ports in 2002, 18 in 2003, and 24 in 2004.[6]

Need to Incorporate Work Done by Others and Correct Shortcomings in Contractor's Assessments Led to Revisions in the Approach

Several actions taken by port stakeholders led to substantial changes in the approach. One of these developments was that many port stakeholders were starting or completing assessments on their own. Stakeholders, such as port authorities, and owners and operators of facilities and vessels began conducting assessments in order to identify security vulnerabilities of their assets or to meet application requirements for federal grants. In some cases, initial assessments were performed shortly after the September 11, 2001, terrorist attacks and were followed by more comprehensive assessments conducted either on their own or by

---

[4]The Captain of the Port is a Coast Guard officer who provides direction to Coast Guard law enforcement activities within the general proximity of the zone in which assigned. Under the regulations implementing the Maritime Transportation Security Act of 2002, the Captain of the Port develops the Area Maritime Security Plan for his or her zone in consultation with the Area Maritime Security Committee that is comprised of members from federal, local, and state governments; law enforcement agencies; maritime industry and labor organizations; and other port stakeholders that may be affected by security policies. The Plan is to provide a communication and coordination framework for the port stakeholders and law enforcement officials to follow in addressing security vulnerabilities and responding to any incidents. Prior to the Maritime Transportation Security Act of 2002, this committee and plan were known generically as port security committees and port security plans.

[5]The original program goal, as stated in the Contract Request for Proposals and Statement of Work, was to complete assessments at the 55 ports by March 2005. That goal was accelerated subsequent to contract award in an effort to complete assessments sooner.

[6]In addition to the assessments being performed under the Port Security Assessment Program, the Coast Guard considers five assessments conducted by the Defense Threat Reduction Agency (DTRA) as completed assessments for the purposes of meeting this deadline. DTRA is an agency within the Department of Defense.

contractors. For example, port stakeholders such as chemical producers that were members of certain industry or trade organizations were required to complete assessments of their facilities using approved assessment methodologies as a condition of their membership in the organization. Beginning in September 2002, the Coast Guard also issued a series of suggested guidelines[7] for port stakeholders to use in conducting security assessments and developing security plans to address any identified vulnerabilities.

In addition to the assessment activities that many stakeholders voluntarily undertook after the terrorist attacks, more maritime security information became increasingly available as the Maritime Transportation Security Act began to be implemented. Enacted in November 2002, MTSA mandated major changes in the nation's approach to maritime security and called for a comprehensive framework that includes planning, personnel security, and careful monitoring of vessels and cargo. The regulations implementing MTSA required owners or operators of specific facilities and vessels in the nation's ports to conduct assessments and develop plans to address vulnerabilities. These security assessments and plans were to be reviewed and approved by the Coast Guard prior to July 1, 2004.[8] As a result, facilities and vessels that had not already completed a security assessment were now required to do so, thereby increasing the amount of assessment information available from port stakeholders at the 55 ports as July 1, 2004, drew nearer.

Coupled with the changes in the amount of information to be generated by others, high costs for the first set of assessments prompted the Coast Guard to begin reassessing the Version 1 approach for conducting the assessments. According to the Coast Guard, assessments for the first 8 ports cost nearly three times more than was originally expected, exceeding $1 million per port. To address this issue, the Coast Guard made changes in the assessment approach, including greater emphasis on discussions early on in the assessment process with local Coast Guard Captains of the Port in order to better focus on the facilities and

---

[7]These guidelines were contained in *Navigation and Vessel Inspection Circulars* (NVICs), an approach the Coast Guard uses to provide detailed guidance about enforcement or compliance with certain federal marine safety regulations and Coast Guard marine safety programs.

[8]For more information on these security plans and assessments requirements see GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, GAO-04-838 (Washington, D.C.: June 30, 2004).

infrastructure needing to be assessed and the adoption of a standardized report outline and format to reduce redundancy.[9] The Coast Guard decided to pilot-test this new approach, which the Coast Guard now calls "Version 2," at two ports in the summer of 2003.

As this new approach was being readied, our own review of the contractor's assessments disclosed additional shortcomings. In a September 2003 testimony before the Senate Committee on Commerce, Science, and Transportation, we expressed concern about how the assessment program was being implemented.[10] In talking with some port stakeholders who participated in the assessment, we found that many of them saw little usefulness in the assessments beyond what they already knew about their vulnerabilities from previously completed assessments. Some key port stakeholders declined to participate in the assessment after receiving lengthy questionnaires from the contractor asking for information stakeholders considered proprietary. Port stakeholders also said they had not been given the opportunity to review or comment on the draft assessment report, which contained errors and inaccuracies. Finally, the contractor was moving to use the Version 2 approach in the next set of assessments before the lessons learned from the pilot tests could be identified and incorporated into the assessment approach.

We shared our findings with Coast Guard officials and suggested that the assessment approach be further revised. In addition to giving the Captains of the Port and Coast Guard personnel a larger role in identifying the critical assets to be assessed, we suggested that the Coast Guard reduce duplication and lessen the burden on stakeholders by doing more to take into account already-completed assessments of facilities and assets. The Coast Guard agreed and postponed conducting more assessments until additional changes to address these deficiencies were made.

---

[9]These changes came out of a process improvement workshop the Coast Guard conducted for the assessment program in April 2003. Participants in this workshop included a Captain of the Port representative that had received an assessment of their port, a Captain of the Port who had not yet received an assessment of their port, DHS representatives, and other Coast Guard officials involved in port security.

[10]See GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*, GAO-03-1155T (Washington, D.C.: Sept. 9, 2003).

Subsequent Revisions Incorporated the Use of a GIS and More Focused Assessments

While considering what changes needed to be made to the assessment program, the Coast Guard also determined that it was essential to provide local Coast Guard officials and certain members of the local Area Maritime Security Committee a means to retrieve maritime security information and display it for planning and response purposes at the ports. Although a significant amount of security information was now available, it was kept in disparate locations and was not readily available. With the regulations implementing MTSA requiring Captains of the Port and Area Maritime Security Committees to develop portwide Area Maritime Security Plans, access to the available security information became increasingly important in order for them to carry out this responsibility and improve the protection of the marine transportation system.

To provide local Coast Guard officials and certain members of the local Area Maritime Security Committee access to this information, the Coast Guard decided to incorporate a GIS as a new feature in the assessment program. At the local port level, the GIS would integrate the security information into a single electronic database that would allow the information to be retrieved and displayed within the context of a particular port area. Whereas previous assessment results were compiled into a published report that would characterize the port's security posture at a single point in time, GIS has the capability of being updated as new information becomes available. GIS also provides a tool for visually depicting the port and for retrieving security or assessment information as needed in the development or revision of Area Maritime Security Plans. The Coast Guard believes this will benefit the Captains of the Port and the Area Maritime Security Committees to better visualize the port and enhance their ability to develop security plans as well as respond to a security incident, should one occur.

In addition to the GIS component, the revised program has three other components, all related to assessments. The Coast Guard revised the assessment approach so that it would provide more specialized information about port security. The approach, known as Version 3, has three different types of assessments that collectively are aimed at providing both a synthesis of what is already known about security at a port and studies of specific topics or infrastructure that have not been fully assessed. When completed, these assessments will provide the core security information to populate the GIS. These assessment components are as follows:

- *Assessment of Assessments*—An identification and inventory of completed security assessments of port assets and critical infrastructure

within a port. This inventory is designed to help the assessment team minimize the possibility of needlessly duplicating previously completed assessments as well as to provide the Captain of the Port and the Area Maritime Security Committee with greater awareness of existing security information.

- *Terrorist Operations Assessment*—An assessment utilizing the expertise of contractors comprised of former Navy Special Operations personnel to provide an outsider perspective on the ports' vulnerabilities to a terrorist attack. This assessment is to evaluate potential terrorist targets within the ports and identify likely attack scenarios for the Captain of the Port and Area Maritime Security Committee to consider addressing in the Area Maritime Security Plan.

- *Special Assessment*—Assessment of specific port assets, infrastructure, or operations that are critical to the port but have not been previously assessed from a maritime perspective. Performed at the request of the Captain of the Port and the Area Maritime Security Committee, this assessment is to provide vulnerability, impact, and countermeasure information on those assets, infrastructure, or operations. Examples include blast impact assessments of commercial vessels, plume dispersion assessments of an attack on vessel or facility with hazardous materials, and security assessments of underwater tunnels.

The Coast Guard has a more definite schedule for completing the assessments than for completing the GIS. The Coast Guard resumed assessments in March 2004 using the Version 3 approach and plans to complete assessments at the remaining ports by February 2005.[11] For the GIS component, the Coast Guard plans to use its own GIS. Until this system is operational for port security, the Coast Guard plans to lease a commercial GIS that will enable Coast Guard staff to familiarize themselves with how a GIS works and identify their specific system needs or requirements so the Coast Guard's GIS can be customized accordingly. Project officials chose a commercial-off-the-shelf software application, iMap,[12] that provides the Coast Guard access to over 800 layers of data

---

[11]With the start of the new Version 3 assessment approach, the assessment program had $36 million in appropriated funds remaining. According to the program manager, this amount will be sufficient to complete the three non-GIS components at the ports yet to be assessed.

[12]iMap can be used to collect information, merge it analytically, and provide it interactively to users.

containing information related to the nation's ports. Because the Coast Guard's GIS is still in development for port security, when the GIS component will be made operational and available to all assessed ports is yet to be determined.[13]

Absence of Key Management Elements Places Program's Potential to Enhance Port Security at Higher Risk

The Coast Guard's revised approach appears to provide a useful planning and response tool for port security, but the implementation of the assessment program is at higher risk because of two major problems. First, the centerpiece of the new approach, the GIS component, is being developed without several key project management steps that are critical to success in such projects. Not following these steps increases the risk that the data collected will not provide port security officials with the information they need to adequately assess, identify, and mitigate security risks. Second, for the GIS component and the program as a whole, the Coast Guard lacks a strategy that clearly defines how the program will be managed, how much it will cost, or what activities will continue over the longer term. Lack of a strategy increases the risk of cost overruns, missed deadlines, and a less-than-effective program. At the same time the Coast Guard is facing these problems, it is also conducting security assessments at individual ports using the revised approach, and for this part of the program, the results to date appear more favorable. Early indications from local Coast Guard officials at the ports where the new assessments have been performed are that these assessments are of some usefulness in current security planning activities. However, not resolving the broader planning and management issues could also affect the potential value of these assessments to fill in any remaining gaps in the Coast Guard's awareness of the security posture in the ports.

GIS Component Seen as Having Great Potential, but Coast Guard Is Not Following Established Project Management Practices

The Captains of the Port and other Coast Guard officials we talked with were in agreement in their belief that a GIS with security assessment information would greatly facilitate their security planning and response efforts. They provided such examples as the following, based on their understanding of the tools that would be available with the GIS:

---

[13]According to Coast Guard officials, a "beta"–or test-version was available by the end of August 2004 for the ports of Charleston, Boston, and New York/New Jersey, using the commercial GIS as the platform.

- For planning efforts, the visual nature of the GIS would greatly enhance the Captain of the Port's and Area Maritime Security Committee's understanding of the connections between port facilities, assets, and infrastructure that would otherwise not be possible through paper reports.

- For incident response efforts, the capability of GIS to store and retrieve security information such as plans and assessments of particular assets within the port would quicken response times as the information can be immediately located and viewed.

A useful, well-designed system does appear to carry great promise. For example, if Coast Guard personnel were alerted that a particular port may be targeted and that warehouses containing shipping containers were at risk, officials could quickly create a map showing the location and contents of the warehouses, ingress points located near the warehouses, and depth of the nearby waterways throughout the port. Using this information, security officials could assess the relative risk to each warehouse, prioritize actions based on the risk level, and act almost immediately to secure the most vulnerable locations.

However, developing a useful GIS is a significant and complex challenge. One reason is that every port has its own unique mix of geographic characteristics and operations that must be accurately captured. For example, one port may be located along a stretch of river while another may sit next to the open ocean, one port may have a high volume of cruise ship traffic while another may have a high concentration of chemical and petroleum facilities. These different characteristics will require a GIS that is flexible enough to be of use in a variety of settings. Another reason the GIS can be challenging is that some security-related situations, such as potential terrorist activities, involve a great deal of unpredictability and the kinds of information and analyses needed to address such uncertainty are difficult to anticipate.

This complexity places a premium on proper planning. Over the years, we have analyzed information technology systems across a broad range of federal programs and agencies, and these analyses have repeatedly shown that without adequate planning, the risks increase for cost overruns, schedule slippages, and systems that are not effective or usable. For example, the Bureau of Land Management (BLM) spent more than $67 million on a system that was never deployed. When the system was tested prior to deployment, it was found not to meet users' requirements because it did not support BLM's business activities, was too complex, and significantly impeded worker productivity. We found this system failed

because it was developed without a clear understanding of requirements and without a credible project schedule with reliable milestones.[14] In another example, the Centers for Medicare and Medicaid Services had similar problems that led to its planned Medicare Transaction System being cancelled—the project did not have fully defined and agreed-to requirements and had a flawed project schedule.[15]

These types of problems make it prudent to ensure that planning of GIS applications is adequate. Coast Guard officials indicated that they viewed the development of the port security GIS database as an add-on to existing Coast Guard information systems, not as a new database or information system. Within this context, however, it is still important to ensure that the steps being taken are likely to produce a satisfactory result. In that light, we assessed the Coast Guard's development efforts using established best practices in the industry for developing information technology systems, including those created by the Institute of Electrical and Electronics Engineers/Electronic Industries Alliance.[16] The Coast Guard's current efforts do not apply these criteria in two key ways—defining what the GIS should do and establishing sufficient plans to ensure that the requirements can be successfully realized. That is, successful implementation of the Coast Guard's port security GIS is at higher risk because the Coast Guard has not used established project management practices, including defining

---

[14]See GAO, *Land Management Systems: Progress and Risks in Developing BLM's Land and Mineral Record System*, GAO/AIMD-95-180 (Washington, D.C.: Aug. 31, 1995); *Land Management Systems: BLM Faces Risks in Completing the Automated Land and Mineral Record System*, GAO/AIMD-97-42 (Washington, D.C.: Mar. 19, 1997); *Land Management Systems: Actions Needed in Completing the Automated Land and Mineral Record System Development*, GAO/AIMD-98-107 (Washington, D.C.: May 15, 1998); and *Land Management Systems: Major Software Development Does Not Meet BLM's Business Needs*, GAO/AIMD-99-135 (Washington, D.C.: Apr. 30, 1999).

[15]*Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses*, GAO/AIMD-97-78 (Washington, D.C.: May 16, 1997).

[16]Institute of Electrical and Electronics Engineers/Electronic Industries Alliance, *IEEE/EIA Guide for Information Technology* (IEEE/EIA 12207.1 – 1997), April 1998. The Institute and Alliance developed this guidance to provide a common framework for developing and managing software. IEEE standards are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those outside of IEEE that have expressed an interest in participating in the development of the standard. The Alliance is a national trade organization whose mission is promoting the market development and competitiveness of the U.S. high-tech industry through domestic and international policy efforts.

requirements and developing a project schedule, to oversee and guide the program.

Actions to Develop GIS Requirements Do Not Meet Standards

One aspect of developing any information technology system such as a GIS involves establishing and maintaining a common and unambiguous definition of functional requirements among the project team, system users, and software developer. These requirements define what the system will be expected to do for its users once it is developed and implemented. For example, one requirement could be to ensure that the system can link together specified types of geospatial data to provide the user with sufficient information. Another requirement could be to ensure that the users would be provided the capability of printing paper maps and other information found in the GIS. A third could be that the GIS be available to its users 24 hours a day, 7 days a week. Requirements such as these could be important in ensuring that the system will deliver what users need. It is critical that functional requirements are carefully defined and that they flow directly from how the organization's day-to-day operations are or will be carried out to meet mission needs. Improperly defined or incomplete requirements have been commonly identified as a root cause for why systems fail or do not meet their cost, schedule, or performance goals. Without adequately defined requirements, significant risk exists that a system will need extensive and costly changes before it will meet the organization's needs.

The Coast Guard's actions to develop GIS requirements are not being carried out using established practices. The Coast Guard's approach for addressing these requirements takes three main forms:

- First, the Coast Guard is using the assessments being conducted at the 55 ports to identify requirements for the GIS it is developing.

- Second, the Coast Guard is using feedback from the experiences of local officials with the commercial-off-the-shelf software application currently in use to help determine what requirements should be included.

- Finally, the contractor supporting the interim GIS has been tasked to identify the GIS data layers most frequently used by the Coast Guard.

However, these actions fall short of meeting best practices. First, there are indications that requirements identified during the assessment visits did not necessarily include functional requirements. Second, although tasks to identify the data layers accessed by the Coast Guard using its interim GIS solution could be used to identify requirements for the port security GIS,

these tasks have not yet been completed and there is no estimate as to when the information will be available.

According to Coast Guard officials, the Coast Guard intends to use an existing information system instead of building a new GIS database or information system that is exclusive to port security. However, while the Coast Guard is not developing a new system, greater planning efforts appear paramount. To the extent that the Coast Guard and other users believe they need to add new kinds of data that do not currently exist in the system, both system users and developers need to agree on how to define and capture this information so that it can be of maximum use. In addition, if the Coast Guard decides to take a more limited approach, adding few, if any, new functional requirements, it runs the risk that the system will be of only partial use. Rather than taking advantage of the powerful planning and analysis capabilities that a robust geographic information system could make available, the more limited version could only be used to develop static maps of ports and their assets. Without effectively identifying and documenting the requirements for the new potential functions and data associated with the port security portion of its GIS, the Coast Guard faces the risk that the GIS will not provide port security officials with the functionality and information they need to adequately assess, identify, and mitigate security risks.

Coast Guard GIS Planning Does Not Meet Established Best Practices

Information technology project management principles and industry best practices[17] emphasize that a project management plan is needed to define the technical and managerial processes necessary to satisfy project requirements. The plan should include, among other activities,

- developing a work breakdown structure with a schedule for all of the tasks to be performed;

- identifying and addressing project risks, and

- implementing a security policy.

The planning document identified by the Coast Guard does not meet these standards. According to the Port Security Assessment program manager,

---

[17]Institute of Electrical and Electronics Engineers/Electronic Industries Alliance, *IEEE/EIA Guide for Information Technology* (IEEE/EIA 12207.1 – 1997), April 1998.

the Coast Guard considers the project's Concept of Operations[18] to be its project plan. However, the Concept of Operations, does not include important elements required in a project plan. For example:

- **Tasks and schedules**: The Concept of Operations identifies seven Port Security Assessment Program objectives, one of which is the use of a GIS, but does not identify any of the tasks or a schedule for carrying them out. It also provides a list of eight high-level activities that need to be completed during the project, but again it lists no associated implementation tasks and schedule, although it estimates that port security assessments will be completed by December 2004. Since the document was written in February 2004, the assessment completion date has already been postponed by 2 months, and the project manager is unsure if the interim GIS contract will need to be renewed next spring because he is not sure when the Coast Guard's own port security GIS will be completed and ready for implementation.

- **Project risk**: The Concept of Operations does not address project risks. As a result of not identifying potential risks, the project has encountered unexpected problems. For example, two of the eight high-level activities identified in the Concept of Operations, scheduled to be completed in April and July 2004, encountered unexpected problems that caused delays and could hinder their eventual completion.

- **Security Policy and Project costs**: The Concept of Operations does not address security policy and provides no plan for estimating project costs. For example, we asked program officials to provide documented cost information associated with the GIS component, and while we received some information, it was not sufficient to provide a clear indication of how much the GIS component would likely cost.[19]

---

[18]A concept of operations is a statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations. The concept is designed to give an overall picture of the operation and provide additional clarity of purpose. This written Concept of Operations was dated February 2, 2004.

[19]The Coast Guard indicated to us that for fiscal years 2005-2007, expected program costs for the Port Assessment Program as a whole will total about $30.8 million. Of this amount, $5.4 million is for the GIS component. For fiscal year 2004, the Coast Guard indicated that $1.5 million was supplied towards the development of its own GIS and that an estimated $900,000 will be spent for the use of the commercial GIS that the Coast Guard is using on an interim basis. The Coast Guard projected costs for continued development and implementation of the GIS for fiscal years 2005 to 2007 to total $3 million. However, the documentation we received lacks sufficient detail to indicate whether these amounts are all that will be spent, and the information the Coast Guard supplied is silent on any costs beyond fiscal year 2007.

Creating a plan that meets these requirements is essential to ensuring that the port security assessment GIS project can be successfully completed in the estimated timeframes with the resources that are available. The Coast Guard has already encountered problems caused by lack of a reliable project schedule and risk assessment. According to Coast Guard Officials, the Coast Guard is adding to an existing system rather than building a new one. Adding to an existing system, however, does not obviate the need for careful planning. Until the Coast Guard develops a project management plan that includes a schedule and milestones, it is at increased risk that the GIS component of its port security assessment program could be inadequately managed, resulting in schedule slippages and inaccurate costs estimates. In addition, without identifying and mitigating risks and security concerns, the project could encounter unexpected issues that would need to be addressed, resulting in additional schedule and cost problems.

Incomplete GIS Planning Places Usefulness of New Assessments at Greater Risk

The Coast Guard has proceeded to carry out the revised assessments of individual ports with generally favorable results. The Coast Guard resumed its assessment program using the Version 3 assessment components in March 2004 and as of August 1, 2004, had completed on-site assessments of 12 additional ports in 6 Captain of the Port zones.[20] To provide an indication of the usefulness of these assessments, we spoke with the local Captain of the Port or other Coast Guard officials that participated in the assessment process at each of these zones. In general, all agreed that the assessments were of some usefulness. Two said that the assessments provided substantially new information that they did not previously have or consider. The other four found the completed assessment results useful by bringing an outside perspective to look at the port. They said the assessments were helpful in validating their previously completed assessments or the current awareness of the security posture within their ports.

The value of these assessments could be enhanced, we believe, if the Coast Guard addressed the key management practices we have already discussed in its approach for developing its GIS. By themselves, the current assessments have value to local Coast Guard officials mostly in supplementing or validating their knowledge. However, when used with

---

[20]There are a total of 45 Captains of the Port zones nationwide. These zones may contain more than one port depending on how their geographic boundaries are defined.

the GIS, these assessments also have potential value in helping the officials "close the loop" on information they may lack. The three assessment components involve mainly data gathering and analysis, the results of which are to be fed into the GIS. Without the GIS to integrate and organize information gathered from these and other sources, those responsible for planning security cannot as easily identify the vulnerabilities in their ports and gaps in their awareness of the security posture within their ports that need to be addressed. At all of the six ports, the Captain of the Ports or other Coast Guard officials said the value of the three assessment components would be enhanced if used in conjunction with a GIS that would be better able to visually display the entire security posture of the port rather than having to review individual hard copy assessment reports as they are now published. However, the functional requirements need to be first defined in order to effectively integrate these assessment components into the GIS. Until this planning step is taken, the value of these assessments could fail to reach their full potential.

Planning Concerns for GIS Component Extends to Overall Management and Direction of the Program

Finally, the uncertainty brought on by the lack of planning for the GIS component is reflected in a similar uncertainty for the Port Security Assessment Program as a whole. For the assessment components, future plans are unclear beyond fiscal year 2005. Once all assessment reports of the 55 strategic ports are completed—a task the Coast Guard expects to be done by February 2005— the Coast Guard currently expects the assessment of assessments component to be an ongoing effort that will be updated by Coast Guard personnel as new assessment information becomes available. It expects the special assessments and terrorist operations assessments to continue through fiscal year 2005 as ports previously assessed under earlier assessment approaches are revisited, but it has made no decision about continuing them beyond that time.

Beyond fiscal year 2005, the Coast Guard is currently considering two options for what to do with the special assessment and terrorist operations assessment components of the program. The options are (1) continuing the program at other ports beyond the initial 55 or (2) conducting some recurring assessment at the 55 ports. Our discussions with Captains of the Port and Coast Guard officials surfaced mixed views of the future need for the three assessment components. One Captain whose port had been assessed under the Version 3 approach said he would like the assessment team to return to his port within 2 years, in order to assess the security measures put in place after the completion of the last assessment. By contrast, Captains for two other ports said they did not think that the team needed to return unless the critical infrastructure in

their ports changed dramatically. The Coast Guard official responsible for the program said that as of July 2004, discussions were underway between program officials, other Coast Guard teams, and DHS officials as to how the program should proceed in the future to best augment port security efforts. The outcome of these discussions and future funding provided to the program will largely determine the extent to which the three assessment components continue to be implemented as part of the program.

Although the GIS component will continue to be enhanced, its schedule for completion and implementation is uncertain. Thus, when the various program components—GIS and port assessments—are taken together, it is not clear what activities will be conducted over the longer term, who will do them, or how much they will cost.

Conclusions

As the Coast Guard attempts to determine the future of the Port Security Assessment Program, it needs to ensure that the program provides maximum effectiveness to its main customers, Captains of the Port and Area Maritime Security Committees. The initial program had shortcomings that created a product of marginal value. The revised program has potential to be more useful because it intends to integrate all of the assessment information collected by the Coast Guard and other relevant security authorities and place this information in a GIS. However, the Coast Guard risks producing a system that is not as useful as it could be, because its approach lacks a defined management strategy, specific cost estimates, and a clear implementation schedule. Developing the program's GIS component in this way is of particular concern, given the problems that have resulted when other agencies used the same approach in attempting to develop their information technology systems. And without a clear development strategy for GIS, the usefulness of the three assessment components may also be limited, because local Coast Guard officials and Area Maritime Security Committees will be less able to use them to fill the remaining gaps in their awareness of the security posture within their ports. Getting this project right is important, because the prospect of a well functioning GIS has great appeal to many Coast Guard and other port stakeholders, who believe such a tool will be of considerable help in providing effective port security.

Recommendations for Executive Action

To help ensure that the revised Port Security Assessment Program provides the most effective tool possible for security planning and response, we recommend that the Secretary of Homeland Security direct the Commandant of the Coast Guard to (1) define and document the GIS functional requirements and (2) develop a long-term project plan for the GIS and the Port Security Assessment Program as a whole (including cost estimates, schedule, and management responsibilities).

Agency Comments

We provided a draft of this report to the Department of Homeland Security and the Coast Guard for their review and comment. The Coast Guard's Marine Safety, Security And Environmental Protection Directorate generally agreed with our recommendations, including the need to finalize data types and develop a detailed work plan for adding map layers. Coast Guard officials provided a number of technical clarifications, which we incorporated where appropriate to ensure the accuracy of our report.

The Coast Guard commented in detail on two aspects of our report:

- The Coast Guard said our report tended to overlook many of the program's significant achievements, particularly the value of the three assessment components. The Coast Guard emphasized the progress that it had made on tailoring assessments, completing them on schedule, and reducing their cost from more than $1 million per port to about $200,000 per port.

- The Coast Guard also said our characterization of its GIS made it appear that the Coast Guard was developing an entirely new information technology system. The Coast Guard emphasized that its GIS was part of an existing information technology system.

Regarding these concerns, we would make the following points:

- First, the amount of emphasis the report places on GIS reflects our review of Coast Guard documents and interviews with numerous local Coast Guard officials, which showed that when compared with the three assessment components, the GIS had the potential to provide substantially more value. The program's Concept of Operations contains multiple references to the critical and central role the GIS component will hold in providing a dynamic tool to its users (Captains of the Port and Area Maritime Security Committees) for port security planning and response. Further, the end users we talked with expressed near unanimous need for
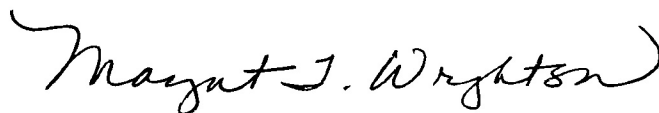
a dynamic GIS planning and response tool to increase maritime domain awareness.

- Second, we acknowledge that the Coast Guard's GIS is part of a pre-existing information technology system. In our view, however, this is not the key point. The point is the need for GIS planning and functional requirements. When we assessed the Coast Guard's development efforts against established industry best practices for developing information technology systems, we found the Coast Guard's current efforts do not apply two key practices: defining what the GIS system should do and establishing plans sufficient to ensure that the functional requirements can be successfully realized. Our past work has shown that when other agencies tried to develop systems without these practices, problems resulted. In short, without adequate planning, we believe that the GIS—and with it, the Port Security Assessment Program—is at risk of foundering. Hence, the aim of our recommendation is to produce a more effective GIS tool for port security officials. If the Coast Guard does establish functional requirements and a clear strategy for its GIS, the system will more likely meet its potential, and port security officials will be more likely to use it effectively.

We are sending copies of this report to relevant congressional committees and subcommittees, the Secretary of Homeland Security, the Commandant of the Coast Guard, and other interested parties.

If you or your staffs have any questions about this report, please contact me at (415) 904-2200 or at wrightsonm@gao.gov or Steve Calvo, Assistant Director, at (206) 287-4800 or at calvos@gao.gov. Key contributors to this report are listed in appendix II. This report will also be available at no charge on the GAO Web site at http://www.gao.gov.

Margaret T. Wrightson
Director, Homeland Security
  and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Our two objectives for this report were to (1) discuss why and how the Port Security Assessment Program has changed over time and (2) assess the Coast Guard's approach for implementing the Port Security Assessment Program as it is currently configured

To address why and how the assessment program changed, we reviewed Coast Guard documents, interviewed officials at Coast Guard headquarters responsible for implementing the program, and visited three ports that had been assessed under the previous program assessment approach. At these ports, we interviewed local Coast Guard personnel as well numerous stakeholders to determine their views about how the assessment process was carried out. These stakeholders included, for example, operators of container terminals, power plants, cruise ship terminals, port authorities, and chemical facilities. We also relied on our previous work related to the program.[1] For background information on the role of the geographic information system (GIS) as a tool for planning and response, we identified city and state government agencies that have GIS's in place and talked with GIS managers and experts from these agencies. We also met with federal government GIS experts who had experience with implementing GIS within the federal environment. They included experts from the Federal Emergency Management Agency, Bureau of Customs and Border Patrol, and United States Geological Survey. Finally, we met with GIS experts at universities and elsewhere to further our understanding.

To assess the Coast Guard's approach for implementing the Port Security Assessment Program in its current form, we interviewed a variety of Coast Guard and other officials. For GIS, we interviewed the Coast Guard's GIS Program Manager and others to determine the progress made to date. For the assessment portion of the program, we interviewed Coast Guard officials from the six Captain of the Port zones that are responsible for the security of the 12 ports assessed under the most recent program approach. To establish criteria for assessing the program's current approach, we reviewed Coast Guard documents. We also reviewed information and documentation related to GIS applications and identified industry best practices for information systems acquisition and development to determine criteria for managing such a project. We reviewed documentation of the Coast Guard's efforts to modify its port security GIS

---

[1]See GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain,* GAO-03-1155T (Washington, D.C.: Sept. 9, 2003).

to determine whether the progress made met the criteria we established. In conducting our assessment, we also relied upon our work on the development of major information technology systems throughout the federal government.[2]

Our work, which was conducted from June 2003 through August 2004, was done in accordance with generally accepted government auditing standards.

---

[2]See GAO, *Land Management Systems: Progress and Risks in Developing BLM's Land and Mineral Record System*, GAO/AIMD-95-180 (Washington, D.C.: Aug. 31, 1995); *Land Management Systems: BLM Faces Risks in Completing the Automated Land and Mineral Record System*, GAO-AIMD-97-42 (Washington, D.C.: Mar. 19, 1997); *Land Management Systems: Actions Needed in Completing the Automated Land and Mineral Record System Development*, GAO-AIMD-98-107 (Washington, D.C.: May 15, 1998); *Land Management Systems: Major Software Development Does Not Meet BLM's Business Needs*, GAO-AIMD-99-135 (Washington, D.C.: Apr. 30, 1999); and *Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses*, GAO/AIMD-97-78 (Washington, D.C.: May 16, 1997).

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Margaret Wrightson (415) 904-2200
Steven Calvo (206) 287-4800

Staff Acknowledgments

In addition to those named above, Chuck Bausell, Jason Berman, Christopher Hatscher, Nicholas Larson, Elizabeth Roach, and Stan Stenersen made key contributions to this report.